

Author index

- Abdalla, M., 469, 474
 Adleman, L. M., 2, 323–326
 Agnew, G. B., 416
 Agrawal, M., 240
 Agrell, E., 379
 Ajtai, M., 378
 Akishita, T., 197
 Alexi, W., 450
 Alon, N., 533
 Ankeny, N. C., 29
 Antipa, A., 463
 Araki, K., 558
 Arney, J., 273
 Arène, C., 173
 Atkin, A. O. L., 37, 164

 Babai, L., 253, 366, 371
 Bach, E., 29, 299, 532
 Bachem, A., 33
 Balasubramanian, R., 557, 558
 Barreto, P. S. L. M., 552, 553, 561
 Bellare, M., 57, 414, 453, 455, 461, 469, 474, 508, 509, 511
 Bellman, R., 219
 Bender, E. A., 273
 Bentahar, K., 23, 426
 Berlekamp, R., 40
 Bernstein, D. J., 40, 172, 215, 240, 279, 509, 510
 Birkner, P., 172
 Bisson, G., 540
 Blackburn, S. R., 273
 Blake, I. F., 219, 317, 319
 Bleichenbacher, D., 395, 461, 467, 494, 507
 Blichfeldt, H. F., 343
 Block, H., 247
 Blum, M., 440, 491
 Blömer, J., 390, 506
 Boneh, D., 233, 394, 412, 426, 434, 443, 445, 448, 450, 463, 480, 481, 489, 501, 506, 511
 Boppa, R. B., 533
 Bos, J. W., 272, 278, 280

 Bosma, W., 140
 Bostan, A., 526, 528
 Bourgain, J., 448
 Boyen, X., 463
 Boyko, V., 416
 Brands, S., 257
 Brauer, A., 215
 Brent, R. P., 29, 269, 273, 298, 300
 Brickell, E. F., 216
 Brier, E., 502, 504
 Brown, D. R. L., 423, 435, 437, 463
 Brumley, B. B., 228
 Bröker, R., 166, 524, 543
 Burgess, D. A., 29
 Burmester, M., 407

 Canetti, R., 58, 414
 Canfield, E. R., 302, 310
 Cantor, D. G., 42, 191, 193, 197
 Carter, G., 272
 Cash, D., 424, 474
 Cassels, J. W. S., 178, 204, 206
 Catalano, D., 499
 Chao, J., 230
 Charlap, L. S., 546
 Charles, D. X., 535, 543
 Chaum, D., 57, 502
 Cheon, J.-H., 272, 435, 437
 Chor, B., 450
 Clavier, C., 502, 504
 Cocks, C., 2
 Cohen, H., 163, 219
 Cohen, P., 524
 Coley, R., 546
 Collins, T., 487
 Cook, S., 22
 Coppersmith, D., 258, 317, 319, 380, 381, 384, 388, 489, 502, 504
 Coron, J.-S., 388, 417, 490, 501, 502, 504, 508, 509
 Couveignes, J.-M., 528, 529, 532
 Couvreur, C., 487

604

Author index

- Cox, D. A., 162, 167, 523, 530
 Cramer, R., 408, 470, 471, 474, 478, 511
 Crandall, R. E., 298
- Damgård, I. B., 29, 56
 Davenport, H., 211
 Davies, D., 57
 Dawson, E., 272
 De Feo, L., 529
 De Jonge, W., 502
 de Rooij, P., 459
 Deligne, P., 159
 DeMarras, J., 324–326
 den Boer, B., 426, 427
 Denny, T. F., 317
 Desmedt, Y., 407, 478, 501
 Deuring, M., 162
 Dewaghe, L., 522, 532
 Diem, C., 328, 332, 333
 Diffie, W., 2, 405
 Dimitrov, V. S., 221
 Dixon, J., 303
 Doche, C., 222
 Dujella, A., 27, 506
 Durfee, G., 394, 506
 Duursma, I. M., 211, 278, 553
- Edwards, H. M., 172
 Elgamal, T., 408, 459
 Elkies, N. D., 164, 525
 Ellis, J., 2
 Enge, A., 326, 333, 524
 Erdős, P., 302, 310
 Erickson, S., 203
 Eriksson, T., 379
 Euchner, M., 365, 375
- Farashahi, R. R., 172
 Finke, U., 375
 Fischlin, R., 450
 Flajolet, P., 264, 266
 Flassenberg, R., 326
 Floyd, 267
 Flynn, E. V., 178, 204, 206
 Fontaine, C., 479
 Fouquet, M., 538
 Franklin, M. K., 233, 480, 481, 501, 502
 Freeman, D., 494, 561
 Frey, G., 328, 545, 548, 550, 557
 Fuji-Hara, R., 317, 319
 Fujisaki, E., 511
 Fürer, M., 23
- Galand, F., 479
 Galbraith, S. D., 176, 198, 200, 230, 286, 295, 296, 507, 532, 541, 543, 553, 560
- Gallant, R. P., 220, 226, 228, 276, 279, 423, 435, 437, 463
 Gao, S., 44
 Garay, J. A., 461
 Garefalakis, T., 548
 von zur Gathen, J., 44, 233
 Gaudry, P., 170, 179, 197, 278, 292, 327, 328, 330, 333
 Gauss, C. F., 347
 Gel'fond, A. O., 250
 Gennaro, R., 499
 Gentry, C., 494, 511
 Giesbrecht, M., 44
 Girault, M., 468, 502
 Goldreich, O., 58, 394, 450, 494
 Goldwasser, S., 8, 453
 Gong, G., 99
 González Vasco, M. I., 448
 Gordon, D. M., 322
 Goren, E. Z., 535
 Granger, R., 99, 552
 Granville, A., 396
 Grieu, F., 504
 Gross, B. H., 167, 535
- Hafner, J. L., 32, 325
 Halevi, S., 58, 504
 Hanrot, G., 377
 Harley, R., 196, 279, 328
 Harn, L., 99
 Harrison, M., 198, 200
 Hasse, H., 211
 Håstad, J., 380, 383, 442, 500
 Havas, G., 33
 van Heijst, E., 57
 Helfrich, B., 375
 Hellman, M. E., 2, 247, 317, 405
 Heneghan, C., 507
 Hess, F., 328, 532, 541, 542, 548, 550, 552–557, 560
 Hilbert, D., 69
 Hildebrand, A., 311
 Hildebrand, M. V., 273
 Hitchcock, Y., 272
 Hoffstein, J., 416
 Hofheinz, D., 512
 Hohenberger, S., 507
 Holmes, M., 296
 Hong, J., 272
 Hopkins, D., 487
 Horwitz, J., 272
 Howe, E. W., 176
 Howgrave-Graham, N. A., 381, 394, 398, 400, 447, 466, 499
 Huang, M.-D., 325, 326
- Icart, T., 222, 234
 Iijima, T., 230

