

Author Index

- Abdalla, M., 494, 497
Adleman, L. M., 28, 341, 343–345
Agnew, G. B., 445
Agrawal, M., 263
Agrell, E., 394
Ajtai, M., 393
Akavia, A., 473
Akishita, T., 220
Alexi, W., 475, 513
Alon, N., 561
Ankeny, N. C., 51
Antipa, A., 486
Araki, K., 584
Arney, J., 297
Arène, C., 196
Atkin, A. O. L., 59, 186, 188
Avanzi, R. M., 241
- Babai, L., 275, 383, 388
Bach, E., 51, 52, 321, 560
Bachem, A., 55
Balasubramanian, R., 584
Banks, W. D., 170
Barreto, P. S. L. M., 579, 580, 587
Bauer, A., 529
Bellare, M., 78, 443, 479, 480, 485, 494, 497, 531, 532, 534, 537
Bellman, R., 243
Bender, E. A., 297
Bentahar, K., 46, 454
Berlekamp, R., 63
Bernstein, D. J., 59, 62, 196, 237, 263, 302, 517, 532, 534
Birkner, P., 196
Bisson, G., 567
Blackburn, S. R., 297
Blake, I. F., 241, 336, 338
Bleichenbacher, D., 410, 485, 490, 516, 526, 530
Blichfeldt, H. F., 361
Block, H., 270
Blum, M., 466, 514
- Blömer, J., 406, 529
Boneh, D., 254, 409, 442, 454, 461, 469, 470, 473, 474, 487, 502, 504, 511, 523, 529, 538, 541, 640
Boppana, R. B., 561
Bos, J. W., 295, 302, 303
Bosma, W., 167
Bostan, A., 556
Bourgain, J., 473
Boyen, X., 487
Boyko, V., 445
Brands, S., 278
Brauer, A., 237
Brent, R. P., 52, 293, 297, 320, 321
Brickell, E. F., 238, 427, 430
Brier, E., 525, 526
Brown, D. R. L., 452, 462, 464, 486, 487
Brumley, B. B., 250
Bröker, R., 190, 553, 570
Burgess, D. A., 51
Burmester, M., 437
- Camion, P., 282
Canetti, R., 79, 443, 475
Canfield, E. R., 324, 331
Cantor, D. G., 64, 214, 217, 220, 229
Carter, G., 199, 295
Cash, D., 453, 497
Cassels, J. W. S., 202, 226, 228
Catalano, D., 522
Chan, W. F., 251
Chao, J., 252
Charlap, L. S., 137, 574
Charles, D. X., 563, 570
Chaum, D., 78, 525
Cheon, J.-H., 295, 462, 464
Cherепnev, M. A., 457
Chor, B., 475, 513
Clavier, C., 525, 526
Cobham, A., 606
Cocks, C., 28
Cohen, H., 187, 241

- Cohen, P., 553
 Coley, R., 574
 Collins, T., 509
 Conway, J. H., 622
 Cook, S., 45
 Coppersmith, D., 280, 337, 339, 388, 397,
 398, 401, 404, 475, 511, 524, 526
 Cornelissen, G., 229
 Coron, J.-S., 404, 445, 512, 517, 524–526,
 531, 532
 Coster, M. J., 431
 Courtois, N., 422
 Couveignes, J.-M., 557, 560
 Couvreur, C., 509
 Cox, D. A., 187, 192, 553, 559
 Cramer, R., 438, 495, 498, 501, 541
 Crandall, R. E., 319

 Damgård, I. B., 51, 77
 Damgård, I. B., 522
 Davenport, H., 234
 Davidoff, G., 561
 Davies, D., 78
 Dawson, E., 199, 295
 De Feo, L., 557
 De Jonge, W., 525
 de Rooij, P., 483
 Deligne, P., 184
 DeMarrais, J., 343–345
 den Boer, B., 454, 455
 Denny, T. F., 337
 Desmedt, Y., 437, 501, 523
 Deuring, M., 187
 Dewaghe, L., 551, 560
 Diem, C., 346, 347, 349, 350
 Diffie, W., 28, 436
 Dimitrov, V. S., 244, 251
 Dipippo, S. A., 232
 Dixon, J., 325
 Doche, C., 245
 Dujella, A., 50, 529
 Durfee, G., 409, 529
 Duursma, I. M., 234, 302, 580

 Eagle, P. N. J., 260
 Edwards, H. M., 196
 Elgamal, T., 438, 483
 Elkies, N. D., 188, 554
 Ellis, J., 28
 Enge, A., 344, 350, 553
 Erdős, P., 324, 331

 Erickson, S., 225
 Eriksson, T., 394
 Euchner, M., 381, 391

 Farashahi, R. R., 196
 Feige, U., 535
 Fiat, A., 535
 Finiasz, M., 422
 Finke, U., 391
 Fischlin, R., 475, 513
 Flajolet, P., 287, 289
 Flassenberg, R., 345
 Floyd, 289
 Flynn, E. V., 202, 226, 228
 Fong, K., 62
 Fontaine, C., 501
 Fouquet, M., 565
 Franklin, M. K., 254, 502, 504, 524
 Freeman, D., 516, 587
 Frey, G., 346, 573, 576, 577, 584
 Friedlander, J., 475
 Fuji-Hara, R., 336, 338
 Fujisaki, E., 537
 Fürer, M., 45

 Galand, F., 501
 Galbraith, S. D., 200, 221, 222, 252, 260,
 308, 317, 318, 530, 560, 567–569,
 580, 586
 Gallant, R. P., 243, 248, 251, 300, 302, 452,
 462, 464, 486
 Gama, N., 393, 423
 Gao, S., 66
 Garay, J. A., 485
 Garefalakis, T., 576
 von zur Gathen, J., 66, 254
 Gaudry, P., 194, 202, 220, 229, 302, 315,
 345, 346, 348, 350
 Gauss, C. F., 365, 366
 Gel'fond, A. O., 273
 Gennaro, R., 522
 Gentry, C., 422, 423, 516, 538
 Giesbrecht, M., 66
 Girault, M., 491, 525
 Goldreich, O., 79, 409, 417, 418, 475, 513,
 516
 Goldwasser, S., 33, 417, 418, 479, 487
 Gong, G., 120
 González Vasco, M. I., 473
 Gordon, D. M., 341, 621
 Gordon, J., 636

