

List of Publications of Moni Naor

Books Edited

1. *Theory of Cryptography*, First TCC Proceedings, Lecture Notes in Computer Science 2951, Springer Verlag, 2004.
2. *Advances in Cryptology - EUROCRYPT 2007*, 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, May 20-24, 2007, Proceedings, Lecture Notes in Computer Science 4515, Springer Verlag, 2007.

Journal Papers

3. J. Naor, M. Naor, A. Schäffer. *Fast parallel algorithms for chordal graphs*, Siam Journal on Computing, vol 18, pp. 327–349, 1989.
4. M. Naor, *Succinct representation of general unlabeled graphs*, Discrete Applied Mathematics, vol 28, 1990, pp. 303–307.
5. J. Bruck, M. Naor, *The hardness of decoding with preprocessing*, IEEE Transactions on Information Theory, vol 36, No. 2, 1990, pp. 381–385 .
6. A. Bar-Noy, J. Naor, M. Naor, *One Bit Algorithms*, Distributed Computing, vol 4, 1990, pp. 3–8.
7. A. Fiat, J. I. Munro, M. Naor, A. Schäffer, J.P. Schmidt, and A. Siegal, *An implicit data structure for searching a multi-key table in logarithmic time*, J. of Computer and Systems Sciences, vol 43, pp. 406–424, 1991. (Special issue of STOC 88).
8. M. Naor, *A lower bound on probabilistic algorithms for distributive ring coloring*, Siam Journal on Discrete Mathematics, vol 4, pp. 409–412, 1991.
9. M. Naor. *Bit commitment using pseudo-randomness*, Special issue of Crypto 89. Journal of Cryptology, vol. 4, 1991, pp. 151–158.
10. A. Fiat, M. Naor, J.P. Schmidt, and A. Siegal, *Non-oblivious hashing*, Journal of the ACM, vol 39, 1992, pp. 764–782.
11. S. Kannan, M. Naor and S. Rudich, *Implicit representation of graphs*, SIAM J. on Discrete Math. , vol 5, 1992, pp. 596–603.
12. N. Alon, J. Bruck, J. Naor, M. Naor and R. M. Roth, *Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs*, IEEE Transactions on Information Theory, vol 38, 1992, pp. 509–516.
13. S. Irani, M. Naor and R. Rubinfeld, *On the time and space complexity of computation using write once memory*, Mathematical Systems Science, vol 25, 1992, pp. 141–159.
14. A. Fiat and M. Naor, *Implicit $O(1)$ probe search*, SIAM J. on Computing, vol 22, 1993, pp. 1–10.
15. D. Feldman, R. Impagliazzo, M. Naor, N. Nisan, S. Rudich, A. Shamir, *On dice and coins*, Information and Computation, vol 104, 1993, pp. 159–174.