- Jacobson Jr., M. J., 198, 203
 Jager, T., 255
 Jao, D., 450, 466, 534, 543, 544
 Jetchev, D., 450
 Jiang, Z.-T., 443
 Joux, A., 323, 324, 412, 501
 Joye, M., 172, 219, 545
 Jullien, G. A., 221
 Jutla, C. S., 387, 504
 Järvinen, K. U., 228
- Kaib, M., 350, 365
 Kaihara, M. E., 272, 280
 Kannan, R., 33, 373, 375
 Karatsuba, A. A., 22
 Katagi, M., 197
 Katz, J., 6, 231
 Kayal, N., 240
 Kiltz, E., 424, 474, 494, 512
 Kim, H. Y., 552
 Kim, J. H., 272
 Kim, M., 272
 King, B., 237
 Kitamura, I., 197
 Klein, P. N., 371
 Kleinjung, T., 272, 278
 Knudsen, E. W., 221
 Knuth, D. E., 264
 Koblitz, N., 176, 178, 209, 222, 416, 557, 558
 Kohel, D. R., 99, 222, 236, 522, 535, 536, 538–540
 Konyagin, S.-V., 448
 Kozaki, S., 436
 Kraitchik, M., 303, 313
 Krawczyk, H., 414
 Kuhn, F., 264, 271
 Kuhn, R. M., 206
 Kumar, R., 378
 Kurosawa, K., 478
 Kutsuma, T., 436
- Labahn, G., 33
 Lagarias, J. C., 379
 Lagrange, J.-L., 347
 Laih, C.-S., 220, 461
 Lambert, R. J., 220, 226, 228, 276, 279, 463
 Lanczos, C., 32, 308, 316
 Lang, S., 162, 523, 530
 Lange, T., 40, 172, 173, 215
 Langford, S., 487
 Lauter, K. E., 524, 535, 543
 Lee, E., 554
 Lee, H.-S., 553, 554
 Lehmer, D. H., 242
 Lehmer, D. N., 242
 Lennon, M. J. J., 94
 Lenstra Jr., H. W., 44, 140, 162, 163, 176, 177, 228, 244, 269, 309, 311, 347, 358, 379, 416, 434
- Lenstra, A. K., 97, 98, 220, 228, 237, 279, 347, 358, 504
 Lercier, R., 323, 324, 526, 528, 529
 Leurent, G., 58
 Li, W.-C., 443, 449
 Lichtenbaum, S., 548
 Lin, X., 230
 Lindell, Y., 6, 231
 Lindner, R., 371, 402
 Lipton, R. J., 426, 434
 Lockhart, P., 187
 Lovorn Bender, R., 318, 319
 Lovász, L., 347, 358, 365, 397
 Lubicz, D., 170, 179
 Lucas, E., 92
 Lynn, B., 552
 Lüneburg, H., 44
- M'Raihi, D., 417, 461
 Majewski, B. S., 33
 Matsuo, K., 230, 436
 Matthews, K. R., 33
 Maurer, U. M., 311, 426, 429
 May, A., 390, 490, 506, 507
 McCurley, K. S., 32, 322, 325
 McKee, J. F., 163, 176, 507
 Meier, W., 224–226
 Menezes, A. J., 6, 222, 545, 557, 558
 Merkle, R., 2, 56
 Mestre, J.-F., 164, 534, 535
 Micali, S., 8, 440
 Micciancio, D., 33, 400, 453
 Miller, G. L., 490
 Miller, S. D., 272, 534, 544
 Miller, V. S., 236, 333, 548, 552
 Miller, W. C., 221
 Minkowski, 344
 Mireles, D. J., 198, 200
 Misarsky, J.-F., 502
 Miyaji, A., 219
 Monico, C., 280
 Montague, P., 272
 Montenegro, R., 272, 284, 287
 Montgomery, P. L., 30, 31, 168, 243, 269, 280
 Morain, F., 38, 216, 278, 526, 528, 529, 532, 538
 Mullin, R. C., 317, 319, 416
 Mumford, D., 189, 190
 Murphy, S., 273
 Murty, M. R., 533, 534
 Murty, R., 176
 Muzereau, A., 426, 434
 Möller, B., 219, 220
 Müller, V., 228
- Naccache, D., 396, 461, 501, 502, 504
 Naehrig, M., 173, 561
 Nechaev, V. I., 247, 250, 253