- Goren, E. Z., 563
 Granger, R., 120, 579
 Granville, A., 411
 Grieu, F., 526
 Gross, B. H., 192, 563
 Guillou, L. C., 535
 Guy, R. K., 622

 Hafner, J. L., 55, 343
 Halevi, S., 79, 417, 418, 526
 Hankerson, D., 62
 Hanrot, G., 393
 Harley, R., 219, 302, 346
 Harn, L., 120
 Harrison, M., 221, 222
 Hasse, H., 234
 Håstad, J., 398, 399, 468, 522
 Håstad, J., 513
 Havas, G., 55
 van Heijst, E., 78
 Helfrich, B., 391
 Hellman, M. E., 28, 270, 337, 423, 436
 Heneghan, C., 530
 Hess, F., 346, 347, 560, 567, 569, 576, 577,
 579–583, 586
 Hilbert, D., 90
 Hildebrand, A., 331
 Hildebrand, M. V., 297
 Hisil, H., 199
 Hitchcock, Y., 295
 Hoffstein, J., 423, 445
 Hofheinz, D., 541
 Hohenberger, S., 531
 Holmes, M., 318
 Honda, T., 232
 Hong, J., 295
 Hopkins, D., 509
 Horwitz, J., 296
 Howe, E. W., 200, 232
 Howgrave-Graham, N. A., 398, 409, 413,
 414, 423, 424, 472, 489, 522
 Huang, M.-D., 344, 345
 Huang, Z., 251
 Hurwitz, A., 211

 Icart, T., 245, 256
 Igusa, J.-I., 210
 Iijima, T., 252
 Itoh, T., 62

 Jacobson Jr., M. J., 220, 225
 Jacobson, M. J., 251
 Jager, T., 277
 Jao, D., 474, 489, 562, 570
 Järvinen, K. U., 250
 Järvinen, K. U., 251
 Jetchev, D., 474, 475
 Jiang, Z.-T., 469
 Joux, A., 341, 343, 424, 431, 442, 523, 573
 Joye, M., 196, 241, 573
 Jullien, G. A., 244
 Jurik, M. J., 522
 Jutla, C. S., 403, 526

 Kaib, M., 368, 381
 Kaihara, M. E., 295, 303
 van der Kallen, W., 55
 Kampkötter, W., 229
 Kannan, R., 55, 390, 391
 Karatsuba, A. A., 45
 Kasahara, M., 573
 Katagi, M., 220
 Katz, J., 31, 253
 Kayal, N., 263
 Kiltz, E., 453, 497, 516, 541
 Kim, H. Y., 579
 Kim, J. H., 296
 Kim, M., 295
 King, B., 259, 260, 621
 Kitamura, I., 220
 Klein, P. N., 388
 Kleinjung, T., 295, 302
 Knudsen, E. W., 244, 611
 Knuth, D. E., 287
 Koblitz, N., 200, 201, 232, 245, 445, 584
 Kohel, D. R., 120, 245, 258, 551, 562–564,
 566, 567
 Konyagin, S.-V., 473
 Koyama, K., 520
 Kozaki, S., 463
 Kraitchik, M., 325, 334
 Krawczyk, H., 443
 Kuhn, F., 287, 295
 Kuhn, R. M., 228
 Kumar, R., 393
 Kunihiro, N., 520
 Kurosawa, K., 501
 Kutsuma, T., 463

 Labahn, G., 55
 Lagarias, J. C., 395, 428, 430
 Lagrange, J.-L., 365, 366

- Laih, C.-S., 243, 485
 LaMacchia, B. A., 431
 Lambert, R. J., 243, 248, 251, 300, 302, 486
 Lanczos, C., 55, 329, 336
 Lang, S., 187, 553, 559
 Lange, T., 62, 196, 237, 302
 Langford, S., 509
 Lauter, K. E., 553, 563, 570
 Lee, E., 581
 Lee, H.-S., 580, 581
 Lehmer, D. H., 265
 Lehmer, D. N., 265
 Lennon, M. J. J., 116
 Lenstra Jr., H. W., 66, 167, 187, 199, 200, 250, 266, 293, 330, 332, 365, 375, 395, 445, 461
 Lenstra, A. K., 119, 243, 251, 259, 302, 365, 375, 526
 Lercier, R., 341, 343, 556, 557
 Leurent, G., 78
 Li, W.-C., 469, 474
 Lichtenbaum, S., 576
 Lin, X., 252
 Lindell, Y., 31, 253
 Lindner, R., 388, 416
 Lipton, R. J., 454, 461
 Lockhart, P., 210
 Lovorn Bender, R., 337, 338
 Lovász, L., 365, 375, 381, 412
 Lubicz, D., 194, 202
 Lucas, E., 114
 Lynn, B., 579
 Lyubashevsky, V., 424
 Lüneburg, H., 66
 López, J., 62

 M'Raihi, D., 445, 485
 Majewski, B. S., 55
 Martín Molleví, S., 520
 Matsuo, K., 252, 463
 Matthews, K. R., 55
 Mauduit, C., 51
 Maurer, U. M., 332, 454, 457
 May, A., 406, 423, 512, 529, 530
 McCurley, K. S., 55, 341, 343
 McEliece, R., 417
 McKee, J. F., 187, 199, 200, 530
 Meier, W., 247, 248
 Menezes, A. J., 31, 62, 245, 573, 584
 Merkle, R., 28, 77, 423
 Mestre, J.-F., 188, 210, 562, 563
 Micali, S., 33, 466, 487
 Micciancio, D., 55, 393, 414, 419, 479
 Miller, G. L., 512
 Miller, S. D., 296, 562, 570
 Miller, V. S., 258, 351, 575, 579, 620
 Miller, W. C., 244
 Minkowski, 362
 Mireles, D. J., 221, 222
 Misarsky, J.-F., 525
 Miyaji, A., 241
 Monico, C., 303
 Montague, P., 295
 Montenegro, R., 296, 307, 309
 Montgomery, P. L., 52–54, 192, 266, 293, 303
 Morain, F., 60, 238, 302, 556, 557, 560, 565
 Morillo, P., 520
 Muir, J., 241
 Mullin, R. C., 336, 338, 445
 Mumford, D., 213, 214
 Murphy, S., 297
 Murty, M. R., 561
 Murty, R., 200
 Muzereau, A., 454, 461
 Möller, B., 242, 243
 Müller, V., 250

