

Index

Author Index

Adleman, L., 479, 587
Awerbuch, B., 757

Barak, B., 481, 775, 781
Beaver, D., 757
Ben-Or, M., 757
Blum, M., 479, 480, 757

Canetti, R., 753, 757
Chaum, D., 757
Chor, B., 757
Crépeau, C., 757

Damgård, I., 757
Diffie, W., 475, 478, 587
Dolev, D., 480
Dwork, C., 480, 778, 779

Even, S., 757

Feige, U., 782
Feldman, P., 480

Goldreich, O., 479, 756, 757, 780
Goldwasser, S., 379, 382, 479, 480, 587, 588,
589, 757

Hellman, M. E., 475, 478, 479, 587

Impagliazzo, R., 481

Kilian, J., 778
Krawczyk, H., 780

Lapidot, D., 782
Lempel, A., 757
Lipton, R., 480

Merkle, R. C., 479
Micali, S., 379, 382, 479, 480, 587, 588, 589,
756, 757

Naor, M., 480, 588, 778, 779

Pfitzmann, B., 589

Rabin, M., 587, 757
Richardson, R., 778
Rivest, R. L., 478, 587, 588, 589
Rogaway, P., 757
Rompel, J., 588
Rudich, S., 481

Sahai, A., 480, 778, 779
Shamir, A., 478, 587, 782
Shannon, C. E., 378, 476, 478

Wigderson, A., 756, 757

Yao, A. C., 479, 587, 756, 757
Yung, M., 480, 588

Subject Index

Averaging Argument. *See* Techniques

Byzantine Agreement, 711
Authenticated, 711–714, 717, 758

- Chinese Remainder Theorem, 421
- Claw-free pairs. *See* One-way permutations
- Collision-free hashing. *See* Hashing
- Collision-resistant hashing. *See* Hashing
- Commitment schemes
 - non-oblivious, 771
 - perfectly binding, 465–469
- Computational indistinguishability, 382,
 - 395–402, 446, 447–449, 457, 465, 467–468, 479, 618, 770
- by circuits, 382–393, 412, 417, 419, 431, 454, 618
- Cryptographic protocols, 599–764
 - active adversary, 603
 - adaptive adversary, 603, 748–751
 - Authenticated Computation, 664–668, 671–674, 717–722
 - Coin-tossing, 659–664, 674–677, 722–725
 - Communication models, 602–603
 - Computational limitations, 603
 - Concurrent executions, 752–755
 - Definitional approach, 601–607
 - Definitions, 615–634, 694–700, 742–743, 749, 752–754
 - Environmentally-secure, 753–755
 - Fairness, 604, 747–748
 - functionality, 599
 - General circuit evaluation, 645–648, 705–707
 - honest-but-curious adversary, 603
 - Image Transmission, 668–671, 672, 718–721
 - Input-Commitment, 677–680, 725–726
 - Multi-party, 599, 600, 604–606, 607–609, 610–611, 613–615, 693–747, 755
 - non-adaptive adversary, 603
 - number of dishonest parties, 604
 - Oblivious Transfer, 612, 614, 635, 640–645
 - Oracle-aided, 636, 639, 644, 646, 652, 672, 674, 678, 681, 701, 704, 715, 718, 721, 722, 726, 729, 737
 - Overview, 599–615
 - passive adversary, 603
 - Privacy reductions, 635–640, 643, 644, 647, 648, 701–703, 704
 - Private Channels, 741–747
 - Pure oracle-aided, 721–722
 - Reactive, 609, 751–752
 - Secret Broadcast, 716–717, 718, 722
 - Security reductions, 652–657, 673, 675, 677, 678, 714–716, 719, 721, 723
 - Setup assumptions, 602, 608, 755
 - The malicious model, 600, 603, 608, 610–611 626, 634, 650–693, 697–700, 708–741, 746–747
 - The semi-honest model, 600, 603, 608, 610–615, 619 626, 634–650, 696, 697, 700–708, 743–746
 - Two-party, 599, 600, 606–607, 608, 611–613, 615–693, 755
 - Universally Composable, 753
 - Verifiable Secret Sharing. *See* Secret Sharing
- Discrete Logarithm Problem. *See* DLP
 - function
- DLP function, 584
- Encryption schemes, 373–496
 - active attacks, 422–425, 431–474
 - asymmetric, 376
 - Basic Setting, 374–377
 - Block-Ciphers, 408–418, 420
 - chosen ciphertext attacks, 423, 438–469, 472–474
 - chosen plaintext attacks, 423, 431–438
 - Definitions, 378–403
 - indistinguishability of encryptions, 378, 382–383, 403, 412, 415, 417, 419, 424, 432, 459, 461, 479
 - multiple messages, 378, 389–393, 394–402, 429, 437–438, 443–449, 489
 - non-malleability, 422, 470–474
 - passive attacks, 422, 425–431
 - perfect privacy, 378, 476–477
 - perfect security, 476–477
 - Private-Key, 375–376, 377, 380, 381, 404–408, 410–413
 - Probabilistic Encryption, 404, 410–422
 - Public-Key, 376, 377, 380, 381, 413–422
 - Randomized RSA, 416–417, 478
 - Semantic Security, 378, 379–382, 478
 - Stream-Ciphers, 404–408
 - symmetric, 375
 - The Blum-Goldwasser, 420–422, 478
 - the mechanism, 376–377
 - uniform-complexity treatment, 393–403
- Factoring integers, 421, 584
- Hard-core predicates. *See* One-way permutations
- Hash and Sign. *See* Techniques