- Neven, G., 455, 457, 545
 Nguyen, P. Q., 58, 337, 347, 350, 365, 378, 395, 412, 447, 448, 466, 499, 501
 Nicolas, J.-L., 38
 Niederreiter, H., 40
 Nivasch, G., 269
 Näslund, M., 442, 443, 448, 449
- Odlyzko, A. M., 266, 317, 501
 Oesterlé, J., 535
 Ó hÉigeartaigh, C., 553
 Okamoto, T., 511, 545, 557, 558
 Olivos, J., 216
 O'Malley, S. W., 416
 Ono, T., 219
 Onyszchuk, I. M., 416
 van Oorschot, P. C., 6, 269, 281, 285, 287, 288, 296, 297
 Orman, H. K., 416
 Oyono, R., 552
- Paillier, P., 457, 463, 497, 498, 509
 Park, C.-M., 554
 Patarin, J., 502
 Patel, S., 442
 Paulus, S., 198, 200, 203, 326
 Peikert, C., 371, 402
 Peinado, M., 416
 Peres, Y., 272
 Peters, C., 172
 Pfitzmann, B., 57
 Pila, J., 311, 434
 Pinch, R. G. E., 506
 Pizer, A. K., 535
 Pohst, M., 375
 Pointcheval, D., 414, 454, 455, 457, 460, 463, 511
 Pollard, J. M., 242, 245, 262, 273, 281, 282, 286, 287, 290, 297, 298, 312
 Pomerance, C., 298, 302, 308–311, 318, 319, 434
 van der Poorten, A. J., 198
 Poupard, G., 468
 Price, W. L., 57
- Quisquater, J.-J., 487
- Rabin, M. O., 487, 491
 Rabin, T., 461
 Rackoff, C., 306
 Raphaeli, D., 461
 Regev, O., 400, 466
 Reiter, M. K., 501, 502
 Reiter, R., 224
 Reitwiesner, G., 216
 Reyneri, J. M., 317
 Ritter, H., 365
 Ritzenthaler, C., 173
- Rivest, R. L., 2, 8, 269
 Rogaway, P., 55, 57, 414, 469, 474, 508, 509, 511
 Ron, D., 394
 Rosen, A., 494
 Rubin, K., 88, 89, 95
 Ruprai, R. S., 286, 295
 Rück, H.-G., 161, 198, 200, 203, 545, 548, 550, 557–559
- Sabin, M., 487
 Salvy, B., 526, 528
 Satoh, T., 439, 558
 Sattler, J., 272
 Saxena, N., 240
 Scarf, H. E., 365
 Schinzel, A., 233
 Schirokauer, O., 317, 324
 Schnorr, C.-P., 269, 272, 350, 364, 365, 375, 379, 416, 450, 452, 456, 467
 Schoof, R., 38, 162, 164, 525
 Schost, E., 292, 526, 528
 Schroepel, R. C., 221, 247, 308, 317, 416
 Schulte-Geers, E., 276
 Schwarz, J. T., 255
 Schwenk, J., 255
 Schönhage, A., 23
 Scott, M., 230, 552, 553, 555, 561
 Sedgewick, R., 264, 269
 Segev, G., 494
 Semaev, I. A., 329, 558
 Seroussi, G., 219
 Serre, J.-P., 534, 558
 Shallit, J. O., 29, 216
 Shallue, A., 233
 Shamir, A., 2, 219, 468
 Shang, N., 203
 Shanks, D., 197, 250
 Shen, S., 203
 Shoup, V., 231, 250, 253, 306, 408, 422, 424, 470, 471, 474, 478, 511
 Shparlinski, I. E., 176, 233, 236, 396, 443, 447–450, 466, 504
 Sidorenko, A., 231
 Silver, R. I., 247
 Silverberg, A., 88, 89, 95
 Silverman, J. H., 334, 416
 Silverman, R. D., 272
 Sinclair, A., 233
 Sirvent, T., 526
 Sivakumar, D., 378
 Skalba, M., 233
 Skinner, C., 94
 Smart, N. P., 1, 219, 324, 328, 426, 434, 447, 457, 466, 532, 541, 542, 553, 558
 Smith, B. A., 333

