

Index

A

Alon–Boppana theorem, 139

B

Babai’s nearest plane algorithm, 221

BKZ algorithm, 221

Bounded distance decoding, 221, 279

Branch-and-bound algorithm, 239

C

Cayley graphs, 63, 97, 139, 159

Class number, 63, 257, 279

Code-based cryptography, 43

Continued fractions, 118

Coppersmith’s method, 297

CPLEX, 240

Cyclotomic fields, 257, 279

D

Differential equations, 1, 118

Digital signature, 17, 43, 316

Dirichlet L-functions, 257, 279

Discrete logarithm problem, 81, 97

E

Elliptic curves, 63, 81, 97

EUFCMA, 316

Expander graphs, 63, 97, 159

G

Gröbner bases, 17, 221

H

Hardy–Littlewood conjecture, 159

Hash function, 63, 159, 316

Hermite factor, 221

Homomorphic encryption, 221, 279, 332

I

Ideal lattices, 279

Identity-based encryption, 349

IND-CCA, 332

Information theoretic security, 178

Integer programming, 239

Isogeny, 63, 97

K

Kawazoe–Takahashi curves, 81

Key exchange, 97

L

Lattice basis reduction, 221, 297

Lattice-based cryptography, 1, 257, 349

Learning with errors, 221

LLL algorithm, 221, 239

M

MAGMA, 1, 17, 279

MinRank problem, 17

Multivariate public key cryptography, 1, 17

N

Noisy/Leakage model, 199, 316

NP-hard, 17, 239

Number field sieve, 81

P

Physical attacks, 17
Post-quantum cryptography, 1, 17, 97, 279
Public key encryption, 1, 17, 43, 349

Q

Quantum Rabi models, 1, 118
Quaternion algebra, 159

R

Ramanujan graphs, 63, 139, 159
Representations of \mathfrak{sl}_2 , 118
Riemann hypothesis, 139, 159, 257
RSA key recovery attacks, 1, 199

S

Security modeling, 1
Shor's algorithm, 1

Shortest vector problem, 221, 239
Side channel attacks, 1, 17
Siegel zeros, 257
Spectra of graphs, 139
Spectrum, 118

U

Uniform random number generation, 178

V

Vélu's formula, 81, 97

W

Weil pairing, 81, 97

Z

Zeta functions, 1, 118, 257, 279