16. M. Naor, A. Orlitzky and P. Shor, *Three results on interactive communication*, IEEE Transactions on Information Theory, vol 39, 1993, pp. 1608–1615.
17. J. Naor and M. Naor, *Small bias probability spaces: efficient constructions and applications*, SIAM J. on Computing, vol 22, 1993, pp. 838–856. Preliminary version: STOC 90.
18. N. Alon and M. Naor, *Coin-flipping games immune against linear-sized coalitions*, SIAM J. on Computing, vol 22, 1993, pp. 403–417. Preliminary version: FOCS 90.
19. R. Motwani, J. Naor and M. Naor, *The probabilistic method yields deterministic parallel algorithms*, J. of Computer and Systems Sciences, Vol. 49, No. 3, December 1994, pp. 478–516. Special issue of FOCS 89,
20. M. Blum, W. Evans, P. Gemmell, S. Kannan and M. Naor, *Checking the correctness of memories*, Algorithmica, 1994, pp. 225–244. Preliminary version: FOCS 91.
21. L. Lovász, M. Naor, I. Newman and A. Wigderson, *Searching in the decision tree model*, SIAM Journal on Discrete Mathematics, vol 8, 1995, pp. 119–132. Preliminary version: FOCS 91.
22. M. Naor and R. Roth, *Optimal file sharing in distributed networks*, SIAM J. on Computing, 24 (1995), 158–183. Preliminary version: FOCS 91.
23. T. Feder, E. Kushilevitz and M. Naor and N. Nisan, *Amortized communication complexity*, SIAM J. on Computing, vol 25, 1995, pp. 736–750. Preliminary version: FOCS 91.
24. R. Fagin, M. Naor and P. Winkler, *Comparing Information Without Leaking It*, C. of the ACM, vol 39, May 1996, pp. 77–85.
25. N. Alon and M. Naor, *Derandomization, witnesses for Boolean matrix multiplication and construction of perfect hash functions*, Algorithmica, vol 16, 1996, pp. 434–449. Preliminary version: FOCS 92.
26. M. Naor and L. Stockmeyer, *What can be computed locally*, SIAM J. on Computing, vol 24, 1995, pp. 1259–1277. Preliminary version: STOC 93.
27. R. Impagliazzo and M. Naor. *Efficient Cryptographic schemes provably secure as subset sum*, Journal of Cryptology, vol 9, 1996, pp. 199–216. Preliminary version: FOCS 89.
28. M. Naor, R. Ostrovsky, R. Venkatesan and M. Yung, *Zero-Knowledge Arguments for NP can be Based on General Assumptions*, Journal of Cryptology, vol 11, 1998, pp. 87–108. Preliminary version: Advances in Cryptology – Proceedings of Crypto '92, Lecture Notes in Computer Science 740, Springer Verlag, 1993, pp. 196–214.
29. C. Dwork and M. Naor, *An Efficient Existentially Unforgeable Signature Scheme and its Applications*, Journal of Cryptology, vol 11, 1998, pp. 187–208. Preliminary version: Advances in Cryptology – Crypto'94 Proceeding, Springer-Verlag,
30. M. Naor and A. Wool, *The load capacity and availability of quorum systems*, SIAM J. on Computing, vol 27, 1998, pp. 423–447. Preliminary version: FOCS 94.
31. M. Naor and B. Pinkas, *Secure accounting and auditing on the Web*, Computer Networks vol. 30, 1998, pp. 541–550. (Proceedings of the 7th International World Wide Web Conference).

32. M. Ajtai, J. Aspnes, M. Naor, Y. Rabani, L. Schulman and O. Waarts, *Fairness in scheduling*, Journal of Algorithms, vol. 29 (2), Nov 1998, pp. 306–357. (Special issue of ACM-SIAM SODA 1995).
33. M. Naor and A. Wool, *Access Control and Signatures via Quorum Secret Sharing*, IEEE Trans. on Parallel and Distributed Systems, vol. 9, 1998, pp. 909–922. Preliminary version: 3rd ACM Conference of Computer and Communication Security, 1996, pp. 157–168.
34. A. Fiat and M. Naor, *Rigorous time-space tradeoffs for inverting functions*, SIAM J. on Computing 29(3), 1999, pp. 790–803. Preliminary version: STOC 1991.
35. M. Naor and O. Reingold, *On the Construction of Pseudo-Random Permutations: Luby-Rackoff Revisited*, Journal of Cryptology, vol 12, 1999, pp. 29–66. Preliminary version: Proceedings of the 27th ACM Symposium on Theory of Computing, 1997.
36. M. Naor and O. Reingold, *Synthesizers and Their Application to the Parallel Construction of Pseudo-Random Functions*, J. of Computer and Systems Sciences, vol. 58 (2), April 1999, pp. 336–375. (Special Issue of FOCS’95.)
37. M. Naor and K. Nissim, *Certificate Revocation and Certificate Update*, IEEE Journal on Selected Areas in Communications (JSAC) Vol. 18 no. 4, April 2000, pp. 561–570. Preliminary version: 7th USENIX Security Symposium, 1998.
38. C. Blundo, A. De Santis and M. Naor, *Visual cryptography for grey level images*, Information Processing Letters 75(6): pp. 255–259 (2000).
39. B. Chor, A. Fiat, M. Naor and B. Pinkas, *Tracing Traitors*, IEEE Transactions on Information Theory, Vol. 46, No. 3, May 2000, pp. 893–910.
40. M. Naor and S. Ruah, *On the Decisional Complexity of Problems Over the Reals*, Information and Computation 167(1), 2001, pp. 27–45.
41. D. Dolev, C. Dwork and M. Naor, *Non malleable cryptography*, SIAM J. on Computing 30(2), 2000, pp. 391–437. Reprinted (with update) in SIAM Review Volume 45, Number 4 pp. 727–784. Preliminary version: STOC 1991.
42. M. Naor and B. Pinkas, *Efficient Trace and Revoke Schemes*, to appear, International Journal of Information Security, Preliminary version: Financial Cryptography 2000, Lecture Notes in Computer Science 1962, Springer.
43. C. Dwork, M. Naor and A. Sahai, *Concurrent Zero-Knowledge*, Journal of the ACM, vol 51(6) Nov 2004. Prel. version: Proc. 30th Annual ACM Symposium on the Theory of Computing, Houston, 1998, pp. 409–418.
44. M. Naor, O. Reingold and A. Rosen, *Pseudo-Random Functions and Factoring*, Siam J. on Computing Vol. 31 (5), pp. 1383–1404, 2002. Preliminary version: Proc. 32nd Annual ACM Symposium on the Theory of Computing, 2000, pp. 11–20.
45. R. Fagin, A. Lotem and M. Naor, *Optimal Aggregation Algorithms for Middleware*, J. of Computer and Systems Sciences, Vol. 66(4), 2003, pp. 614–656 (2003) (Special issue of PODS 2001). Preliminary version: Proc. 2001 ACM Symposium on Principles of Database Systems, pp. 102–113.