- Smith, P. J., 94
 Solinas, J. A., 219, 221, 224, 226
 Soukharev, V., 543
 Soundararajan, K., 318
 Spatscheck, O., 416
 Staffelbach, O., 224–226
 Stam, M., 97, 168, 221, 228
 Stapleton, J., 272
 Stark, H. M., 527
 Stehlé, D., 350, 364, 365, 377
 Stein, A., 203, 326
 Stein, J., 25
 Stern, J., 337, 454, 455, 457, 460, 468, 511
 Stern, J. P., 504
 Stichtenoth, H., 207, 208, 211
 Stinson, D. R., 1, 258, 298
 Stolbunov, A., 543
 Storjohann, A., 33
 Strassen, V., 23, 245
 Straus, E. G., 219
 Struik, R., 264, 271, 463
 Sudan, M., 394
 Sundaram, G. S., 442
 Sutherland, A. V., 49, 250, 524, 540
 Suyama, H., 170
 Szemerédi, E., 253
 Szymanski, T. G., 269
- Takagi, T., 197, 487
 Tate, J., 209, 548
 Tenenbaum, G., 311
 Teske, E., 265, 269, 272, 288, 561
 Tetali, P., 272, 284, 287
 Thomé, E., 320, 322, 328, 333
 Thurber, E. G., 215
 Thériault, N., 328, 552
 Tibouchi, M., 501
 van Tilborg, H. C. A., 506
 Toom, A., 22
 Tsujii, S., 230
 Tymen, C., 417
- Vallée, B., 347, 350
 Vanstone, S. A., 6, 220, 222, 226, 228, 276, 279, 317, 319, 416, 463, 545, 557, 558
 Vardy, A., 379
 Vaudenay, S., 1, 461, 463
 Venkatesan, R., 272, 416, 443, 445, 448, 450, 489, 534, 544
 Vercauteren, F., 99, 324, 426, 434, 552–555, 560
 Vergnaud, D., 457, 463
 Verheul, E. R., 97, 98, 237, 506, 562
 Vidick, T., 378
 Villar, J. L., 497
 Voloch, J. F., 161
 Vèlu, J., 517
- Wang, Y.-M., 443
 Warinschi, B., 33, 457
 Washington, L. C., 163
 Waters, B., 507
 Weber, D., 317
 Weinmann, R.-P., 501
 Wiedemann, D. H., 32, 308, 316
 Wiener, M. J., 269, 276, 281, 285, 287, 288, 296, 297, 505
 Williams, H. C., 493, 497
 Williamson, M. J., 405
 Winterhof, A., 448
 van de Woestijne, C. E., 233
 Wolf, S., 311, 426
- Xing, C., 211
 Xu, W.-L., 443
- Yao, A. C.-C., 269
 Yen, S.-M., 219, 220, 461
 Yoshida, K., 466
- Zassenhaus, H., 42
 Zeger, K., 379
 Zierler, N., 46
 Zimmermann, P., 23, 29
 Zuccherato, R. J., 276

Subject index

- Abel-Jacobi map, 119, 205
- Abelian variety, 204
- absolutely simple, 204
- adaptive chosen-message attack, 8
- adaptive chosen-ciphertext attack, 7
- addition chain, 35
- additive group, 62
- additive rho walk, 265
- adjacency matrix, 533
- advantage, 19, 407, 440, 472
- adversary against an identification protocol, 454
- affine n -space over k , 66
- affine algebraic set, 66
- affine coordinate ring, 69
- affine line, 66
- affine plane, 66
- affine variety, 75
- affine Weierstrass equation, 105
- AKS primality test, 240
- algebraic, 568
- algebraic closure, 568
- algebraic group, 61
- algebraic group quotient, 63
- algebraic torus, 88
- algebraically independent, 387
- algorithm, 13
- amplifying, 21
- amplitude, 395
- anomalous binary curves, 160
- anomalous elliptic curves, 558
- approximate CVP, 345
- approximate SVP, 345
- ascending chain, 572
- ascending isogeny, 536
- asymmetric cryptography, 2
- ate pairing, 553
- attack goals for public key encryption, 6
- attack goals for signatures, 8
- attack model, 6
- automorphism, 143
- auxiliary elliptic curves, 433
- average-case complexity, 16
- B -power smooth, 242
- B -smooth, 242
- Babai nearest plane algorithm, 370
- Babai rounding, 225
- Babai's rounding technique, 371
- baby step, 199
- Barret reduction, 31
- base- a probable prime, 240
- base- a pseudoprime, 240
- basic Boneh–Franklin scheme, 480
- basis matrix, 339
- batch verification of Elgamal signatures, 461
- BDH, 481
- Big O notation, 14
- big Omega, 15
- big Theta, 15
- bilinear Diffie–Hellman problem, 481
- binary Euclidean algorithm, 25
- birational equivalence, 80
- birthday bound, 253
- birthday paradox, 262, 578
- bit i , 576
- bit-length, 576
- black box field, 427
- Blichfeldt Theorem, 343
- block Korkine–Zolotarev, 379
- Blum integer, 491
- Boneh–Joux–Nguyen attack, 412
- Brandt matrix, 535
- Burmester–Desmedt key exchange, 407
- canonical divisor class, 135
- Cantor reduction step, 193
- Cantor's addition algorithm, 192
- Cantor's algorithm, 191
- Cantor's composition algorithm, 192
- Cantor–Zassenhaus algorithm, 42
- Carmichael lambda function, 239, 486
- Cayley graph, 533
- CCA, CCA1, CCA2, 7
- c -expander, 533
- characteristic, 565