 Naccache, D., 411, 485, 517, 524–526
 Naehrig, M., 196, 587
 Namprempre, C., 534
 Nechaev, V. I., 270, 273, 275
 Neven, G., 480, 482, 534, 573
 Nguyen, P. Q., 78, 355, 365, 368, 381, 393, 410, 421–423, 431, 442, 472, 473, 489, 522, 523
 Nicolas, J.-L., 60
 Niederreiter, H., 63
 Nivasch, G., 293
 Näslund, M., 468, 469, 473, 474, 513

 Odlyzko, A. M., 289, 337, 430, 431, 523
 Oesterlé, J., 563
 Ó hÉigearthaigh, C., 580
 Ohgishi, K., 573
 Okamoto, T., 522, 537, 573, 584, 638
 Olivos, J., 238
 O'Malley, S. W., 445
 Ono, T., 241
 Onyszchuk, I. M., 445

- van Oorschot, P. C., 31, 293, 304, 307, 311, 318, 319
 Orman, H. K., 445
 Oyono, R., 579

 Paillier, P., 482, 487, 519, 521, 532
 Park, C.-M., 581
 Patarin, J., 282, 524
 Patel, S., 468
 Paulus, S., 221, 222, 225, 345
 Peikert, C., 388, 416, 422
 Peinado, M., 445
 Peres, Y., 296
 Peters, C., 196
 Pfitzmann, B., 78
 Pila, J., 229, 332, 461
 Pinch, R. G. E., 529, 530
 Pipher, J., 423
 Pizer, A. K., 561, 563
 Pohst, M., 391
 Pointcheval, D., 443, 479, 480, 482, 484, 487, 537
 Pollard, J. M., 265, 267, 285, 297, 304, 308, 309, 311, 313, 319, 320, 332
 Pomerance, C., 319, 324, 329–332, 337, 338, 461
 van der Poorten, A. J., 220
 Poupard, G., 491
 Price, W. L., 78
 Pujol, X., 393

 Quisquater, J.-J., 509, 535

 Rabin, M. O., 509, 513, 637
 Rabin, T., 485
 Rackoff, C., 328
 Raphaeli, D., 485
 Regev, O., 393, 414, 422, 489
 Reiter, M. K., 524
 Reiter, R., 246
 Reitwiesner, G., 238
 Reyneri, J. M., 337
 Ritter, H., 381
 Ritzenthaler, C., 196
 Rivest, R. L., 28, 33, 293
 Robbins, D. P., 137
 Rogaway, P., 76, 78, 443, 494, 497, 531, 532, 537
 Ron, D., 409
 Roquette, P., 211
 Rosen, A., 516

 Rubin, K., 111, 112, 117
 Ruprai, R. S., 308, 317, 318
 Rück, H.-G., 186, 221, 222, 225, 573, 576, 577, 584, 585

 Sabin, M., 509
 Sakai, R., 573
 Salvy, B., 556
 Sarnak, P., 561
 Satoh, T., 465, 584
 Sattler, J., 296
 Saxena, N., 263
 Scarf, H. E., 381
 Schinzel, A., 255
 Schirokauer, O., 337, 342
 Schmidt-Samoa, K., 242
 Schnorr, C.-P., 293, 296, 368, 380, 381, 391, 395, 431, 445, 475, 477, 480, 490, 513
 Schoof, R., 60, 186–188, 554
 Schost, E., 229, 315, 556
 Schroeppe, R. C., 244, 270, 329, 337, 424, 445
 Schulte-Geers, E., 299
 Schwabe, P., 302
 Schwarz, J. T., 277
 Schwenk, J., 277
 Schönhage, A., 45
 Scott, M., 252, 579, 580, 582, 587
 Sedgewick, R., 287, 293
 Segev, G., 516
 Semaev, I. A., 347, 584
 Semay, O., 242
 Sendrier, N., 422
 Seroussi, G., 241, 260, 611
 Serre, J.-P., 562, 584
 Shallit, J. O., 51, 52, 238
 Shallue, A., 255, 424
 Shamir, A., 28, 243, 424, 428, 430, 491, 510, 534, 535
 Shang, N., 225
 Shanks, D., 220, 273
 Shen, S., 225
 Shioda, T., 210
 Shoup, V., 253, 272, 275, 328, 438, 450, 453, 495, 497, 498, 501, 537, 541, 625
 Shparlinski, I. E., 170, 200, 254, 258, 411, 469, 472–475, 489, 526
 Sidorenko, A., 252
 Silver, R. I., 270

- Silverberg, A., 111, 112, 117
 Silverman, J. H., 351, 423, 445
 Silverman, R. D., 54, 295
 Sinclair, A., 254
 Sirvent, T., 556
 Sivakumar, D., 393
 Skafba, M., 255
 Skinner, C., 116
 Smart, N. P., 27, 241, 343, 346, 454, 461,
 472, 482, 489, 560, 567, 569, 580,
 584
 Smith, B. A., 350
 Smith, P. J., 116
 Solinas, J. A., 241, 244, 246, 248
 Soukharev, V., 570
 Soundararajan, K., 337
 Spatscheck, O., 445
 Staffelbach, O., 247, 248
 Stam, M., 119, 192, 244, 251
 Stapleton, J., 295
 Stark, H. M., 556
 Stehlé, D., 368, 380, 381, 393
 Stein, A., 225, 344
 Stein, J., 48
 Stern, J., 355, 431, 479, 480, 482, 484, 491,
 537
 Stern, J. P., 526
 Stewart, C., 51
 Stichtenoth, H., 211, 230, 231, 234
 Stinson, D. R., 27, 241, 280, 319
 Stolarsky, K. B., 57
 Stolbunov, A., 569
 Storjohann, A., 55
 Strassen, V., 45, 267
 Straus, E. G., 243
 Struik, R., 287, 295, 486
 Sudan, M., 409
 Suk, A. H., 529
 Sundaram, G. S., 468
 Sutherland, A. V., 54, 71, 272, 553, 567
 Suyama, H., 194
 Szemerédi, E., 275
 Szymanski, T. G., 293
 Sárközy, A., 51