46. M. Naor and O. Reingold *Constructing Pseudo-Random Permutations with a Prescribed Structure*, Journal of Cryptology 15(2), 2002, pp. 97–102. Preliminary version: Twelfth Annual ACM-SIAM Symposium on Discrete Algorithms, 2001.
47. D. Naor and M. Naor *Protecting Cryptographic Keys: The Trace and Revoke Approach*, IEEE Computer Journal, vol. 36 no. 7, July 2003, pp. 47–53.
48. C. Dwork, M. Naor, O. Reingold and L. Stockmeyer, *Magic Functions*, J. of the ACM, vol. 50 no. 6, 2003, pp. 852–921. Prelim. version FOCS'99.
49. M. Naor and O. Reingold, *Number-Theoretic Constructions of Efficient Pseudo-Random Functions*, J. of the ACM 51(2), 2004, pp. 231–262.
50. M. Naor and U. Wieder, *Scalable and Dynamic Quorum Systems*, Special issue of PODC 2003, Distributed Computing, vol 17 (4), 2005, pp. 311–322.
51. M. Naor, *On Fairness in the Carpool Problem*, J. of Algorithms, vol. 55(1) 2005, pp. 93–98.
52. M. Naor and Benny Pinkas *Computationally Secure Oblivious Transfer*, J. of Cryptology 18(1), 2005, pp. 1–35.
53. M. Naor, and B. Pinkas, *Oblivious Polynomial Evaluation*, SIAM J. Computing, vol. 35(5), 1254–1281, 2006.
54. Danny Harnik, Moni Naor, Omer Reingold and Alon Rosen, *Completeness in Two-Party Secure Computation - A Computational View*, Journal of Cryptology, vol. 19, no. 4, October 2006, pp. 521–552. Preliminary version: Proc. 36th ACM Symp. on Theory of Computing 2004, pp. 252–261.
55. Moni Naor and Udi Wieder, *Novel architectures for P2P applications: The continuous-discrete approach*, ACM Transactions on Algorithms 3(3), 2007.
56. C. Dwork and M. Naor, *Zaps and their Applications*, SIAM J. Computing SIAM J. Computing 36(6), 2007, pp. 1513–1543. Preliminary version: FOCS 2000.
57. Ronen Gradwohl, Moni Naor, Benny Pinkas and Guy Rothblum, *Cryptographic and Physical Zero-Knowledge Proof Systems for Solutions of Sudoku Puzzles*, Theory of Computing Systems, 2008. Special issue of "Fun with Algorithms", 4th International Conference, FUN 2007. Preliminary version: Lecture Notes in Computer Science, Vol. 4475, Springer, 2007, pp. 166–182.
58. M. Naor, G. Segev and A. Smith, *Tight Bounds for Unconditional Authentication Protocols in the Manual Channel and Shared Key Models*, IEEE Transactions on Information Theory, vol 54(6), June 2008, pp. 2408–2425. Preliminary version: Advances in Cryptology – CRYPTO 2006 Proceeding, Lecture Notes in Computer Science 4117, Springer, 2006, pp. 214–231.
59. E. Kaplan, M. Naor and O. Reingold, *Derandomized Constructions of k -Wise (Almost) Independent Permutations*, Algorithmica, Vol. 55(1), 2009, pp. 113–133. Special issue of RANDOM 2005.
60. Tal Moran, Moni Naor and Gil Segev, *Deterministic History-Independent Strategies for Storing Information on Write-Once Memories*, Theory of Computing 5(1), 2009, pp. 43–67. Preliminary Version: ICALP 2007 pp. 303–314.
61. M. Naor and G. Rothblum, *The Complexity of Online Memory Checking*, Journal of the ACM, Volume 56, Issue 1 (January 2009). Preliminary Version: FOCS 2005, pp. 573–584.

