Index

Adaptive chosen ciphertext attack, 166
Advanced Encryption Standard, 104
AES, 104
Affine map, 14, 95
AKE, 187
Algebraic degree, 14
Algebraic normal form, 13
Algorithm, 9
AND, 9
Authenticated encryption scheme, 158
Average-case complexity, 17

Babai's rounding method, 259
Babystep-Giantstep, 192
BB84 protocol, 248
Bell state, 235
Big-O, 16
Bijective, 10
Binomial coefficient, 15
Binomial distribution, 23
Birthday paradox, 25
Bit permutation, 16
Bloch sphere, 231
Block cipher, 52
Block code, 287
Blockchain, 140
Boolean function, 13

Caesar cipher, 34
Canonical verification, 152
Cardinality, 7
CBC MAC, 154
CBC mode, 53
CCA, 38
CCA-secure, 45, 177
CCA1-secure, 45
CCA2-secure, 45, 158, 166, 196–199, 307, 308
CDH problem, 189
Ceiling function, 11
CFB mode, 118
ChaCha, 133
Characteristic of a field, 83
Chinese Remainder Theorem, 80, 173
Chosen ciphertext attack, 38, 166
Chosen message attack, 152, 204
Chosen plaintext attack, 38, 165
CMAC, 155
CNOT gate, 236
Code, 287
Codeword, 287
Codomain, 8
Collision, 137
Combination generator, 126
Compression function, 137, 140
Computational security, 36
Conditional probability, 21
Congruences, 65
Connection polynomial, 121
Convolution product, 271

Coset, 290
Coset leader, 290
Countable set, 11
Covolume, 256
CPA, 38
CPA-secure, 42, 43, 55, 57, 165, 195, 197, 198, 279
CPRNG, 46
Cryptocurrency, 140
Cryptosystem, 32
CSPRNG, 46
CTR mode, 54
Cumulative distribution function, 21
CVP, 258
Cyclic group, 77

Davies-Meyer construction, 141
DDH problem, 189
Decision problem, 17
Degree of a field extension, 82
Degree of a polynomial, 83
Derivative, 85
Deutsch-Josza algorithm, 240
DFT, 241
DHIES, 198
Diffie-Hellman, 188, 190, 223
Digital signature, 204
Discrete Fourier Transform, 241
Discrete Gaussian, 276
Discrete logarithm, 189
Discriminant, 216
DL problem, 189
Domain, 8
DSA, 211
DSS, 211

EAV-secure, 40, 187
ECB mode, 53
ECC, 213
ECDH, 223
ECDSA, 228
ECIES, 199
ECM, 225
ElGamal encryption, 202
ElGamal signature, 211
Elliptic curve, 217
Elliptic curve cryptography, 213
Encryption scheme, 32
Enigma machine, 35
Equivalence relation, 12
Euclidean Algorithm, 63, 85
EUF-CMA secure, 152, 204
Euler's phi function, 67
Euler's Theorem, 76
Event, 19
Existential forgery, 206
Expectation, 21
Experiment, 38
Extended Euclidean Algorithm, 63, 85

Factor ring, 86
Factorial, 15
Factoring, 177
Factoring assumption, 168
Fast exponentiation, 67
Feedback polynomial, 121
Feistel network, 102
Fermat factorization, 178
Fermat's Little Theorem, 76
Field, 82
Field extension, 82
Filter generator, 126
Floor function, 11
Floyd's cycle finding algorithm, 26
Formal derivative, 85
Function, 8

Galois Field, 88
Galois field, 83
Game, 38
Gap-CDH problem, 197
Gaussian heuristic, 259
GCM mode, 159
Geometric distribution, 20
GGH cryptosystem, 269
Gilbert-Varshamov bound, 293
Goppa code, 296
Gram-Schmidt orthogonalization, 262
Greatest common divisor, 63, 85
Group, 73
Grover's algorithm, 248
GSO, 262

Hadamard gate, 232
Hamming bound, 293
Hamming distance, 287
Hard problem, 17

Hash function, 137
Hermite normal form, 261
HMAC, 156
HNF, 261
Homomorphism, 74, 81
Hybrid encryption, 197

Ideal cipher model, 142
Image, 8
IND, 37
IND-CCA1, 45
IND-CCA2, 45, 158, 166, 177, 196–199, 307, 308
IND-CPA, 42, 43, 55, 57, 165, 195, 197, 198, 279
IND-EAV, 40
Independent, 20, 22
Index-Calculus algorithm, 194
Indistinguishability, 37
Information rate, 287
Information-set decoding, 305
Injective, 10
Integers, 61
Inverse map, 10
Irreducible, 87
Isomorphism, 74, 81