 Takagi, T., 220, 242, 510, 522
 Tate, J., 232, 576
 Tenenbaum, G., 331
 Teske, E., 288, 293, 296, 311, 313, 587
 Tetali, P., 296, 307, 309

 Thomé, E., 339, 341, 346, 350
 Thurber, E. G., 237
 Thériault, N., 346, 579
 Tibouchi, M., 524
 van Tilborg, H. C. A., 529
 Toom, A., 45
 Tsujii, S., 62, 252
 Tymen, C., 445

 Uchiyama, S., 522, 638
 Ulas, M., 256

 Vaikuntanathan, V., 422
 Valette, A., 561
 Vallée, B., 365, 368
 Vanstone, S. A., 31, 243, 245, 248, 251, 300,
 302, 336, 338, 445, 486, 573, 584
 Vardy, A., 394
 Vaudenay, S., 27, 485, 487
 Venkatesan, R., 296, 445, 469, 470, 473–475,
 511, 562, 570
 Vercauteren, F., 120, 343, 454, 461, 579–
 582, 586
 Vergnaud, D., 482, 487
 Verheul, E. R., 119, 259, 529, 588
 Vidick, T., 393
 Villar, J. L., 519, 520
 Voloch, J. F., 186, 343
 Voulgaris, P., 393
 Vélu, J., 547

 Wagner, D., 282, 393, 424
 Wang, Y.-M., 469
 Warinschi, B., 55, 482
 Washington, L. C., 188
 Waters, B., 531
 Weber, D., 337
 Weinmann, R.-P., 524
 Weng, A., 210
 Wiedemann, D. H., 55, 329, 336
 Wiener, M. J., 293, 300, 304, 307, 311, 318,
 319, 527, 528
 Williams, H. C., 515, 519
 Williamson, M. J., 436
 Winterhof, A., 473
 van de Woestijne, C. E., 255
 Wolf, S., 332, 454
 Wong, K. K.-H., 199

 Xing, C., 234
 Xu, W.-L., 469

- Yao, A. C.-C., 293
Yen, S.-M., 241, 243, 485
Yoshida, K., 489
- Zassenhaus, H., 64
Zeger, K., 394
Zierler, N., 68
Zimmermann, P., 46, 52
Zuccherato, R. J., 300

Subject Index

- Abel-Jacobi map, 142, 227
- Abelian variety, 226
- absolutely simple, 226
- adaptive chosen message attack, 34
- adaptive chosen-ciphertext attack, 32
- addition chain, 57
- additive group, 85
- additive rho walk, 288
- adjacency matrix, 561
- advantage, 42, 437, 467, 495
- adversary against an identification protocol, 479
- affine n -space over k , 87
- affine algebraic set, 88
- affine coordinate ring, 89
- affine line, 87
- affine plane, 87
- affine variety, 96
- affine Weierstrass equation, 127
- AKS primality test, 263
- algebraic, 593
- algebraic closure, 593
- algebraic group, 83
- algebraic group quotient, 85
- algebraic torus, 111
- algebraically independent, 403
- algorithm, 37
- amplifying, 44
- amplitude, 410
- anomalous binary curves, 185
- anomalous elliptic curves, 584
- approximate CVP problem, 363
- approximate SVP problem, 363
- ascending chain, 597
- ascending isogeny, 563
- asymmetric cryptography, 28
- ate pairing, 580
- attack goals for public key encryption, 31
- attack goals for signatures, 33
- attack model, 31
- automorphism, 170
- auxiliary elliptic curves, 460
- average-case complexity, 40
- B -power smooth, 265
- B -smooth, 265
- Babai nearest plane algorithm, 386
- Babai rounding, 248
- Babai's rounding technique, 388
- baby step, 222
- Barret reduction, 53
- base- a probable prime, 263
- base- a pseudoprime, 263
- basic Boneh-Franklin scheme, 502
- basis matrix, 357
- batch verification of Elgamal signatures, 485
- BDH, 503
- Big O notation, 38
- big Omega, 39
- big Theta, 39
- bilinear Diffie-Hellman problem, 503
- binary Euclidean algorithm, 48
- birational equivalence, 101
- birthday bound, 275
- birthday paradox, 285, 602
- bit i , 601
- bit-length, 601
- black box field, 455
- Blichfeldt Theorem, 361
- block Korkine-Zolotarev, 395
- Blum integer, 514
- Boneh-Joux-Nguyen attack, 442
- bounded distance decoding problem (BDD), 363
- Brandt matrix, 563
- Burmester-Desmedt key exchange, 437
- canonical divisor class, 160
- Cantor reduction step, 217
- Cantor's addition algorithm, 215
- Cantor's algorithm, 214
- Cantor's composition algorithm, 215