62. T. Moran and M. Naor, *Basing Cryptographic Protocols on Tamper-Evident Seals*, Theor. Comput. Sci. 411(10), pp. 1283-1310 (2010). Special issue of ICALP 2005.
63. D. Harnik and M. Naor, *On the Compressibility of NP Instances and Cryptographic Applications*, Siam Journal on Computing, vol 39(5), 2010, pp. 1667-1713. Prelim. version: FOCS 2006.
64. Tal Moran and Moni Naor, *Split-Ballot Voting: Everlasting Privacy With Distributed Trust*, ACM Trans. Inf. Syst. Security, vol. 13(2), 2010. Special issue of ACM Conference on Computer and Communications Security (CCS) 2007.

Conference Proceedings Papers
(not including papers that appeared in Journals)

65. R. Impagliazzo and M. Naor, *Decision trees and downward closures*, Proceedings of the Third Symposium on Structure in Complexity, 1988, pp. 29–38.
66. D. Chaum, A. Fiat and M. Naor, *Untraceable electronic cash*, Advances in Cryptology – Proceedings of Crypto '88, Lecture Notes in Computer Science 403, Springer Verlag, 1989, pp. 319–327.
67. M. Naor and M. Yung, *Universal one-way hash functions and their cryptographic applications*, Proceedings of the Twenty First ACM Symposium on Theory of Computing, May 1989, pp. 33–43.
68. M. Naor and M. Yung, *Public key cryptosystems provable secure against chosen ciphertext attacks*, Proceedings of the Twenty second ACM Symposium on Theory of Computing, May 1990, pp. 427–437.
69. M. Naor, *String matching with preprocessing of pattern and text*, 18th International Colloquium on Automata, Languages and Programming, Lecture Notes in Computer Science 510, Springer Verlag, 1991.
70. C. Dwork, U. Feige, J. Kilian, M. Naor and S. Safra, *Low communication perfect zero knowledge two provers proof systems*, Advances in Cryptology – Proceedings of Crypto '92, Lecture Notes in Computer Science 740, Springer Verlag, 1993, pp. 215–227.
71. C. Dwork and M. Naor, *Pricing via Processing or Combatting Junk Mail*, Advances in Cryptology – Proceedings of Crypto '92, Lecture Notes in Computer Science 740, Springer Verlag, 1993, pp. 139–147.
72. M. Ajtai, N. Alon, J. Bruck, B. Cypher, M. Naor and E. Szemerédi, *Fault Tolerant Graphs, Perfect Hash Functions and Disjoint Paths* Proceedings of the IEEE Thirty third Annual Symposium on the Foundations of Computer Science, October 1992, pp. 693–702.
73. N. Megiddo, M. Naor and D. P. Anderson, *The minimum reservation rate problems and its applications in digital audio/video systems*, Proceedings of the second ISTCS, 1993, pp. 43–48.
74. P. Gemmell and M. Naor, *Codes for interactive authentication*, Advances in Cryptology – Crypto'93 Proceeding, Lecture Notes in Computer Science 740, Springer Verlag, 1994, pp. 355–367.
75. A. Fiat and M. Naor, *Broadcast Encryption*, Advances in Cryptology – Crypto'93 Proceeding, Springer-Verlag. Lecture Notes in Computer Science 740, Springer Verlag, 1994, pp. 480–491.
76. N. Alon, M. Blum, A. Fiat, R. Kannan, M. Naor and R. Ostrovsky, *Matching Nuts and Bolts*, Proc. ACM-SIAM Symposium on Discrete Algorithms, 1994.
77. U. Feige, J. Kilian, M. Naor *A minimal model for secure computation*, Proceedings of the 25th ACM Symposium on Theory of Computing, 1994.
78. M. Naor and A. Shamir, *Visual Cryptography*, Advances in Cryptology – Eurocrypt 94 Proceeding, LNCS vol. 950, Springer-Verlag, 1995, pp. 1–12.
79. J. Kilian and M. Naor, *Complexity of statistical reasoning*, Proceedings of the third ISTCS, 1995, pp. 209–217.

