
Index

- $(t + 1)$ -reconstruction, 236
- (t, n) -threshold, 260
- (t, n) -threshold black box secret sharing, 288
- (t, n) -threshold black box secret sharing scheme, 290, 291
- L -polynomial, 332
- \circ , 26
- \circ , 23
- n -out-of- n secret-sharing scheme, 237
- p th cyclotomic number field, 223
- p th ring of cyclotomic integers, 223
- r -reconstruction, 258
- r -wise determined, 302
- t -disconnected, 304
- (Ihara) limit, 335
- 0-disconnected, 304

- abelian group, 204
- Abhyankar's Lemma, 340
- access structure, 142, 258
- activation, 25, 56
- activation driven, 26
- activation port, 24, 56
- activation token, 26, 56
- active, 60, 249
- active adversary, 82
- active corruption, 66, 72
- active secure, 82
- actual influence, 54
- adaptive adversary, 79
- adaptive corruption, 79
- adaptively secure, 79
- admissible, 283
- admissible pair, 295
- admissible pairs, 294
- admissible sets, 283
- advantage, 18–20, 68
- adversarially chosen output round, 90, 105
- adversary structure, 140, 142, 258
- algebraic, 216
- algebraic closure, 217
- algebraic function field, 327
- algebraic number field, 220
- algebraically closed, 217
- algebraically independent, 217

- algorithm, 16
- allowed influence, 54
- allowed values, 51
- alphabet, 237, 253
- alternating forms, 309
- antimonotone, 140
- antimonotone structure, 259
- arithmetic circuit, 36
- arithmetic codex, 299
- arithmetic embedding, 305
- arithmetic secret-sharing scheme, 305
- assign, 15
- associativity, 204
- at least as secure as, 58, 69, 76
- auction, 4
- automorphism, 204
- average encoding length, 256
- average length of the shares, 258

- basis, 211
- Bertrand's Postulate, 294
- bilinear map, 210
- bilinear multiplication algorithm, 313
- bilinear multiplication complexity, 306
- black box secret sharing, 288, 290
- black box secret sharing (eq. def.), 291
- black box secret-sharing schemes, 282
- Brickell's vector space construction, 260
- broadcast, 85
- Byzantine, 52
- Byzantine agreement, 85

- called, 60
- calling, 60
- canonical divisor, 331
- canonical morphism, 212
- cardinality of admissible pair, 295
- challenge bit, 240
- challenger, 240
- characteristic, 208
- characteristic polynomial, 224
- circuit, 36
- class number, 221, 329
- class of environments, 73

370

clock preserving, 67, 83
 clock synchronization, 84
 clock-driven execution, 59
 clock-in phase, 83
 clock-out phase, 83
 clocked, 60
 clocked entity, 59
 closed, 26
 closed system, 67
 closure, 27
 code, 238
 codeword, 238
 codex, 299, 305
 commutative, 204, 206
 compatible, 26
 complement, 237
 complete breakdown, 88, 86, 92
 composability, 30
 composed party, 71
 composed protocol, 71
 composing, 58
 composition, 26
 compositum, 208
 computation vertex, 269
 computational, 69
 computational ordering, 36
 computational security, 82
 computationally indistinguishable, 22
 computationally unbounded adversary, 82
 conditional entropy, 256
 conjugates, 218
 connected, 260
 connected monotone structure, 259
 consensus broadcast, 85
 contraction, 274
 coordinate vector, 237
 coprime, 215
 corrupted share vector, 251
 corruption preserving, 66, 79, 80, 82
 M additivity, 15
 current state, 24
 cyclic, 205

decryption algorithm, 31
 Dedekind Different Theorem, 337
 Dedekind domain, 220
 degenerate, 211
 degree, 212
 degree of divisor, 329
 degree of the place, 328
 determinant, 224
 differ from 0, 226
 different, 337, 338
 dimension, 211
 direct limit, 217
 direct sum, 214
 disconnection, 304

