

Index

Author Index

Adleman, L., 26, 89, 334
Ajtai, M., I., 91
Bach, E., 90
Bellare, M., 321
Ben-Or, M., 321
Blum, M., 89, 169, 321, 337
Brassard, G., 321
Carter, L., 170
Chaitin, G.J., 102
Chaum, D., 321
Crépeau, C., 321
Diffie, W., 26, 89
Even, S., 187
Feige, U., 321
Feldman, P., 321
Fiat, A., 321
Fischer, M., 26
Goldreich, O., 89, 170, 320–322
Goldwasser, S., 22, 26, 169, 170, 320, 321, 337
Håstad, J., 170
Hellman, M.E., 26, 89, 90
Impagliazzo, R., 170
Kilian, J., 321
Kolmogorov, A., 102
Krawczyk, H., 170
Lapidot, D., 321
Levin, L.A., 89, 91, 170
Lipton, R., 26
Luby, M., 170
Merkle, R.C., 26, 90
Micali, S., 22, 26, 89, 169, 170, 320, 321, 337
Naor, M., 320
Odlyzko, A., 90

Pratt, V., 90
Rabin, M., 26, 89
Rackoff, C., 26, 89, 170, 320, 321
Rivest, R.L., 22, 26, 89, 334
Shamir, A., 26, 89, 90, 321, 334
Shannon, C.E., 26
Sipser, M., 170
Solomonov, R.J., 102
Turing, A., 188
Vadhan, S., 322
Virgil, 195, 207
von Kant, P., 195, 207
Wegman, M., 170
Wigderson, A., 320, 321
Wittgenstein, L., 21
Yao, A.C., 89, 169

Subject Index

Arguments. *See* Interactive proofs
Averaging argument. *See* Techniques

Blum integers, 57, 60, 62, 283, 337

Chebyshev inequality, 10, 29, 70, 72, 137
Chernoff bound, 11, 28, 29, 106, 147
Chinese Remainder Theorem, 60, 335
Classic cryptography, 2, 26
Claw-free pairs. *See* One-way functions
Collision-free hashing. *See* Hashing
Commitment schemes, 223–240, 242–243, 252,
274, 276, 287, 320
 based on one-way function, 226–227
 based on one-way permutation, 225–226

- canonical revealing, 225, 280, 290, 315
- computational secrecy, 290
- computationally binding, 225, 278–286
- computationally hiding, 225, 228, 278, 285, 289, 290
- non-oblivious, 269, 294–297, 352
- non-uniform computational secrecy, 227, 229–240, 242
- non-uniform computational unambiguity, 283
- perfect a posteriori secrecy, 283–284, 293
- perfect secrecy, 288, 290
- perfectly binding, 225, 278, 284, 285, 289, 290, 313
- perfectly hiding, 225, 278–286, 289–294, 300, 313
- terminology, 278
- two senders, 313–317, 321
- with trapdoor, 297–298
- Complexity classes
 - \mathcal{AM} , 250–251
 - \mathcal{BPP} , 15–16, 18, 29, 31, 188, 194, 195, 201, 205, 209, 247–249, 253–255, 270, 277, 282, 287, 306, 309, 311, 319, 330
 - $\text{co}\mathcal{AM}$, 250
 - $\text{co}\mathcal{NP}$, 199, 250
 - \mathcal{CZK} , 205
 - \mathcal{IP} , 194, 199, 205
 - \mathcal{MA} , 324
 - \mathcal{NP} , 13, 26, 31, 184, 188–189, 194, 195, 198, 199, 223, 240–243, 246, 249–251, 254–261, 263, 268–269, 276, 284–288
 - \mathcal{NPC} , *see* \mathcal{NP} -completeness 12
 - \mathcal{P} , 12, 31, 189
 - \mathcal{PCP} , *See* Probabilistically checkable proofs
 - \mathcal{PSPACE} , 199
 - \mathcal{PZK} , 205
 - \mathcal{SZK} , 205, 322
 - \mathcal{ZK} , 205
- Composite numbers
 - Blum integers. *See* Blum integers
 - some background, 334–337
- Computational complexity
 - assumptions, 19–20
 - average-case complexity, 20, 31, 91
 - background, 12–20
 - classes. *See* Complexity classes
 - non-uniform complexity, 16–19
- Computational difficulty. *See* One-way functions
- Computational indistinguishability, 26, 74, 76–77, 101, 103–112, 115–118, 120–123, 127–128, 132, 139, 148, 164–165, 169, 202–204, 207, 213–216, 220–222, 224, 231–239, 255, 256, 300, 302, 307, 309
- by circuits, 106–107, 111–112, 148, 173–174, 214–216, 221, 222, 228, 232–239
- by repeated sampling, 107–110, 152, 157
- versus statistical indistinguishability, 106–107, 113, 170
- Computational models
 - interactive machines. *See* Interactive machines
 - non-determinism. *See* Non-determinism.
 - non-uniform. *See* Non-uniform complexity.
 - oracle machines. *See* Oracle machines
 - probabilistic machines. *See* Probabilistic machines
- Cryptographic protocols, 6–8, 350–353
- Density-of-primes theorem, 94, 333
- DES
 - high-level structure, 164, 166–167
- Discrete-logarithm problem. *See* DLP function
- DLP. *See* DLP function
- DLP function, 57, 282, 289
 - claw-free property, 61, 282
 - hard-core, 65, 89, 91, 133
- Elliptic curve, 58
- Encryption schemes, 2–3, 31, 169, 338–345
 - chosen message attack, 269
 - private-key, 26
 - public-key, 3, 26, 52, 225, 269, 327
 - Randomized RSA, 342
- Expander graph, 80, 81
 - explicitly constructed, 80, 91
 - random walk on, 80, 82, 83, 91
- Factoring integers, 40, 57
- Factoring polynomials, 332
- Fermat's little theorem, 332
- Fiat-Shamir identification scheme. *See* Identification schemes
- Function ensembles, 149–150
 - constructible, 149, 158
 - constructible and pseudorandom, 150
 - pseudorandom, 149, 158, 162
 - pseudorandom, more about. *See* Pseudorandom functions
- Gödel's Incompleteness Theorem, 188
- Gilbert-Varshamov bound, 41
- Graph Coloring, 228