80. A. Mayer, M. Naor and L. Stockmeyer, *Local computation static and dynamic graphs*, Proceedings of the third ISTCS, 1995, pp. 268–278.
81. M. Naor, A. Srinivasan and L. J. Schulman, *Splitters and near-optimal derandomization*, Proceedings of the IEEE 36th Annual Symposium on the Foundations of Computer Science, Oct. 1995, pp. 182–192.
82. R. Canetti, U. Feige, O. Goldreich and M. Naor, *Adaptively Secure Multi-party Computation*, Proceedings of the 27th ACM Symposium on Theory of Computing, 1996, pp. 639–648.
83. C. Dwork, J. Lotspiech and M. Naor, *Digital Signets: Self-Enforcing Protection of Digital Information*, Proceedings of the 27th ACM Symposium on Theory of Computing, 1996, pp. 489–498.
84. M. Naor, *Evaluation may be easier than generation*, Proceedings of the 27th ACM Symposium on Theory of Computing, 1996, pp. 639–648.
85. R. Canetti, C. Dwork, M. Naor, R. Ostrovsky, *Deniable Encryption*, Advances in Cryptology – Crypto’97 Proceeding, Springer-Verlag, 1997, pp. 90–104.
86. M. Naor and B. Pinkas, *Visual Authentication and Identification*, Advances in Cryptology – Crypto’97 Proceeding, Springer, 1997, pp. 322–336.
87. M. Bellare, R. Impagliazzo and M. Naor, *Does parallel repetition reduce the error in computationally sound protocols?*, Proceedings of the IEEE 38th Annual Symposium on the Foundations of Computer Science, Oct. 1997, pp. 374–383.
88. M. Blaze, J. Feigenbaum and M. Naor, *A Formal Treatment of Remotely Keyed Encryption*, Advances in Cryptology – Eurocrypt’98 Proceeding, Lecture Notes in Computer Science No. 1403, Springer-Verlag, 1998, pp. 251–265.
89. M. Naor and B. Pinkas, *Secure and efficient metering*, Advances in Cryptology – Eurocrypt’98 Proceeding, Lecture Notes in Computer Science No. 1403, Springer-Verlag, 1998, pp. 576–590.
90. M. Naor and B. Pinkas, *Threshold Tracing Traitors*, Advances in Cryptology – Crypto’98 Proceeding, Lecture Notes in Computer Science No. 1462, Springer-Verlag, 1998, pp. 502–517.
91. M. Naor and O. Reingold, *From Unpredictability to Indistinguishability: A Simple Construction of Pseudo-Random Functions from MACs*, Advances in Cryptology – Crypto’98 Proceeding, Lecture Notes in Computer Science No. 1462, Springer-Verlag, 1998, pp. 267–282.
92. R. Canetti, J. Garay, G. Itkis, D. Micciancio M. Naor and B. Pinkas *Multicast Security: A Taxonomy and Efficient Constructions*, Proc. INFOCOM ’99, Vol. 2, pp. 708–716, New York, NY, March 1999.
93. M. Naor, B. Pinkas and O. Reingold, *Distributed Pseudo-Random Functions and KDCs*, Advances in Cryptology – Eurocrypt’99 Proceeding, Lecture Notes in Computer Science, Springer-Verlag 1592, 1999, pp. 327–346.
94. M. Naor and B. Pinkas, *Oblivious Transfer and Polynomial Evaluation*, Proc. 31st Annual ACM Symposium on the Theory of Computing, 1999, pp. 245–254.
95. M. Naor and B. Pinkas, *Oblivious Transfer with Adaptive Queries*, Advances in Cryptology – Crypto’99 Proceeding, Lecture Notes in Computer Science vol. 1666, Springer-Verlag, 1999, pp. 573–590.