- characteristic polynomial, 157, 571
 characteristic polynomial of Frobenius, 158, 208
 Cheon's variant of the DLP, 435
 Chinese remainder theorem, 571
 Chinese remaindering with errors problem, 394
 chord-and-tangent rule, 116
 chosen plaintext attack, 7
 ciphertext, 3
 circle group, 67
 classic textbook ElGamal encryption, 408
 clients, 273
 closest vector problem (CVP), 345
 CM method, 163
 co-DDH problem, 560
 coefficient explosion, 357
 cofactor, 237
 collapsing the cycle, 279
 collision, 262, 298
 Collision resistance, 54
 complete group law, 172, 174
 complete system of addition laws, 140
 Complex multiplication, 159, 162, 175, 530
 complex multiplication method, 163
 Complexity, 14
 composite residuosity problem, 499
 compositeness witness, 238
 composition and reduction at infinity, 199
 composition of functions, 564
 compositum, 568
 compression function, 56
 compression map, 91, 96
 computational problem, 13
 COMPUTE-LAMBDA, 489
 COMPUTE-PHI, 489
 conditional probability, 577
 conductor, 536, 576
 conjugate, 90
 connected graph, 530
 conorm, 126, 128
 constant function, 77
 continuation, 243
 continued fraction expansion, 26
 convergents, 26
 Coppersmith's theorem, 384
 Cornacchia algorithm, 38
 coupon collector, 578
 covering attack, 329
 covering group, 63, 94, 98
 CPA, 7
 Cramer–Shoup encryption scheme, 475
 crater, 538
 CRT list decoding problem, 394
 CRT private exponents, 487
 cryptographic hash family, 54
 curve, 104
 cycle, 266
 cyclotomic polynomial, 86
 data encapsulation mechanism, 471
 DDH algorithm, 407
 DDH assumption, 407
 de-homogenisation, 72
 decision closest vector problem (DCVP), 345
 decision Diffie–Hellman problem (DDH), 406
 decision learning with errors, 400
 decision problem, 14
 decision shortest vector problem, 345
 decision static Diffie–Hellman problem, 423
 decompression map, 91, 96
 decrypt, 3
 decryption algorithm, 5
 decryption oracle, 439
 Dedekind domain, 123
 defined, 77
 defined over \mathbb{k} , 68, 70, 71, 111
 degree, 111, 122, 146, 325, 568
 DEM, 471
 den Boer reduction, 427
 dense, 81
 density, 218
 derivation, 131
 derivative, 566
 descending isogeny, 536
 Desmedt–Odlyzko attack, 501
 determinant, 340, 574
 deterministic algorithm, 14
 deterministic pseudorandom walk, 264
 DHIES, 469
 diameter, 530
 Dickman–de Bruijn function, 301
 Diem's algorithm, 332
 differentials, 133
 Diffie–Hellman tuples, 407
 digit set, 222
 dimension, 83
 diophantine approximation, 25, 397
 discrete, 339
 discrete logarithm assumption, 405
 discrete logarithm in an interval, 252
 discrete logarithm problem, 14, 246
 discrete valuation, 108
 discriminant, 105, 575
 d -isogeny, 146
 distinguished point, 269
 Distinguished points, 269
 distortion map, 561, 562
 distributed computing, 273
 Distributed rho algorithm, 273
 distribution, 576
 division polynomials, 156
 divisor, 111
 divisor class, 115
 divisor class group, 115
 divisor of a differential, 134
 divisor of a function, 112

610

Subject index

- divisor-norm map, 127
- Dixon's random squares, 303
- DL-LSB, 439
- DLP, 14, 246
- DLP in an interval, 252
- DLWE, 400
- dominant, 81
- DSA, 462
- DStatic-DH, 423
- DStatic-DH oracle, 472
- dual isogeny, 151
- dual lattice, 343
- eavesdropper, 406
- ECDSA, 462
- ECIES, 469
- ECM, 244
- edge boundary, 533
- effective, 111
- effective affine divisor, 188
- eigenvalues of a finite graph, 533
- Eisenstein's criteria, 566
- Elgamal encryption, 439
- Elgamal public key signatures, 460
- elliptic curve, 105
- elliptic curve method, 244
- embedding degree, 550
- embedding technique, 373
- encapsulates, 471
- encoding, 254
- encrypt, 2
- encryption algorithm, 5
- encryption scheme, 5
- endomorphism ring, 146
- entropy smoothing, 55
- epact, 267
- ephemeral keys, 406
- equation for a curve, 104
- equivalence class, 63
- Equivalence classes, 276
- equivalence of functions, 77
- equivalent, 20, 144, 188, 225
- equivalent isogenies, 516
- eth roots problem, 489
- Euclidean norm, 573
- Euler phi function, 565
- Euler's criterion, 28
- Euler–Mascheroni constant, 565
- event, 576
- existential forgery, 8
- expander graph, 533
- expectation, 577
- expected exponential-time, 16
- expected polynomial-time, 16
- expected subexponential-time, 16
- expected value, 264
- explicit representation, 426
- exponent, 564
- exponent representation, 61
- exponential-time, 15
- exponential-time reduction, 20
- extended Euclidean algorithm, 24
- extension, 124, 568
- Extra bits for Rabin, 493
- FACTOR, 489
- factor base, 303, 305
- family of groups, 441
- FDH-RSA, 508
- Fermat test, 238
- Fiat–Shamir transform, 456
- field of fractions, 572
- final exponentiation, 551
- finitely generated, 565, 568, 571
- fixed base, 215, 219
- fixed pattern padding, 391, 502
- Fixed-CDH, 418
- Fixed-Inverse-DH, 420
- Fixed-Square-DH, 420
- floating-point LLL, 364
- floor, 536
- Floyd's cycle finding, 267
- Forking Lemma, 455
- four-kangaroo algorithm, 287
- free module, 565
- Frobenius expansion, 222
- Frobenius map, 122, 149, 208
- full domain hash, 508
- full rank lattice, 338
- fully homomorphic, 478
- function, 564
- function field, 76, 77
- function field sieve, 322
- fundamental parallelepiped, 575
- Galbraith's algorithm, 541
- Galbraith–Hess–Smart algorithm, 542
- Galois, 569
- Galois cohomology, 570
- Galois group, 569
- game, 6
- gap Diffie–Hellman problem, 472
- Garner's algorithm, 32
- Gaudry's algorithm, 327
- Gaussian heuristic, 344
- generic algorithm, 254
- generic chosen-message attack, 464
- genus, 130, 182
- genus 0 curve, 136
- geometric distribution, 577
- geometrically irreducible, 75
- GIMPS, 273
- GLV lattice, 226, 229
- GLV method, l -dimensional, 229