- Graph connectivity, 13–14, 28–29
- Graph Isomorphism, 64, 97, 196, 207, 270, 275
- Hamiltonian cycle, 276, 297, 302
- Hard-core predicates. *See* One-way functions
- Hashing
 - collision-free, 52, 286, 287, 349
 - universal. *See* Hashing functions
 - universal one-way, 349
- Hashing functions, 136–137, 177–178
- Hoeffding inequality, 12, 28
- Hybrid argument. *See* Techniques
- Identification schemes, 270–274
 - Fiat-Shamir, 272, 321
- Identifying friend or foe, 157
- Interactive machine, 191
 - joint computation, 191
 - the complexity of, 192
 - two-partner model, 311, 312
- Interactive proofs, 190–200, 277
 - arguments, 223, 247, 251, 277–288, 321
 - Arthur-Merlin, 198, 254, 320
 - auxiliary inputs, 199–200, 213, 230, 234, 240–242, 255, 277
 - completeness, 193–195, 198
 - computationally sound, 223, 251–253, 277–288, 321
 - constant-round, 199
 - definition, 190–195, 320
 - error reduction, 194, 195, 230
 - for Graph Non-Isomorphism, 195–199, 320
 - for $PSPACE$, 199, 320
 - general definition, 194
 - multi-prover, 223, 311–321
 - \mathcal{NP} as a special case, 188, 194
 - perfect completeness, 198, 199, 243
 - proving power of, 198–199
 - public-coin, 198, 199, 243, 253–254
 - round-efficient, 288
 - simple definition, 193
 - soundness, 193–195, 198
 - unidirectional, 247
 - zero-knowledge. *See* Zero-knowledge
- IP
 - as a class. *See* Complexity classes
 - the notion. *See* Interactive proofs
- Kolmogorov complexity, 102, 105, 170
- Markov inequality, 9, 28, 29, 67
- Message authentication, 5, 344, 345, 347
- Negligible function, 16, 32, 33, 35, 105, 106, 202, 204, 266, 274
- NIZK. *See* Zero-knowledge
- Non-determinism, 13, 15, 19
- Non-interactive zero-knowledge. *See* Zero-knowledge
- Non-uniform complexity, 16–19, 41–43, 59, 88, 93, 111–112, 148, 214–216, 221, 222, 228–240, 242, 283, 287, 294, 297, 305, 327
- Noticeable function, 35, 266
- \mathcal{NP}
 - as a class. *See* Complexity classes
 - as a proof system. *See* Interactive proofs, 188, 194, 247, 299
 - versus P . *See* P -vs- \mathcal{NP} question
- \mathcal{NP} -completeness, 13, 41, 228, 240–246
 - Bounded Halting, 244
 - $G3C$, 13, 240
 - generic reduction, 241, 326
 - Karp reduction, 241, 327
 - Levin reduction, 326
 - strong sense, 241, 298, 326
- Oblivious transfer, 26
- One-way functions, 1–4, 7, 26, 27, 30–100, 252, 257, 272, 297, 340, 344, 347, 349
 - based on coding theory, 41, 89, 90
 - based on DLP, 57, 90, 282
 - based on factoring, 40, 57, 90, 282
 - based on integer lattices, 91
 - based on subset sum, 41, 89, 90
 - candidates, 40–41, 55–58, 63–64
 - claw-free collections, 53, 60–63, 89, 282, 294
 - collection of, 53–63, 65, 249
 - definitions, 32–43
 - distributional, 96, 174
 - hard-core, 64–78, 89, 170
 - hard-core functions, 74–78, 89, 134–135, 138–141
 - length conventions, 35–40
 - length-preserving, 39
 - length-regular, 39
 - modular squaring, 57
 - motivation, 31–32
 - non-uniform hardness, 41–43, 59, 88, 93, 148, 205, 228, 249, 259, 269, 276, 297, 323, 327