96. M. Naor, B. Pinkas and R. Sumner, *Privacy Preserving Auctions and Mechanism Design*, Proceedings of the 1st ACM Conf. on Electronic Commerce, Nov. 1999.
97. D. Boneh and M. Naor, *Time-Commitments*. Advances in Cryptology – Crypto’2000 Proceeding, Lecture Notes in Computer Science 1880, Springer, 2000, pp. 236–254.
98. M. Naor and B. Pinkas, *Distributed Oblivious Transfer*, Advances in Cryptology – Asiacrypt’2000 Proceeding, Lecture Notes in Computer Science 1976, Springer, 2000, pp. 205–219.
99. M. Naor and B. Pinkas, *Efficient Oblivious Transfer Protocols*, Proceedings of the Twelfth Annual ACM-SIAM Symposium on Discrete Algorithms, 2001, pp. 448–457.
100. C. Dwork, S. Ravi Kumar, M. Naor and D. Sivakumar, *Rank aggregation methods for the Web*, Proceedings of the Tenth International World Wide Web Conference (WWW 10), 2001, pp. 613–622
101. D. Naor, M. Naor and J. B. Lotspiech, *Revocation and Tracing Schemes for Stateless Receivers*, Advances in Cryptology – CRYPTO 2001 Proceeding, pp. 41–62. Lecture Notes in Computer Science 2139, Springer, 2001, pp. 205–219.
102. M. Naor and V. Teague: *Anti-persistence: History Independent Data Structures*, Proc. 33rd ACM Symp. on Theory of Computing 2001, pp. 492–501.
103. M. Naor and K. Nissim, *Communication preserving protocols for secure function evaluation*, Proc. 33rd ACM Symp. on Theory of Computing 2001, pp. 590–599.
104. D. Malkhi, M. Naor and D. Ratajczak, *Viceroy: A Scalable and Dynamic Emulation of the Butterfly*, Proc. ACM PODC 2002.
105. M. Naor, *Deniable Ring Authentication*, Advances in Cryptology – CRYPTO 2002 Proceeding, Lecture Notes in Computer Science 2442, Springer, 2002, pp. 481–498.
106. M. Naor, U. Wieder, *A Simple Fault Tolerant Distributed Hash Table*, Peer-to-Peer Systems II, Second International Workshop, IPTPS 2003, Lecture Notes in Computer Science 2735, Springer, pp. 88–97.
107. M. Naor, U. Wieder, *Novel Architectures for P2P Applications: the Continuous-Discrete Approach*, Proceedings of the Fifteenth Annual ACM Symposium on Parallel Algorithms (SPAA’2003), pp. 50–59.
108. C. Dwork, A. Goldberg and M. Naor, *On Memory-Bound Functions for Fighting Spam*, Advances in Cryptology – CRYPTO 2003 Proceeding, Lecture Notes in Computer Science 2729, Springer, 2003, pp. 426–444.
109. M. Naor, *On Cryptographic Assumptions and Challenges*, invited presentation, Advances in Cryptology – CRYPTO 2003 Proceeding, Lecture Notes in Computer Science 2729, Springer, 2003, pp. 96–109.
110. M. Naor *Moderately Hard Functions: From Complexity to Spam Fighting*, invited paper, FST TCS 2003: 23rd Conference on Foundations of Software Technology and Theoretical Computer Science, Lecture Notes in Computer Science 2914, Springer, 2003, pp. 434–442.
111. M. Naor, U. Wieder, *Know thy Neighbor’s Neighbor: Better Routing for Skip-Graphs and Small Worlds*, Peer-to-Peer Systems III: Third International Workshop, IPTPS 2004, Lecture Notes in Computer Science 3279, Springer, 2005, pp. 269–277.