- Gong-Harn cryptosystem, 99
 Gordon's algorithm, 241
 Gram–matrix, 341
 Gram–Schmidt orthogonalisation, 574
 Gram–Schmidt algorithm, 574
 greatest common divisor, 190
 Group automorphism, 63
 group decision Diffie–Hellman problem, 422
 group defined over \mathbb{k} , 150
 GSO, 574

 Hafner–McCurley algorithm, 325
 half trace, 45
 Hamming weight, 35, 258
 hardcore bit, 440
 hardcore bit for the DLP, 441
 hardcore bits, 440
 hardcore predicate, 440
 hardcore predicate for the DLP, 441
 hash Diffie–Hellman, 474
 hash-DH, 474
 Hasse interval, 159
 Håstad attack, 500
 head, 266
 Hensel lifting, 43
 Hermite constant, 344
 Hermite normal form, 575
 hidden number problem, 444, 467
 Hilbert 90, 70, 570
 Hilbert Nullstellensatz, 69
 HNF, 575
 HNP, 444
 homogeneous coordinate ring, 72
 homogeneous coordinates, 70
 homogeneous decomposition, 566
 homogeneous ideal, 71
 homogenisation, 73
 homomorphic, 479
 homomorphic encryption, 479
 horizontal isogeny, 536
 Horner's rule, 39
 Hurwitz class number, 162, 167, 175, 529
 Hurwitz genus formula, 137
 hybrid encryption, 410, 471, 512
 hyperelliptic curve, 182
 hyperelliptic equation, 178
 hyperelliptic involution, 178
 hyperplane, 67
 hypersurface, 67

 ideal, 68, 571
 identity matrix, 573
 identity-based cryptography, 468, 480
 imaginary hyperelliptic curve, 182
 imaginary quadratic field, 575
 implicit representation, 426
 IND, 6

 IND-CCA security, 7
 independent events, 577
 independent random variables, 577
 independent torsion points, 235
 index calculus, 314
 indistinguishability, 6
 indistinguishability adversary, 6
 inert model of a hyperelliptic curve, 182
 inert place, 182
 inner product, 573
 input size, 14
 inseparable, 122
 inseparable degree, 122
 instance, 13
 instance generator, 17
 interleaving, 220
 invalid parameter attacks, 411
 invariant differential, 153
 inverse limit, 156
 Inverse-DH, 419
 irreducible, 75, 565, 566
 isogenous, 146
 isogeny, 146, 204
 isogeny class, 529
 isogeny problem for elliptic curves, 540
 isomorphic, 81
 isomorphism of elliptic curves, 142
 isomorphism of pointed curves, 142
 i th bit, 576

 Jacobi symbol, 28
 Jacobian matrix, 103
 Jacobian variety, 116, 204
 j -invariant, 142
 joint sparse form, 221

 kangaroo method, 282
 kangaroo, tame, 282
 kangaroo, wild, 282
 Karatsuba multiplication, 22, 486
 KEM, 471
 kernel, 146
 Kernel lattice, 345
 Kernel lattice modulo M , 345
 key derivation function, 408
 key encapsulation, 2
 key encapsulation mechanism, 471
 key only attack, 8
 key transport, 2, 471
 keyed hash function, 54
 KeyGen, 5
 known message attack, 8
 Koblitz curves, 160
 Korkine–Zolotarev reduced, 379
 k -regular, 530
 Kronecker substitution, 39
 Kronecker symbol, 28, 531

612

Subject index

- Krull dimension, 83
- Kruskal's principle, 285
- Kummer surface, 178
- L*-polynomial, 207
- ℓ_2 -norm, 573
- ℓ_a -norm, 573
- ladder methods, 93
- Lagrange–Gauss reduced, 348
- large prime variation, 309
- Las Vegas algorithm, 16
- lattice, 338
- Lattice basis, 338, 345
- lattice dimension, 338
- Lattice membership, 345
- lattice rank, 338
- l*-bit string, 576
- learning with errors, 400
- least significant bit, 576
- Legendre symbol, 27
- length, 22, 216
- Length of a Frobenius expansion, 222
- linear congruential generator, 410, 453
- linear map, 573
- linearly equivalent, 115
- Little O notation, 15
- LLL algorithm, 358
- LLL-reduced, 353
- local, 572
- local properties of varieties, 101
- local ring, 101
- localisation, 101, 572
- loop shortening, 553
- Lovász condition, 353
- low Hamming weight DLP, 258
- low-exponent RSA, 486
- LSB, 576
- LUC, 92, 94, 449
- lunchtime attack, 7, 501
- LWE, 400
- LWE distribution, 400
- MAC, 56
- map, 564
- match, 262
- maximal ideal, 108, 572
- mean step size, 282
- meet-in-the-middle attack, 296
- Merkle–Damgård construction, 56
- Mersenne prime, 442
- message authentication code, 56
- message digest, 3
- messages, 406
- Miller function, 550
- Miller–Rabin test, 239
- Minkowski convex body theorem, 343
- Minkowski theorem, 344
- mixing time, 272
- $M(n)$, 23
- mod, 564
- model, 82
- model for a curve, 104
- modular curve, 523
- modular exponentiation, 33
- modular polynomial, 523
- module, 565
- monic, 566
- Monte Carlo algorithm, 16
- Montgomery model, 168
- Montgomery multiplication, 30, 33
- Montgomery reduction, 30
- Montgomery representation, 30
- morphism, 81
- most significant bits, 441, 443
- MOV/FR attack, 557
- MSB, 443
- MTI/A0 protocol, 415
- multi-base representations, 221
- multi-dimensional discrete logarithm problem, 257, 292
- multi-exponentiation, 219
- multiplicative group, 62
- multiplicative subset, 572
- multi-prime-RSA, 487
- Mumford representation, 190
- NAF, 216
- naive Schnorr signatures, 456
- nearly Ramanujan graph, 534
- negligible, 18
- Newton identities, 208
- Newton iteration, 23
- Newton root finding, 23
- NFS, 312, 317
- NIST primes, 31
- Noetherian, 572
- non-adjacent form, 216, 223
- non-singular, 103, 104
- non-uniform complexity, 15
- Norm, 88, 90, 128, 568, 571
- norm map, 224
- normal basis, 570
- normalised isogeny, 521
- noticeable, 18
- n*-torsion subgroup, 139
- NUCOMP, 197
- Nullstellensatz, 110
- number field sieve, 312, 317
- OAEP, 511
- $O(n)$, 14
- $\hat{O}(n)$, 15
- $o(n)$, 15
- one-way encryption, 6