Kannan's embedding technqiue, 280
Keccak, 148
KEM, 194
Kerberos, 186
Kerkhoff's principle, 33
Kernel, 75
Ket notation, 230
Key distribution, 186
Key encapsulation mechanism, 194
KMAC, 157
KSA, 128

Lattice, 254
Learning with errors, 277
LFSR, 119
Linear code, 287
Linear Feedback Shift Register, 119
Linear map, 14, 93
Linear recurring sequence, 119
LLL algorithm, 265
LLL-reduced basis, 265
Lovacz condition, 265
LWE, 277

MAC, 152
Malleable, 45, 58
Man-in-the-Middle attack, 190
Matrix, 93
Maximum-likelihood decoding, 288
McEliece cryptosystem, 304
MDS code, 291
Merkle tree, 140
Merkle-Damgård, 141
Mersenne prime, 63
Message authentication code, 152
Metric, 287
Miller-Rabin test, 171
Minkowski Theorem, 258

Nearest-codeword decoding, 288
Negligible, 18
Next-bit test, 46
Niederreiter cryptosystem, 308
NMAC, 156
Nonce, 55
Nonsingular, 216
NTRU cryptosystem, 272
Number field sieve, 180, 194

OAEP, 175
OFB mode, 117
One-time pad, 34
One-way permutation, 166, 190
Operation mode, 53, 117
Order, 76
Order of a polynomial, 124
Orthogonal, 94
Orthogonality defect, 262

Parity-check matrix, 289
Patterson algorithm, 299
Pauli-X gate, 232
Pauli-Y gate, 233
Pauli-Z gate, 233
Perfect code, 293
Perfect secrecy, 35
Period, 120
Permutation, 15
PFS, 187
Phase gate, 233
Pointcheval's conversion, 307

Pollard's $p-1$ method, 180
Pollard's rho algorithm, 26, 178, 193
Polynomial growth, 17
Polynomial ring, 83
Preimage, 8
Preimage resistance, 138
PRF, 49
PRG, 46
PRGA, 129
Prime number, 62
Primitive polynomial, 124
Primitive root, 79
Probability distribution, 19
Probability mass function, 21
Probability space, 19
Proof by reduction, 48, 57
Pseudorandom function, 49
Pseudorandom generator, 46
Pseudorandom permutation, 50
Public-key encryption, 164

q-ary lattice, 257
QFT, 242
QKD, 248
Quadratic sieve, 179
Quantum bit, 230
Quantum computing, 230
Quantum Fourier Transform, 242
Quantum gate, 232
Quantum key distribution, 248
Qubit, 230
Quotient ring, 86
Quotient set, 12

Random bit generator, 24
Random oracle model, 138
Random variable, 21
Range, 8
RC4, 128
Related-key attacks, 51
Relation, 11
Residue classes, 12, 65, 86
Ring, 81
Ring-LWE, 281
RKA, 51
Rounding function, 11
RSA, 166, 206
RSA assumption, 169
RSA-FDH, 207
RSA-OAEP, 175
RSA-PSS, 207

Safe prime, 191
SageMath, 1
Salsa20, 130
Self-synchronizing stream cipher, 117
Set, 7
SHA-1, 142
SHA-2, 145
SHA-3, 148
Shor's algorithm, 243
Signature, 204
Singular point, 216
SIVP, 258
Size, 18
Size-reduced basis, 264
Smooth curve, 216
Soft-O notation, 19
Sphere-covering bound, 292
Sphere-packing bound, 293
Sponge construction, 148
Square-and-multiply, 68
Stream cipher, 116
Strong primes, 181
Strong pseudorandom permutation, 50
Subgroup, 75
Substitution-permutation network, 102
Surjective, 10
SVP, 258
Symmetric-key encryption, 33
Synchronous stream cipher, 116
Syndrome, 289

Toffoli gate, 238
Transposition cipher, 34
Trapdoor permutation, 166

Unary string, 18
Uniform distribution, 20
Unitary, 94
Units, 67

Variance, 21
Vector space, 92
Vigenère cipher, 34
Von Neumann extractor, 24

Walsh-Hadamard, 237
Weierstrass equation, 214
Worst-case complexity, 17

XOR, 9