- One-way functions (*cont.*)
 - on some lengths, 36
 - one-to-one, 40, 98, 135, 138, 141, 225, 226
 - quantitative hardness, 48, 79
 - Rabin function, 57, 89, 90
 - regular, 79, 142, 146
 - RSA, 56, 89, 90
 - strong, 32, 66
 - strong vs weak, 43–51, 78–89
 - the inner-product hard-core, 65–76
 - universal, 52–53, 89
 - weak, 35, 89, 96
- One-way permutations, 79, 225, 256, 281, 305, 310, 328, 349
 - based on DLP, 57, 133
 - based on factoring, 57, 134
 - claw-free collections, 61–63, 89, 349
 - collection of, 53, 56–61, 66, 88
 - hard-core, 66, 131, 225, 250, 301–302, 328, 341
 - modular squaring, 57
 - non-uniform hardness, 286
 - RSA, 56, 133
 - with trapdoor, 53, 58–60, 66, 88, 302, 305, 311, 340–344, 352
- Oracle machines, 20, 148–169, 262–277
- P-vs-NP question, 13, 20, 22, 31, 93
- Parallel composition
 - in computationally sound proofs, 223, 278, 323
 - in interactive proofs, 209
 - in multi-prover proofs, 223, 313, 317, 318, 322, 323
 - in proofs of knowledge, 223, 268, 328
 - in witness-indistinguishable proofs, 258–259
 - in zero-knowledge protocols, 222–223, 240, 246, 251–254, 321
- PCP. *See* Probabilistically checkable proofs
- Permutation ensembles, 164
 - invertible, 165
 - pseudorandom, 164
 - strongly pseudorandom, 165
- Primality testing, 332–333
- Prime numbers
 - generation of, 134, 333
 - some background, 331–334
- Probabilistic machines, 14–16
- Probabilistically checkable proofs, 254, 286, 287, 319, 322
- Probability ensembles, 104
 - efficiently constructible, 108
- Probability theory
 - conventions, 8–9
 - inequalities, 9–12
- Proofs of ability, 270, 273–274
- Proofs of identity. *See* Identification schemes
- Proofs of knowledge, 223, 252, 262–277, 294–296, 298, 321, 352
 - ability. *See* Proofs of ability
 - applications, 269–274
 - definition, 262–266
 - error reduction, 266–268, 328
 - for Hamiltonian cycle, 276, 329
 - for \mathcal{NP} in zero-knowledge, 269, 277
 - in zero-knowledge, 268–269, 275–277
 - strong, 274–277, 329
- Protocols. *See* Cryptographic protocols
- Pseudorandom Ensembles, 112
 - unpredictability of, 119–123, 176
- Pseudorandom functions, 101, 148–163, 170, 171, 274, 341, 347, 348
 - applications, 157–158, 170, 171
 - based on pseudorandom generators, 150–157
 - generalized notion, 158–163
 - methodology, 157–158
- Pseudorandom generators, 3–4, 101, 226–227, 307–309, 340
 - applications, 119, 171, 226
 - based on 1-1 one-way functions, 135–141
 - based on DLP, 133, 170
 - based on factoring, 134, 170
 - based on one-way functions, 135–148, 170, 171
 - based on one-way permutations, 124–135, 169
 - based on regular one-way functions, 141–147
 - based on RSA, 133
 - computational indistinguishability. *See* Computational indistinguishability
 - construction of, 124–148
 - definitions, 112–124, 169
 - direct access, 179
 - increasing the expansion, 114–118
 - motivation, 102–103
 - necessary condition, 123–124
 - non-uniform hardness, 148
 - on-line, 176–177, 179
 - standard definition, 113
 - unpredictability of, 119–123, 169
 - variable-output, 114, 118–119
- Pseudorandom permutations, 164–171
 - based on pseudorandom functions, 166–169