112. C. Dwork, M. Naor and O. Reingold, *Immunizing Encryption Schemes from Decryption Errors*, Advances in Cryptology – Eurocrypt’2004 Proceeding, Lecture Notes in Computer Science 3027, Springer, 2004, pp. 342–360.
113. G. S. Manku, M. Naor and U. Wieder, *Know thy Neighbor’s Neighbor: The Power of Lookahead in Randomized P2P Networks*, Proc. 36th ACM Symp. on Theory of Computing 2004, pp. 54–63.
114. U. Nadav and M. Naor, *Fault-Tolerant Storage in a Dynamic Environment*, Distributed Computing, 18th International Conference, DISC 2004 Proceedings, Lecture Notes in Computer Science 3274, Springer, 2004, pp. 390–404.
115. M. Naor, A. Nussbaum and E. Tromer, *Efficiently Constructible Huge Graphs that Preserve First Order Properties of Random Graphs*, second Theory of Cryptography Conference (TCC ’05), Lecture Notes in Computer Science 3378, Springer, 2005, pp. 66–85.
116. D. Harnik, J. Kilian, M. Naor, A. Rosen and O. Reingold, *On Robust Combiners for Oblivious Transfer and other Primitives*, Advances in Cryptology – Eurocrypt’2005 Proceeding, Lecture Notes in Computer Science 3494, Springer, 2005, pp. 96–113.
117. C. Dwork, M. Naor and H. Wee, *Pebbling and Proofs of Work*, Advances in Cryptology – CRYPTO 2005 Proceeding, Lecture Notes in Computer Science 3621, Springer, 2005, pp. 37–54.
118. U. Nadav and M. Naor, *The Dynamic And-Or Quorum System*, Distributed Computing, 19th International Conference, DISC 2005 Proceedings, Lecture Notes in Computer Science 3724, Springer, 2005, pp. 472–486.
119. C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov and M. Naor, *Our Data, Ourselves: Biased Coins and Privacy*, Advances in Cryptology – Eurocrypt 2006 Proceeding, Lecture Notes in Computer Science 4004, Springer, 2006, pp. 486–503.
120. T. Moran and M. Naor, *Polling with Physical Envelopes: A Rigorous Analysis of a Human-Centric Protocol*, Advances in Cryptology – Eurocrypt 2006 Proceeding, Lecture Notes in Computer Science 4004, Springer, 2006, pp. 88–108.
121. M. Naor and G. Rothblum, *Learning to Impersonate*, Proceedings of the Twenty-Third International Conference on Machine Learning (ICML 2006), June. 2006, pp. 649–656.
122. D. Harnik and M. Naor, *On Everlasting Security in the Hybrid Bounded Storage Model*, Proceedings of the 33rd International Colloquium on Automata, Languages and Programming. Lecture Notes in Computer Science 4052, Springer, 2006, pp. 192–203.
123. T. Moran and M. Naor, *Receipt-Free Universally-Verifiable Voting With Everlasting Privacy*, Advances in Cryptology – CRYPTO 2006 Proceeding, Lecture Notes in Computer Science 4117, Springer, 2006, pp. 373–392.
124. Moni Naor, Asaf Nussboim, *Implementing Huge Sparse Random Graphs*, APPROX-RANDOM 2007, Lecture Notes in Computer Science 4627, Springer, 2007, pp. 596–608.
125. Gillat Kol and Moni Naor *Cryptography and Game Theory: Designing Protocols for Exchanging Information*, Proc. 5th Theory of Cryptography Conference (TCC ’08), Lecture Notes in Computer Science, vol 4948, Springer, 2008, pp. 320–339.