- one-way function, 3
 one-way permutation, 3
 optimal normal basis, 40
 optimal pairing, 554
 oracle, 6, 19
 oracle replay attack, 454
 orbit, 63
 order, 108, 134, 564, 575
 ordinary, 165, 210
 original rho walk, 265
 orthogonal, 573
 orthogonal complement, 574
 orthogonal matrix, 573
 orthogonal projection, 366, 574
 orthogonality defect, 342
 orthonormal, 574
 output distribution, 17, 408
 output size, 14
 overwhelming, 18
 OWE, 6
- padding scheme, 4
 Paillier encryption, 498
 pairing inversion problem, 559
 pairing-friendly curves, 561
 parallel collision search, 296
 parallel computing, 273
 parameterised assumption, 465
 passive attack, 7, 8, 406
 path, 530
 path in a graph, 530
 perfect adversary, 7
 perfect algorithm, 17
 perfect field, 569
 perfect oracle, 19
 perfect power, 24
 π -adic expansions, 222
 π -NAF, 223
 place of a function field, 122
 plane curve, 104
 Pohlig–Hellman, 247
 Poincaré reducibility theorem, 204
 point at infinity, 105, 182
 pointed curve, 142
 pole, 109
 Pollard kangaroo method, discrete logarithms, 280
 Pollard rho algorithm, factoring, 298
 Pollard rho pseudorandom walk, factoring, 298
 Pollard's FFT continuation, 243
 polynomial basis, 570
 polynomial-time, 15
 polynomial-time equivalent, 20
 polynomial-time reduction, 20
 p -rank, 210
 preimage resistant, 54, 408
 primality certificate, 241
 primality test, 238
- prime, 565
 prime divisor, 191, 325
 prime number theorem, 240
 primitive, 86
 primitive element theorem, 569
 principal divisor, 112
 principal ideal, 571
 private key, 2
 probable prime, 240
 processors, 273
 product discrete logarithm problem, 257
 product tree, 47
 projective algebraic set, 71
 projective closure, 73
 projective hyperelliptic equation, 183
 projective line, 70
 projective plane, 70
 projective space, 70
 projective variety, 75
 pseudoprime, 238
 pseudorandom, 265
 PSS, 509
 public key cryptography, 2
 public key identification scheme, 452
 pullback, 81, 82, 126
 purely inseparable, 568
 pushforward, 127
- q -SDH, 465
 q -strong Diffie–Hellman problem, 465
 quadratic non-residue, 27
 Quadratic reciprocity, 28
 quadratic residue, 27, 571
 quadratic sieve, 308
 quadratic twist, 144, 145, 170, 187
 quotient, 63
- Rabin cryptosystem, 491
 Rabin–Williams cryptosystem, 492, 493
 radical, 571
 Ramanujan graph, 533, 535
 ramification index, 125
 ramified model of a hyperelliptic curve, 182
 ramified place, 182
 random oracle model, 58
 random self-reducible, 20
 random variable, 577
 randomised, 16
 randomised algorithm, 16
 randomised encryption, 4
 randomised padding scheme, 485
 randomness extraction, 235
 rank, 565, 573
 rational, 89
 rational functions, 77
 rational map, 79
 Rational parameterisation, 95

- rational points, 67
- re-winding attack, 454
- real hyperelliptic curve, 182
- real or random security, 415
- reduced, 195, 200
- reduced divisor, 197
- reduced Tate–Lichtenbaum pairing, 551
- reducible, 75
- reduction, 19
- redundancy in the message for Rabin, 492
- regular, 77, 79
- relation, 304
- reliable, 19
- reliable oracle, 21
- repeat, 262
- representation problem, 257
- residue degree, 124
- restriction, 124
- resultant, 567
- rho algorithm, discrete logarithms, 264
- rho graph, 272
- rho walks, 265
- Riemann hypothesis for elliptic curves, 159
- Riemann–Roch space, 129
- ring class field, 162
- ring of integers, 575
- Robin Hood, 296
- root of unity, 86
- RSA, 485
- RSA problem, 489
- RSA-PRIVATE-KEY, 489