- Cantor-Zassenhaus algorithm, 64
- Carmichael lambda function, 262, 508
- Cayley graph, 561
- CCA, CCA1, CCA2, 32
- CDH, 436
- c -expander, 561
- chains of isogenies, 546
- characteristic, 590
- characteristic polynomial, 182, 595
- characteristic polynomial of Frobenius, 183, 231
- Cheon's variant of the DLP, 462
- Chinese remainder theorem, 596
- Chinese remaindering with errors problem, 409
- chord-and-tangent rule, 140
- chosen plaintext attack, 32
- ciphertext, 29
- circle group, 88
- circulant matrix, 423
- classic textbook Elgamal encryption, 438
- clients, 297
- closest vector problem (CVP), 363
- CM method, 188
- co-DDH problem, 586
- coefficient explosion, 373
- cofactor, 259
- collapsing the cycle, 302
- collision, 286, 320
- Collision-resistance, 75
- complement, 228
- complete group law, 196, 197
- complete system of addition laws, 167
- Complex multiplication, 185, 187, 199, 558
- complex multiplication method, 188
- Complexity, 38
- composite residuosity problem, 521
- compositeness witness, 262
- composition and reduction at infinity, 222
- composition of functions, 589
- compositum, 593
- compression function, 77
- compression map, 113, 118
- computational problem, 38
- COMPUTE-LAMBDA, 512
- COMPUTE-PHI, 512
- conditional probability, 601
- conductor, 563, 600
- conjugate, 112
- connected graph, 558
- conorm, 150, 153
- constant function, 98
- continuation, 266
- continued fraction expansion, 48
- convergents, 48
- Coppersmith's theorem, 401
- Cornacchia algorithm, 60
- coupon collector, 602
- covering attack, 347
- covering group, 85, 116, 120
- CPA, 32
- Cramer-Shoup encryption scheme, 498
- crater, 566
- CRT list decoding problem, 409
- CRT private exponents, 509
- cryptographic hash family, 75
- curve, 127
- cycle, 289
- cyclotomic polynomial, 109
- cyclotomic subgroup, 111
- data encapsulation mechanism, 495
- DDH, 437
- de-homogenisation, 94
- decision closest vector problem (DCVP), 363
- decision learning with errors, 415
- decision problem, 38
- decision shortest vector problem, 363
- decision static Diffie-Hellman problem, 452
- Decisional Diffie-Hellman problem (DDH), 436
- decompression map, 113, 118
- decrypt, 29
- decryption algorithm, 31
- decryption oracle, 465
- Dedekind domain, 148
- defined, 99
- defined over \mathbb{k} , 89, 91, 93, 135
- degree, 134, 146, 172, 343, 593
- DEM, 495
- den Boer reduction, 455
- dense, 98, 102
- density, 240
- derivation, 155
- derivative, 591
- descending isogeny, 563
- Desmedt-Odlyzko attack, 523
- determinant, 358, 599
- deterministic algorithm, 38
- deterministic pseudorandom walk, 287

- DHIES, 494
- diameter, 558
- Dickman-de Bruijn function, 324
- Diem's algorithm, 350
- differentials, 158
- Diffie-Hellman tuples, 437
- digit set, 245
- dimension, 105
- Diophantine approximation, 48, 412
- discrete, 357
- discrete logarithm assumption, 435
- discrete logarithm in an interval, 274
- discrete logarithm problem, 38, 269
- discrete valuation, 131
- discriminant, 128, 600
- d -isogeny, 172
- distinguished point, 293
- Distinguished points, 293
- distortion map, 586, 588
- distributed computing, 297
- Distributed rho algorithm, 297
- distribution, 601
- division polynomials, 181
- divisor, 134
- divisor class, 138
- divisor class group, 138
- divisor of a differential, 159
- divisor of a function, 136
- divisor-norm map, 151
- Dixon's random squares, 325
- DL-LSB, 466
- DLP, 38, 269
- DLP in an interval, 274
- DLWE, 415
- dominant, 102
- DSA, 486
- DStatic-DH, 452
- DStatic-DH oracle, 496
- dual isogeny, 176, 177
- dual lattice, 360

- eavesdropper, 436
- ECDSA, 486
- ECIES, 494
- ECM, 267
- edge boundary, 561
- effective, 134
- effective affine divisor, 212
- eigenvalues of a finite graph, 561
- Eisenstein's criteria, 591

- Elgamal encryption, 465
- Elgamal public key signatures, 484
- elliptic curve, 128
- elliptic curve method, 267
- embedding degree, 578
- embedding technique, 390
- encapsulates, 495
- encoding, 276
- encrypt, 28
- encryption algorithm, 30
- encryption scheme, 30
- endomorphism ring, 172
- entropy smoothing, 76
- epact, 290
- ephemeral keys, 436
- equation for a curve, 127
- equivalence class in AGQ, 85
- equivalence classes in Pollard rho, 300
- equivalence of functions, 98
- equivalent, 171, 212, 248
- equivalent computational problems, 43
- equivalent isogenies, 546
- e -th roots problem, 511
- Euclidean norm, 598
- Euler phi function, 590
- Euler's criterion, 50
- Euler-Mascheroni constant, 590
- event, 601
- existential forgery, 33
- expander graph, 561
- expectation, 602
- expected exponential-time, 40
- expected polynomial-time, 40
- expected subexponential-time, 40
- expected value, 287
- explicit Chinese remainder theorem, 54
- explicit representation, 454
- exponent, 590
- exponent representation, 83
- exponential-time, 39
- exponential-time reduction, 43
- extended Euclidean algorithm, 47
- extension, 148, 593
- Extra bits for Rabin, 515

- FACTOR, 512
- factor base, 325, 326
- family of groups, 467
- FDH-RSA, 531
- Feige-Fiat-Shamir protocol, 535

