Index

adjoint operator, 792, 1040
admissible variable change, 318
AES, 41
affine line, 171
affine plane, 174
affine space, 163
affine transformation, 198
avalanche effect, 41

B-number, 123
baby step, 95, 659
baby step, giant step, 545
baby steps, 545
baby-step giant-step, 95
baby-step, giant-step, 656
base point, 277
basis state, 726
beamsplitter, 754
Bell qubit, 745
bilinear, 1009, 1033
birational equivalence, 243
Boolean function, 772
bra notation, 795

Caesar chiffre, 23
Carmichael number, 113
Cauchy sequence, 1020
character
  quadratic, 553
characteristic polynomial
    Frobenius, 529
Chinese remainder theorem, 920
chosen plaintext attack, 79
circle, 260
completeness, 1021
complex conjugate, 1010
complex conjugation, 1010
complex number
  absolute value, 726
  length, 1010
complex numbers, 944
conic, 213
continued fraction, 903
continued fraction expansion, 138
convergence, 1020
convergent, 142, 911
cubic, 215
curve
  rational, 240
cusp, 330
cycle detection, 670
cyclic group, 918
decryption key, 69
degree
  point, 568
dehomogenization, 181
DES
  decryption, 40
  encryption, 40
  f-function, 33
  security, 41
  subkey, 37
Deutsch algorithm, 830
Deutsch-Jozsa algorithm, 835
discrete logarithm, 82
Diffie-Hellman, 85
Diffie-Hellman assumption, 87
discrete logarithm, 625, 690
discriminant, 291, 298
divisor, 469
  degree, 470
  function, 474, 479
  order, 475
  principle, 479
  sum, 470
double point, 330
E-gate, 871
ElGamal cryptosystem, 90
elliptic curve, 278
  isomorphic, 320
encryption key, 69
endomorphism, 400
  degree, 406
  Frobenius, 414
  separable, 407
  trivial, 400
Euclidean algorithm, 897
  extended, 900
Euclidean norm, 1019
Euler function, 921
Euler identity, 454
Euler’s rule, 905
Euler’s theorem, 924
exponential gate, 871
F-gate, 778
factor basis, 123
fast modular exponentiation, 926
Fermat’s little theorem, 925
field
   perfect, 418
fingerprint, 49
flex, 259
Floyd’s algorithm, 672
Fourier transform, 778
Freshman’s dream, 415
Frey curve, 307
Frobenius endomorphism, 414
iterate, 515
Frobenius map, 415
r-th iterate, 423
Frobenius trace, 529
general linear group, 201
giant step, 95, 659
giant steps, 545
Goldwasser-Kilian primality test, 706
Gram-Schmidt orthonormalization, 1032
group order, 544
Grover algorithm, 843
Grover’s diffusion operator, 849
H-gate, 753
Hadamard function, 768
Hadamard gate, 753
hash function, 51
Hilbert basis, 1030
Hilbert space, 1021
homogenization, 179
Horner scheme, 385, 927
Householder reflection, 848
I-gate, 748
imaginary unit, 944
index calculus, 690
inner product, 1008
inner product space, 1008
intersection multiplicity, 250
j-invariant, 313
Jacobi symbol, 939
ket notation, 726
key exchange, 85
Kronecker delta, 795
Kronecker product, 759
Kurzsignalheft, 26
least absolute residue, 123
Legendre symbol, 931
Lenstra’s method, 713
linear functional, 1024, 1028
   bounded, 1028
norm, 1028
linear span, 1030
Losing, 27
Massey-Omura, 88
measurement, 794
   partial, 802
qubit, 790
Miller-Rabin primality test, 116, 117
monocyclic permutation, 23
multi-qubit, 735
n-qubit, 735
   entangled, 743
   indirectly separable, 743
   inseparable, 743
   separable, 743
n-torsion subgroup, 434
Newton’s 2nd law, 999
nine point lemma, 364
node, 330
non-cyclic permutation, 23
nonresidue, 930
nonsquare, 930
norm, 1014
normal basis, 581
normed space, 1014
not gate, 749
number field sieve, 154
one-way function, 52
order, 541
   element, 917
   group, 916
order of zero, 251
orthogonal complement, 1022
orthogonality, 1022
orthonormal system, 1030
P-gate, 752
p-norm, 1019
padding, 78
parallelogram law, 1018
permutation, 741
phase gate, 752
phase shifter, 757
plane affine curve, 212
plane projective curve, 211
Playfair cipher, 25
Pocklington primality test, 703
Pohlig-Hellman, 98
point at infinity, 166, 174
pole, 475
Pollard’s p-1 method, 710
Pollard’s rho method, 662
primality testing, 698, 699
prime number theorem, 928
private key, 43
probability, 726
probability amplitude, 726
projective curve
  non-singular, 228
  singular, 227
projective line, 171, 188, 213
projective linear group, 201
projective plane, 174
projective space, 163
projective transformation, 201
pseudoprime, 110
  strong, 114
public key, 43
quadratic residue, 930
quadratic sieve, 154
quantum algorithm, 821
quantum gate, 1044
qubit, 725, 726, 728
  pure, 727, 740
rational mapping, 241
rho method, 103
root of unity, 454, 458
  primitive, 454, 458
rotor cryptomachine, 28–30
RSA, 68
RSA problem, 78
S-box, 33
satisfiability problem, 844
scalar product, 1008
secant-tangent law, 350
separability, 407
sesquilinear form, 1011
Shor algorithm, 864
  quantum part, 870
Sieve of Eratosthenes, 929
singular point, 227
singularity, 227
skew-linear, 1011
smooth integer, 98
square, 930
supersingular, 573
symmetric cryptosystem, 20, 43
tensor permutation, 741
tensor product, 1033
tensor product operator, 1045
torsion subgroup, 434
transposition, 27
trapdoor, 55
trapdoor function, 55
trial division, 109
trusted authority, 646
U-gate, 773
uniformizer, 475
unique factorization theorem, 896
unitary operator, 1044
vector space, 1007
Weierstrass equation, 276
Weierstrass form, 270
Weierstrass polynomial, 276
weight, 321
Weil pairing, 459
  modified, 630
X-gate, 749
Y-gate, 750
Z-function, 560
Z-gate, 751
zero, 475
zeta function, 564
...