- SAEP, 511
- safe prime, 241
- Sato–Tate distribution, 176
- Schnorr identification scheme, 452
- Schnorr signature scheme, 452, 456
- Schönhage–Strassen multiplication, 23
- second stage, 243
- Second-preimage resistance, 54
- security parameter, 5, 17
- security properties, 6
- selective forgery, 8
- self-corrector, 21
- Selfridge–Miller–Rabin test, 239
- semantic security, 6
- semi-reduced, 188
- semi-textbook Elgamal encryption, 408
- separable, 122, 146, 568
- separable degree, 122
- separating element, 131
- separating variable, 131
- Serial computing, 274
- server, 273
- session key, 406
- set of RSA moduli, 489
- SETI, 273

- short Weierstrass form, 105
- shortest vector problem (SVP), 345
- sieving, 308
- signature forgery, 8
- signature scheme, 7
- simple, 204
- simple zero, 108
- simultaneous diophantine approximation problem, 397
- simultaneous modular inversion, 31
- simultaneous multiple exponentiation, 219
- simultaneously hard bits, 442
- singular, 103
- singular point, 104
- sliding window methods, 34
- small private exponent RSA, 505
- Small public exponents, 486
- small subgroup attacks, 411
- smooth, 103, 309, 325
- smooth divisor, 325
- Smooth integers, 242
- smooth polynomial, 317
- SNFS, 324
- snowball algorithm, 49
- Soft O notation, 15
- Solinas, J. A., 224
- Sophie Germain prime, 241
- sparse matrix, 32, 308
- special q -descent, 320
- special function field sieve, 324
- special number field sieve, 312, 324
- split an integer, 41
- split Jacobian, 205
- split model of a hyperelliptic curve, 182
- split place, 182
- splits, 238
- splitting system, 259
- SQRT-MOD-N, 495
- square, 571
- square-and-multiply, 33
- Square-DH, 419
- square-free, 40
- SSL, 2
- Standard continuation, 243
- standard model, 58
- Stark’s algorithm, 527
- static Diffie–Hellman, 410, 423
- Static-DH, 423
- Static-DH oracle, 439
- statistical distance, 578
- statistically close, 578
- Stirling’s approximation to the factorial, 576
- strong Diffie–Hellman, 472
- strong forgery, 8
- strong prime, 241
- strong prime test, 239
- strong–DH, 472

- STRONG-RSA, 490
 strongly B -smooth, 242
 subexponential, 302
 subexponential function, 302
 subexponential-time, 15
 subexponential-time reduction, 20
 subgroup generated by g , 564
 sublattice, 339
 subvariety, 75
 succeeds, 18
 success probability, 18
 successful, 407
 successful adversary, 6
 successive minima, 342
 summation polynomials, 329
 superpolynomial-time, 15
 supersingular, 160, 165, 210
 support, 111
 surface, 536
 system parameters, 410, 452

 tail, 266
 Takagi–RSA, 488
 target collision resistant, 55
 target message forgery, 8
 Tate isogeny theorem, 154, 529, 532
 Tate module, 156
 Tate’s isogeny theorem, 209
 Tate–Lichtenbaum pairing, 548
 tau-adic expansions, 222
 tensor product, 565
 textbook Elgamal public key encryption, 408
 textbook RSA, 2
 three-kangaroo algorithm, 286
 tight security reduction, 509
 TLS, 2
 Tonelli–Shanks algorithm, 36
 Toom–Cook multiplication, 22
 tori, 449
 torsion-free module, 148
 torus-based cryptography, 86, 89
 total break, 6, 8
 total degree, 566
 total variation, 578
 trace, 64, 92, 158, 568, 571
 trace-based cryptography, 86
 trace of Frobenius, 158
 trace polynomial, 42
 transcendence basis, 568
 transcendence degree, 568
 transcendental, 568
 translation, 102
 transpose, 573
 trapdoor, 3

 trapdoor one-way permutation, 3
 trial division, 238
 trivial twist, 144
 tunable balancing of RSA, 487
 twist, 144
 twisted Edwards model, 172

 UF, 8
 UF-CMA, 8
 Unified elliptic curve addition, 138
 uniform complexity, 15
 uniform distribution, 576
 uniformiser, 106
 uniformising parameter, 106
 unimodular matrix, 340, 575
 unique factorisation domain, 565
 unramified, 125, 146
 unreliable, 19
 unreliable oracle, 21
 useless cycles, 278

 valuation ring, 108
 value, 77
 value of a function, 77
 variable base, 215, 219
 Verschiebung, 151
 vertex boundary, 533
 volcano, 538
 volume, 340
 Vèlu’s formulae, 517

 weak chosen-message attack, 464
 Weierstrass equation, 105
 weight, 218
 weight of a Frobenius expansion, 222
 weighted projective space, 74
 Weil bounds, 208
 Weil descent, 328
 Weil pairing, 235, 546
 Weil reciprocity, 545
 Weil restriction of scalars, 84, 88
 Wiener attack, 505
 Williams integer, 493, 509
 window length, 34
 window methods, 34
 worst-case complexity, 15, 16

 Xedni calculus, 334
 XOR, 576
 XTR, 97, 449

 Zariski topology, 72
 zero, 71, 77
 zero isogeny, 146
 zeta function, 207