- Fermat test, 262
- Fiat-Shamir transform, 481
- field of fractions, 597
- final exponentiation, 579
- finitely generated, 590, 593, 596
- fixed base, 237, 243
- fixed pattern padding, 406, 524
- Fixed-CDH, 448
- Fixed-Inverse-DH, 449
- Fixed-Square-DH, 449
- floating-point LLL, 380
- floor, 564
- Floyd's cycle finding, 289
- forking lemma, 480
- four-kangaroo algorithm, 309
- free module, 591
- Frobenius expansion, 245
- Frobenius map, 146, 175, 231
- full domain hash, 531
- full rank lattice, 357
- fully homomorphic, 501
- function, 589
- function field, 98
- function field sieve, 341
- fundamental domain, 422
- fundamental parallelepiped, 599
- Galbraith's algorithm, 568
- Galbraith-Hess-Smart algorithm, 569
- Galois, 594
- Galois cohomology, 594
- Galois group, 594
- game, 32
- gap Diffie-Hellman problem, 496
- Garner's algorithm, 54
- Gaudry's algorithm, 345
- Gaussian heuristic, 362
- generic algorithm, 276
- generic chosen-message attack, 487
- genus, 155, 206
- genus 0 curve, 162
- geometric distribution, 602
- geometrically irreducible, 96
- GGH, 417
- GGH encryption, 417
- GGH signatures, 422
- GIMPS, 297
- GLV lattice, 249, 251
- GLV method, l -dimensional, 251
- Goldreich-Goldwasser-Halevi cryptosystem, 417
- Gong-Harn cryptosystem, 120
- Gordon's algorithm, 264, 621
- Gram matrix, 359
- Gram-Schmidt algorithm, 599
- Gram-Schmidt orthogonalisation, 599
- greatest common divisor, 214
- Greedy algorithm, 424
- Group automorphism, 85
- group decision Diffie-Hellman problem, 450
- group defined over \mathbb{k} , 176
- GSO, 599
- Guillou-Quisquater protocol, 535
- Hafner-McCurley algorithm, 343
- half trace, 67
- Hamming weight, 57, 279
- hardcore bit or predicate, 466
- hash Diffie-Hellman (Hash-DH), 497
- Hasse interval, 184
- Håstad attack, 522
- head, 289
- Hensel lifting, 65
- Hermite constant, 361
- Hermite normal form, 600
- hidden number problem, 470, 490
- Hilbert 90, 92, 105, 595
- Hilbert Nullstellensatz, 90
- HNF, 600
- HNP, 470
- homogeneous coordinates, 91
- homogeneous decomposition, 592
- homogeneous ideal, 92
- homogeneous polynomial, 592
- homogenisation, 94, 95
- homogenous coordinate ring, 93
- homomorphic, 502
- homomorphic encryption, 502
- Honda-Tate theory, 232
- horizontal isogeny, 563
- Horner's rule, 61
- Hurwitz class number, 187, 191, 199, 558
- Hurwitz genus formula, 162
- Hurwitz-Roquette theorem, 211
- hybrid encryption, 438, 495
- hyperelliptic curve, 206
- hyperelliptic equation, 201
- hyperelliptic involution, 201
- hyperplane, 88
- hypersurface, 88
- ideal, 89, 596

- identity matrix, 597
- identity-based cryptography, 491, 502
- Igusa invariants, 210
- imaginary hyperelliptic curve, 206
- imaginary quadratic field, 600
- implicit representation, 454
- IND, 32
- IND-CCA security, 32
- independent events, 601
- independent random variables, 602
- independent torsion points, 258
- index calculus, 334
- indistinguishability, 32
- indistinguishability adversary, 32
- inert model of a hyperelliptic curve, 206
- inert place, 206
- inner product, 598
- input size, 38
- inseparable, 146
- inseparable degree, 146
- instance, 38
- instance generator, 41
- interleaving, 243
- invalid parameter attacks, 441
- invariant differential, 178
- inverse limit, 182
- Inverse-DH, 448
- irreducible, 96, 590, 591
- isogenous, 172
- isogeny, 172, 226, 231
- isogeny class, 557
- isogeny problem for elliptic curves, 567
- isomorphic, 102
- isomorphism of elliptic curves, 168
- isomorphism of pointed curves, 168
- iterated Merkle-Hellman, 426
- i -th bit, 601
- Itoh-Tsujii inversion algorithm, 62

- Jacobi quartic model, 199
- Jacobi symbol, 50
- Jacobian matrix, 126
- Jacobian variety, 140, 226
- j -invariant, 169
- joint sparse form, 244

- \mathbb{k} -algebraic set, 88
- kangaroo method, 305
- kangaroo, tame, 305
- kangaroo, wild, 305
- Karatsuba multiplication, 45, 509

- KEM, 495
- kernel, 172
- kernel lattice, 362
- kernel lattice modulo M , 362
- key derivation function, 438
- key encapsulation, 28
- key encapsulation mechanism, 495
- key only attack, 33
- key transport, 28, 495
- keyed hash function, 75
- KeyGen, 30
- known message attack, 33
- Koblitz curves, 185
- Korkine-Zolotarev reduced, 394
- k -regular, 558
- Kronecker substitution, 61
- Kronecker symbol, 50, 559
- Krull dimension, 105
- Kruskal's principle, 307
- Kummer surface, 202

- L -polynomial, 230
- l -sum problem, 282
- ℓ_2 -norm, 598
- ℓ_a -norm, 598
- ladder methods, 116
- Lagrange-Gauss reduced, 366
- large prime variation, 330
- Las Vegas algorithm, 40
- lattice, 357
- lattice basis, 357, 362
- lattice dimension, 357
- lattice membership, 362
- lattice rank, 357
- l -bit string, 601
- learning with errors, 415
- least significant bit, 601
- Legendre symbol, 50
- length, 44, 238
- Length of a Frobenius expansion, 245
- linear change of variables, 93
- linear congruential generator, 439, 479
- linear map, 597
- linearly equivalent, 138
- Little O notation, 39
- LLL algorithm, 375
- LLL reduced, 370
- local, 597
- local properties of varieties, 123
- local ring, 123

- localisation, 123, 597
- loop shortening, 580
- Lovász condition, 370
- low Hamming weight DLP, 279
- low-exponent RSA, 509
- LSB, 601
- LUC, 114, 116, 474
- lunchtime attack, 32, 523
- LWE, 415
- LWE distribution, 414