- Hashing
 - collision-free, 512–523, 542–543, 558, 560–561, 562, 575
 - based on claw-free permutations, 516–519
 - via block-chaining, 519–521
 - via tree-hashing, 521–523
 - collision-resistant. *See* collision-free, 513
 - Universal. *See* Hashing functions
 - Universal One-Way, 513, 543, 560–575, 588
- Hashing functions, 527–537, 563–565, 596
 - AXU, 535–537, 589
 - collision probability, 528–531, 535
 - generalized, 530–531, 589
- Hybrid Argument. *See* Techniques
- Interactive Proofs
 - perfect completeness, 658
 - Zero-Knowledge. *See* Zero-Knowledge
- Message authentication, 423, 497–537
 - attacks and security, 502–507
 - basic mechanism, 501–502
 - length-restricted, 507–516
 - state-based, 531–537, 548, 585
- NIZK. *See* Zero-Knowledge
- Non-Interactive Zero-Knowledge. *See* Zero-Knowledge
- Non-uniform complexity, 378–393, 402, 618–619, 620, 622
- Oblivious Transfer. *See* Cryptographic protocols
- One-way functions, 423, 525, 538, 539–542, 560–575
 - non-uniform hardness, 403, 411
- One-way permutations, 562, 563–565, 570–571
 - claw-free collections, 516–519, 542, 588
 - collection of, 765–768
 - hard-core, 414–422, 431, 640–643
 - modular squaring, 419–421
 - RSA, 416, 766
 - with trapdoor, 403, 413–422, 423, 640–643, 648, 650, 765–768
- Probabilistic encryption. *see* Encryption schemes
- Probability ensembles, 379
 - efficiently constructible, 394–403
- Proofs-of-Knowledge, 453, 669–671
 - for NP in zero-knowledge, 659, 669, 718–720
- Protocols. *See* Cryptographic protocols
- Pseudorandom functions, 410, 423, 424, 438, 450–452, 523–532, 556–558, 768
 - generalized notion, 556, 768
 - non-uniform hardness, 411–412
 - Verifiable, 590
- Pseudorandom generators, 404
 - Computational indistinguishability. *See* Computational indistinguishability
 - non-uniform hardness, 392
 - on-line, 407–408, 534–537
- Quantum cryptography, 477
- Rabin function, 766
 - hard-core, 422
- Random Oracle Methodology, 478, 586–587
- Random Oracle Model. *See* Random Oracle Methodology
- Reducibility Argument. *See* Techniques
- RSA function, 766
 - hard-core function, 416
- Secret Sharing, 489, 730–731
 - Verifiable, 729–735, 737–740, 752
- Signature schemes, 497–523, 537–598
 - attacks and security, 502–507
 - authentication-trees, 537, 545–560
 - basic mechanism, 501–502, 538
 - Fail-stop, 583–584
 - incremental signing, 581–583
 - length-restricted, 507–516
 - memory-dependent, 546–556, 559–560, 588
 - off-line/on-line signing, 580–581
 - one-time, 465–469, 538–575
 - super-security, 465–469, 576–580
 - The refreshing paradigm, 537, 543–560
 - unique signature, 575–576
- Signatures. *See* Signature schemes
- Simulation paradigm. *See* Techniques
- Synchronous communication, 603, 695, 777
- Techniques
 - Averaging Argument, 386
 - Hash and Sign, 513–516, 526–537, 542–543, 571–575, 576
 - Hybrid Argument, 391, 402, 429, 448–449, 457, 459–461, 467–468, 479, 593, 637–638, 703, 754

INDEX

Techniques (*cont.*)

Reducibility Argument, 385, 387, 402,
410, 510, 514, 518, 525, 540, 551,
564, 567, 569
the simulation paradigm, 379, 479, 601,
620

Trapdoor permutations. *See* One-way
permutations

Universal One-Way Hash Functions. *See*
Hashing

Verifiable Secret Sharing. *See* Secret
Sharing

Witness Indistinguishability, 782–783
Non-Interactive, 464–469
Strong, 768–772

Zero-Knowledge, 775–783
Composition of protocols, 775–780
Concurrent composition, 777–780
for NP, 658, 664–671