Index

disconnection with uniformity, 304
 discrete valuation, 328
 discriminant, 226, 227
 disjoint random variables, 17
 distinguisher, 17, 240
 distinguishing advantage, 18
 distributivity, 206
 divides, 207
 divisor class group, 329
 divisor of, 329
 divisors, 329
 domain, 207, 259
 dual, 210, 259
 dual access structure, 146
 dual of linear code, 262

effective divisor, 329
 embedding, 217
 encryption algorithm, 31
 endomorphism, 204
 entrywise multiplication, 14
 environment, 29, 67
 environment class, 76
 error-correcting codes, 121
 Euclidean algorithm, 217
 evaluation at place, 328
 evaluation map, 242
 event, 15, 253
 event space, 15
 exceptional units, 287
 executable, 26, 27
 expansion factor, 292
 extension, 306
 extension field, 212
 extension ring, 206

factorial, 207
 family of random variables, 20
 field, 208
 field of fractions, 208
 final return port, 26
 finite field, 208
 finite probability space, 253
 forward security, 64
 fractional ideal, 221
 Franklin-Yung's variation, 313
 free R -module, 211
 free abelian group, 214
 Frobenius automorphism, 219
 Frobenius map, 300
 full field of constants, 327
 Fundamental Identity, 222, 335

Galois correspondence, 219
 Galois extension, 218
 Galois group, 218

- Gaussian integers, 220
- general adversary, 271
- generalized linear secret-sharing scheme, 268
- generator, 205
- genus, 331, 335
- global transcript, 193
- group, 204
- guess, 29
- guessing bit, 240

- Hamming distance, 249
- Hamming sphere, 250
- Hamming weight, 249
- Hasse-Weil Theorem, 333
- Hasse-Witt invariant, 351
- Hurwitz Genus Formula, 338
- hyperinvertible, 165

- ideal, 206
- ideal class group, 221
- ideal functionality, 57, 62
- ideal functionality ports, 66
- ideal internal state, 63, 86
- ideal secret-sharing scheme, 260
- ideal threshold secret-sharing scheme, 260
- ideal world, 54
- image, 212
- inactive, 60
- IND-CCA secure, 31
- IND-CPA secure, 31
- independent, 254
- index set, 237, 255
- indexed, 237
- indistinguishability, 21
- indistinguishable, 29
- Indistinguishable Interactive Systems, 29
- infinite place, 332
- influence, 52
- influence port, 58, 62
- initial activation port, 26
- inner product, 14
- inport, 24, 56
- input deprivation, 85, 89
- input substitution, 54
- input vertices, 269
- instance, 191
- integral, 220
- integral closure, 220
- intended functionality, 57
- interactive agent, 24, 56, 62
- interactive system, 24, 26, 56
- interpolation code, 238
- inverse, 204
- inward clocked, 83
- irreducible, 207
- isomorphism, 204

- kernel, 14, 212
- key generator, 31
- key-registration model, 162
- Kummer's Theorem, 336

- labeling function, 141
- Lagrange interpolation, 33
- Latin square, 277
- law of composition, 204
- leakage port, 58, 62
- leaked values, 51
- length of the secret, 258
- lies above, 335
- limit of tower, 335
- linear code, 244
- linear maps, 210
- linear representation, 164, 167
- linearly equivalent divisors, 330
- local ring, 209
- local view, 193
- localization of A at P , 209

- market-clearing price, 183
- matrix multiplication, 14
- matrix transpose, 14
- maximal ideal, 207
- maximal order, 222
- maximum-distance separable, 276
- maximum-distance separable codes, 275
- maximum-likelihood distinguisher, 20
- MDS code, 165, 275, 276
- metric, 249
- minimal polynomial, 216
- minimial set, 259
- minimum distance, 249
- modularity, 30
- module, 209
- monic, 216
- monoid, 204
- monotone, 270
- monotone Boolean formulas, 269
- monotone span programs, 268
- monotone structure, 259
- morphism, 204, 210, 224
- morphism of groups, 205
- morphism of rings, 206
- MPC in the head, 182
- mult, 106
- multiplication-by- α map, 224
- multiplicative, 144, 226
- multiplicativity, 328

- negligible, 21
- negligible in, 21
- negotiation phase, 83
- neutral element, 204

372

nilpotent, 207
 nilradical, 207
 Noetherian, 207, 210
 noncommitting encryption, 81, 160
 nondegenerate, 210
 norm, 219
 normal, 212
 normal closure, 219
 normal field extension, 218
 nullideal, 206

 open inport, 56
 open output, 56
 open ports, 26
 order, 222
 orthogonal, 277
 orthogonal arrays, 238
 output, 24, 56
 output vertex, 269
 outward clocked, 83

 party, 72
 passive, 249
 passive adversary, 82
 passive corruption, 66, 72
 passively secure, 82
 perfect, 69
 perfect correctness, 47
 perfect field, 218
 perfect privacy, 47
 perfect secret-sharing, 260
 perfect secure implementation, 78
 perfect security, 82
 perfectly indistinguishable, 21, 29
 Picard group, 329
 place, 327
 player set, 257, 268
 players hold, 38, 149
 pole, 328
 pole divisor, 329
 polynomial evaluation code, 244, 312
 polyresponsive, 25, 28
 polytime, 25, 28
 polytime adversary, 82
 port, 56
 port compatible, 26
 power basis, 216
 preamble, 80
 prime, 207
 prime ideal, 207
 primitive, 298
 principal divisors, 329
 principal fractional ideal, 221
 principal ideal domain, 207
 principal ideals, 206
 privacy set for, 257
 private, 51, 82