- MAC, 77
- map, 589
- match, 286
- Maurer's algorithm, 621
- maximal ideal, 131, 596
- McEliece cryptosystem, 417
- McEliece encryption, 417
- mean step size, 304
- meet-in-the-middle attack, 318
- Merkle-Damgård construction, 77
- Mersenne prime, 468
- message authentication code, 77
- message digest, 29
- messages, 436
- Mestre's algorithm, 210
- Miller function, 577
- Miller-Rabin test, 262
- Minkowski convex body theorem, 361
- Minkowski theorem, 362
- mixing time, 296
- $M(n)$, 46
- mod, 589
- model, 104
- model for a curve, 127
- modular curve, 553
- modular exponentiation, 55
- modular polynomial, 553
- modular subset sum problem, 424
- module, 590
- monic, 591
- Monte Carlo algorithm, 40
- Montgomery model, 192
- Montgomery multiplication, 52, 55
- Montgomery reduction, 52
- Montgomery representation, 52
- morphism, 102
- most significant bit, 467, 469
- MOV/FR attack, 584
- MSB, 469

- MTI/A0 protocol, 444
- multi-base representations, 244
- multi-exponentiation, 242
- multidimensional discrete logarithm problem, 278, 315
- multiplicative group, 85
- multiplicative subset, 597
- Multiprime-RSA, 509
- Mumford representation, 213, 214
- Mumford theta divisor, 229

- NAF, 238
- naive Schnorr signatures, 481
- nearly Ramanujan graph, 562
- negligible, 41
- Newton identities, 231
- Newton iteration, 46, 47, 65
- Newton root finding, 46
- NFS, 332, 337
- NIST primes, 53
- Noetherian, 597
- non-adjacent form, 238, 246
- non-singular, 125, 126
- non-uniform complexity, 39
- norm, 111, 112, 153, 593, 595
- norm map, 246
- normal basis, 595
- normalised isogeny, 550
- noticeable, 41
- n -torsion subgroup, 166
- NTRU cryptosystem, 423
- NTRU decryption failures, 423
- NUCOMP, 220
- Nullstellensatz, 133
- number field sieve, 332, 337

- OAEP, 537
- Okamoto-Uchiyama scheme, 522
- $O(n)$, 38
- $\tilde{O}(n)$, 39
- $o(n)$, 39
- one way encryption, 31
- one-way function, 29, 424
- one-way permutation, 29
- optimal extension fields, 62
- optimal normal basis, 62
- optimal pairing, 581
- oracle, 31, 42
- oracle replay attack, 479
- orbit, 85
- order, 131, 159, 590, 600

- ordinary, 189, 233
- original rho walk, 288
- orthogonal, 598
- orthogonal complement, 599
- orthogonal matrix, 598
- orthogonal projection, 384, 599
- orthogonality defect, 360
- orthogonalized parallelepiped, 420
- orthonormal, 598
- output distribution, 41, 438
- output size, 38
- overwhelming, 42
- OWE, 31

- p -subgroup problem, 638
- padding scheme, 30
- Paillier encryption, 521
- pairing, 487
- Pairing groups, 487
- pairing inversion problem, 586
- pairing-friendly curves, 587
- parallel collision search, 318
- parallel computing, 297
- parameterised assumption, 488
- parasitic solutions, 431
- passive attack, 32, 33, 436
- path, 558
- path in a graph, 558
- Pell's equation, 50
- perfect adversary, 32
- perfect algorithm, 40
- perfect field, 594
- perfect oracle, 42
- π -adic expansions, 245
- π -NAF, 246
- place of a function field, 146
- plane curve, 127
- Pohlig-Hellman, 270
- Poincaré reducibility theorem, 226
- point at infinity, 128
- pointed curve, 168
- points at infinity, 206
- pole, 132
- Pollard kangaroo method, discrete logarithms, 303
- Pollard rho algorithm, factoring, 320
- Pollard rho pseudorandom walk, factoring, 320
- Pollard's FFT continuation, 266
- polynomial basis, 595
- polynomial-time, 39
- polynomial-time equivalent, 43
- polynomial-time reduction, 43
- p -rank, 233
- preimage-resistance, 75, 438
- primality certificate, 264
- primality test, 261
- prime, 590
- prime divisor, 214, 343
- prime number theorem, 263
- primitive, 109
- primitive element theorem, 594
- principal divisor, 136
- principal ideal, 596
- private key, 28
- probable prime, 263
- processors, 297
- product discrete logarithm problem, 278
- product tree, 69
- projective algebraic set, 92
- projective closure, 95
- projective hyperelliptic equation, 207
- projective line, 91
- projective plane, 91
- projective space, 91
- projective variety, 96
- pseudoprime, 261
- pseudorandom, 288
- PSS, 532
- public key cryptography, 28
- public key identification scheme, 477
- pullback, 103, 150
- purely inseparable, 593
- pushforward, 151

- q -SDH, 488
- q -strong Diffie-Hellman problem, 488
- quadratic non-residue, 50
- Quadratic reciprocity, 51
- quadratic residue, 50, 595
- quadratic sieve, 329
- quadratic twist, 171, 194, 210
- quotient, 85

- Rabin cryptosystem, 513
- Rabin-Williams cryptosystem, 516
- radical, 596
- Ramanujan graph, 561, 563
- ramification index, 149
- ramified model of a hyperelliptic curve, 206
- ramified place, 206