- Rabin function, 57, 60
 - claw-free property, 62, 283
 - hard-core, 65, 89, 91, 134
- Random linear codes, 41
- Random Oracle Methodology, 171–172
- Random Oracle Model, *See* Random Oracle Methodology
- Random variables
 - conventions, 8–9
 - pairwise independent, 10–11, 68, 69
 - totally independent, 11–12, 106
- Reducibility argument. *See* Techniques
- Rigorous treatment
 - asymptotic analysis, 23
 - motivation, 21–25
- RSA function, 56, 60
 - hard-core, 65, 91, 133
 - hard-core function, 74, 342
- Secret sharing schemes, 352
- Sequential composition
 - in computationally sound proofs, 278
 - in multi-prover proofs, 312
 - in proofs of knowledge, 267–268, 275–277
 - in zero-knowledge protocols, 216–222
- Signature schemes, 4–6, 26, 274, 298, 327, 345–350
- Signatures. *See* Signature schemes
- Signatures paradigm. *See* Techniques
- Sources of imperfect randomness, 171
- Statistical difference, 106, 113, 202, 204, 234, 280
- Statistical indistinguishability, 106, 204
- Subset sum, 41
- Techniques
 - averaging argument, 18, 42, 67, 71, 220, 239, 315
 - hybrid argument, 101, 102, 108–111, 115–118, 121–123, 138, 141, 152–157, 159, 163, 170, 182, 220–222, 233, 239, 258–259, 309
 - leftover hash lemma, 136
 - probabilistic argument, 106–107
 - reducibility argument, 30, 37–39, 43–52, 66, 81, 82, 85–88, 108, 110, 124, 125, 133, 139, 140, 142–144, 285
 - the simulation paradigm, 189, 201, 266, 269
- Trapdoor permutation. *See* One-way permutations
- Undecidability
 - Halting Problem, 188
- Witness hiding, 257–261, 273, 298, 321
- Witness indistinguishability, 254–261, 309, 321, 328
 - concurrent composition, 259
 - parallel composition, 258–259
 - strong, 256–257, 328
- Yao's XOR Lemma, 89, 91
- Zero-knowledge, 7–8, 26, 184–330, 352
 - almost perfect, 204–205, 250–252, 280, 322
 - alternative formulation, 203, 255
 - applications, 242–243, 320
 - auxiliary inputs, 213–222, 230, 231, 241–242, 248, 255
 - black box, 214, 245, 251–254, 289
 - class of languages, 205
 - composition of, 216–223
 - computational, 202, 204, 206, 213, 214, 221
 - concurrent, 259, 323
 - constant-round, 253–254, 288–298, 300, 321
 - definitions, 200–207, 213–216, 320
 - deterministic prover, 248
 - deterministic verifier, 247–248
 - efficiency considerations, 243–245
 - expected polynomial time, 205–206, 245, 289–298
 - for Graph Coloring, 228–240
 - for Graph Isomorphism, 207–213, 273, 275, 320
 - for Graph Non-Isomorphism, 270
 - for Hamiltonian cycle, 244, 276, 303, 327, 329
 - for hard languages, 249–250
 - for \mathcal{IP} , 243, 320
 - for \mathcal{NP} , 223–246, 320
 - for Quadratic Non-Residuosity, 320
 - for Quadratic Residuosity, 321
 - honest verifier, 206–207, 299
 - knowledge tightness, 244–246, 327
 - liberal formulation, 205
 - motivation, 185–190
 - multi-prover, 311–321
 - negative results, 246–254, 320
 - non-interactive, 298–311, 321
 - outside \mathcal{BPP} , 249
 - parallel composition, 222–223, 240, 246, 251–254, 258
 - perfect, 201, 204, 205, 214, 221, 250, 311–322

- Zero-knowledge (*cont.*)
 proofs of knowledge. *See* Proofs of knowledge
 public coin, 253–254
 resettable, 323
 round-complexity, 244
 round-efficient, 254, 288–298, 300, 321
 sequential composition, 216–222, 230
 statistical, 204–205, 250–251, 280, 322
 unidirectional, 247–248
 uniform treatment, 215, 322
 witness hiding. *See* Witness hiding
 witness indistinguishability. *See* Witness indistinguishability
 \mathcal{ZK}
 as a class. *See* Complexity classes
 the notion. *See* Zero-knowledge
 ZKIP. *See* Zero-knowledge