Index

probability, 15, 253
 probability distribution of, 254
 probability function, 253
 probability measure, 15
 probability space, 15
 product of ideals, 206
 product of random variables, 254
 projection function, 237
 protocol, 71
 protocol name, 64, 71
 protocol ports, 62, 64, 67
 protocol using resource, 64
 public-key cryptosystem, 30
 puncturing, 239

 Q2, 140
 Q3, 140
 qualified, 142
 quotient group, 212
 quotient ring, 213

 ramification index, 336
 ramifies, 222, 336
 ramp schemes, 241
 random self-reduction, 188
 random variable, 15, 253
 range, 15
 rank, 211, 310
 rational places, 328
 recombination vector, 33, 35, 39, 47, 142, 144, 315
 reconstructing set for, 256
 recursive polytime, 62, 76
 regular, 261
 regular matrices, 165
 relative degree, 336
 replicated secret sharing, 145
 residue class field, 328
 resource, 57
 resource name, 64, 71
 resource ports, 64
 responsive, 25, 28
 return port, 24, 56
 returned the call, 60
 Riemann Hypothesis for Function Fields, 333
 Riemann's Inequality, 331
 Riemann–Roch space, 330
 Riemann–Roch Theorem, 331
 ring of integers, 220
 robust, 51, 54, 82
 round, 83
 rushing, 86, 88, 106

 sample space, 15, 253
 Schur product, 14
 secret, 257
 secret sharing, 7

- secret sharing scheme, 32
- secret-sharing scheme, 257
- secure addition, 8
- secure multiplication, 10
- secure synchronous function evaluation, 87
- securely implements, 58, 68, 76
- separable field extension, 218
- Shamir's secret-sharing scheme, 313
- share, 33, 236, 257
- share space, 257
- shortening, 239, 274
- simple, 215
- simple party, 64
- simple protocol, 64
- simulated values, 52
- simulation paradigm, 38
- simulation ports, 66
- simulator, 40, 52, 58, 66, 72
- simultaneous input, 89
- simultaneous output, 89, 105
- special port, 62, 64
- special ports, 62, 64, 67
- splits completely, 336
- splitting locus, 339
- splitting rate, 335
- standard corruption behavior, 63, 65
- static adversary, 79
- static corruption, 79
- statically secure, 79
- statistical, 69
- statistical distance, 16
- statistically indistinguishable, 21, 29
- stepwise polytime, 25
- Strong Approximation Theorem, 330
- strong multiplication, 313
- strong triangle inequality, 328
- strongly multiplicative, 144
- subfield, 208
- subgroup, 204
- submodule, 209
- submonoid, 204
- subring, 206
- sum of ideals, 206
- support, 15, 255, 329
- symmetric forms, 309
- symmetric tensors, 309
- synchronous communication, 84
- synchronous environment, 83
- synchronous protocol, 84
- tame extension, 336
- tame tower, 336
- tamely ramifies at, 336
- target ciphertext, 31
- tensor, 230
- tensor product, 229
- tensor rank, 309
- threshold, 79
- threshold gap, 280
- threshold security, 79
- tower, 335
- trace, 219, 224
- trace function, 224
- transcendence basis, 217
- transcendence degree, 217
- transcendental, 216
- transcript, 48
- transfer, 106
- transition algorithm, 24
- transition phase, 83
- transpose, 238
- triangle inequality, 249, 328
- trivial ring, 206
- UC model, 51
- UC theorem, 59
- unconditional security, 82
- uniform distribution, 15, 254
- uniformity, 305
- uniformizer, 327
- unit, 206
- unital, 303, 305
- universal composition theorem, 59
- unqualified, 142
- unramified, 222, 336
- valuation ring, 327
- Vandermonde matrix, 247
- vector of random variables, 255
- vector space, 210
- vector space morphisms, 210
- view, 48
- Weak Approximation Theorem, 330
- wild extension, 336
- wild tower, 336
- wildly ramifies at, 336
- witness, 191
- word, 238
- zero divisor, 329
- zeta function, 332