- random oracle model, 78
- random self-reducible, 43
- random variable, 602
- randomised, 39
- randomised algorithm, 39
- randomised encryption, 30
- randomised padding scheme, 507
- randomness extraction, 257
- rank, 591, 597
- rational, 112
- rational functions, 98
- rational map, 100, 101
- Rational parameterisation, 117
- rational points, 88
- real hyperelliptic curve, 206
- real or random security, 444
- reduced, 218, 222
- reduced divisor, 220
- reduced Tate-Lichtenbaum pairing, 578
- reducible, 96
- reduction, 43
- redundancy in message for Rabin, 514
- regular, 99, 100
- regulator, 225
- relation, 325
- reliable, 42
- reliable oracle, 44
- repeat, 286
- representation problem, 278
- residue degree, 148
- Residue number arithmetic, 46
- restriction, 148
- resultant, 592
- rewinding attack, 479
- rho algorithm, discrete logarithms, 287
- rho graph, 296
- rho walks, 288
- Riemann hypothesis for elliptic curves, 184
- Riemann zeta function, 291
- Riemann-Roch space, 154
- ring class field, 187
- ring of integers, 600
- Rivest, R. L., 487
- Robin Hood, 318
- root of unity, 109
- RSA, 507
- RSA for paranoids, 510
- RSA problem, 511
- RSA-PRIVATE-KEY, 512
- SAEP, 538
- safe prime, 259, 264, 508
- Sakurai, K., 522
- Sato-Tate distribution, 200
- Schnorr identification scheme, 478
- Schnorr signature scheme, 480
- Schönhage-Strassen multiplication, 45
- second stage, 266
- second-preimage-resistance, 75
- security parameter, 30, 41
- security properties, 31
- selective forgery, 33
- self-corrector, 44
- Selfridge-Miller-Rabin test, 262
- semantic security, 31
- semi-reduced divisor, 212
- semi-textbook Elgamal encryption, 438
- separable, 146, 172, 593
- separable degree, 146
- separating element, 156
- separating variable, 156
- Serial computing, 297
- server, 297
- session key, 436
- set of RSA moduli, 511
- SETI, 297
- short Weierstrass form, 128
- shortest vector problem (SVP), 362
- sieving, 329
- signature forgery, 34
- signature scheme, 33
- simple, 226
- simple zero, 131
- simultaneous Diophantine approximation, 428
- simultaneous Diophantine approximation problem, 412
- simultaneous modular inversion, 53
- simultaneous multiple exponentiation, 242
- simultaneously hard bits, 468
- singular, 125
- singular point, 126
- sliding window methods, 56
- small private exponent RSA, 527
- small public RSA exponent, 509
- small subgroup attacks, 441
- smooth, 125, 330, 344
- smooth divisor, 343
- Smooth integers, 265
- smooth polynomial, 337
- SNFS, 342
- snowball algorithm, 71

- Soft O notation, 39
- Solinas, J. A., 247
- Sophie-Germain prime, 259, 264, 508
- sparse matrix, 55, 329
- special q -descent, 339
- special function field sieve, 342
- special number field sieve, 332, 342
- split an integer, 63
- split Jacobian, 227
- split model of a hyperelliptic curve, 206
- split place, 206
- splits, 261
- splitting system, 280
- SQRT-MOD-N, 517
- square, 595
- square-and-multiply, 55
- Square-DH, 448
- square-free, 63
- SSL, 28
- Standard continuation, 266
- standard model, 78
- Stark's algorithm, 556
- static Diffie-Hellman key exchange, 438
- static Diffie-Hellman problem, 452
- Static-DH oracle, 465
- statistical distance, 603
- statistically close, 603
- Stirling's approximation to the factorial, 601
- Stolarsky conjecture, 57
- strong Diffie-Hellman (Strong-DH), 496
- strong forgery, 34
- strong prime, 264, 508
- strong prime test, 262
- STRONG-RSA, 513
- strongly B -smooth, 265
- subexponential, 324
- subexponential function, 324
- subexponential-time, 39
- subexponential-time reduction, 43
- subgroup generated by g , 590
- sublattice, 357
- subvariety, 96
- succeeds, 42
- success probability, 42
- successful adversary, 32, 437
- successive minima, 360
- summation polynomials, 347
- superpolynomial-time, 39
- supersingular, 185, 189, 233
- support, 134
- surface, 564
- system parameters, 439, 477
- tail, 289
- Takagi-RSA, 510
- target message forgery, 33
- target-collision-resistant, 76
- Tate isogeny theorem, 179, 557, 560
- Tate module, 182
- Tate's isogeny theorem, 232
- Tate-Lichtenbaum pairing, 576
- tau-adic expansions, 245
- tensor product, 591
- textbook Elgamal public key encryption, 438
- textbook RSA, 28
- three-kangaroo algorithm, 308
- tight security reduction, 532
- TLS, 28
- Tonelli-Shanks algorithm, 58
- Toom-Cook multiplication, 45
- tori, 474
- torsion-free module, 174
- torus based cryptography, 109, 112
- total break, 31, 33
- total degree, 591
- total variation, 603
- trace, 85, 114, 183, 593, 595
- trace based cryptography, 109
- trace of Frobenius, 183
- trace polynomial, 64
- transcendence basis, 593
- transcendence degree, 593
- transcendental, 593
- translation, 124
- transpose, 597
- trapdoor, 29
- trapdoor one-way permutation, 29
- trial division, 261
- trivial twist, 171
- tunable balancing of RSA, 510
- twist, 171
- twisted Edwards model, 196
- UF, 33
- UF-CMA, 34
- Unified elliptic curve addition, 166
- uniform complexity, 39
- uniform distribution, 601
- uniformizer, 129
- uniformizing parameter, 129
- unimodular matrix, 358, 600

- unique factorisation domain, 590
- unramified, 149, 173
- unreliable, 42
- unreliable oracle, 44
- useless cycles, 302

- valuation ring, 131
- value, 99
- value of a function, 99
- variable base, 237, 243
- Verschiebung, 177
- vertex boundary, 561
- volcano, 565
- volume, 358
- Vélu's formulae, 547

- Wagner algorithm, 393
- weak chosen-message attack, 487
- Weierstrass equation, 127
- weight, 240
- Weight of a Frobenius expansion, 245
- weighted projective hyperelliptic equation, 204
- weighted projective space, 96, 204
- weights, 424
- Weil bounds, 231
- Weil descent, 346
- Weil pairing, 258, 574
- Weil reciprocity, 573
- Weil restriction of scalars, 106, 111
- width- w non-adjacent form, 241
- Wiener attack, 527
- Williams, 515
- Williams integer, 515, 532
- window length, 56
- window methods, 56
- worst-case complexity, 39, 40

- Xedni calculus, 351
- XOR, 601
- XTR, 119, 474
- XTR cryptosystem, 120
- XTR representation, 119

- Zariski topology, 93
- zero, 92, 99
- zero isogeny, 172
- zeta function, 230