126. Gillat Kol and Moni Naor, *Games for Exchanging Information*, Proc. 40th ACM Symp. on Theory of Computing 2008, pp. 423–432.
127. Ilya Mironov, Moni Naor and Gil Segev, *Sketching in Adversarial Environments*, Proc. 40th ACM Symp. on Theory of Computing 2008, pp. 651–660.
128. Moshe Babaioff, Liad Blumrosen, Moni Naor and Michael Schapira, *Informational overhead of incentive compatibility*, Proceedings of the 9th ACM conference on Electronic commerce (EC'08), July 2008, pp. 88–97.
129. Moni Naor, Gil Segev and Udi Wieder, *History-Independent Cuckoo Hashing*, Proceedings of the 35th International Colloquium on Automata, Languages and Programming (ICALP 2008), Lecture Notes in Computer Science, vol 5126, Springer, 2008, pp. 631–642.
130. Dan Boneh and Moni Naor, *Traitor Tracing with Constant Size Ciphertext*, Proceedings of the 2008 ACM Conference on Computer and Communications Security, (CCS 2008), pp. 501–510.
131. Cynthia Dwork, Guy Rothblum, Moni Naor and Vinod Vaikuntanathan, *How Efficient Can Memory Checking Be?*, Proceedings of the 6th Theory of Cryptography Conference (TCC '09), Lecture Notes in Computer Science, vol. 5444, Springer, 2009, pp. 503–520 .
132. Tal Moran, Moni Naor and Gil Segev, *An Optimally Fair Coin Toss*, Proceedings of the 6th Theory of Cryptography Conference (TCC '09), Lecture Notes in Computer Science, vol. 5444 Springer, 2009, 1–20.
133. Cynthia Dwork, Moni Naor, Guy Rothblum, Omer Reingold and Salil Vadhan, *When and How Can Data be efficiently Released with Privacy?*, Proc. 41st ACM Symp. on Theory of Computing - STOC 2009, pp. 381–390.
134. Ran Halprin, Moni Naor, *Games for extracting randomness*, Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS 2009).
135. Yuriy Arbritman, Moni Naor and Gil Segev, *De-amortized Cuckoo Hashing: Provable Worst-Case Performance and Experimental Results*, to appear, Proceedings of the 36th International Colloquium on Automata, Languages and Programming (ICALP 2009).
136. Mihir Bellare, Zvika Brakerski, Moni Naor, Thomas Ristenpart, Gil Segev, Hovav Shacham and Scott Yilek, *Hedged Public-Key Encryption: How to Protect Against Bad Randomness*, Asiacrypt 2009, Lecture Notes in Computer Science, vol. 5912 Springer, 2009, pp. 232–249.
137. Moni Naor and Gil Segev, *Public-Key Cryptosystems Resilient to Key Leakage*, CRYPTO 2009, Lecture Notes in Computer Science, vol. 5677 Springer, 2009, pp. 18–35.
138. Cynthia Dwork, Moni Naor, Toniann Pitassi, Guy N. Rothblum, and Sergey Yekhanin, *Pan-Private Streaming Algorithms*, in Proceedings of The First Symposium on Innovations in Computer Science (ICS 2010), Tsinghua University Press, January 2010.
139. Jo'el Alwen, Yevgeniy Dodis, Moni Naor, Gil Segev, Shabsi Walfish, Daniel Wichs, *Public-key encryption in the bounded-retrieval model*, EUROCRYPT 2010, Lecture Notes in Computer Science, to appear, 2010.
140. Cynthia Dwork, Moni Naor, Toniann Pitassi, and Guy N. Rothblum, *Differential Privacy Under Continual Observation*, in STOC, Association for Computing Machinery, June 2010.

Technical Reports

141. M. Naor, *Constructing Ramsey graphs from small probability spaces*, IBM Research Report RJ 8810, 1992.
142. S. Kannan, M. Naor and S. Rudich, *Anchors in Tournaments*, TR 92-08, Dept. of Computer Science, University of Arizona, 1992.
143. M. Naor and A. Shamir, *Visual Cryptography II: Improving the Contrast Via the Cover Base*, Cryptology ePrint Archive, Report 1996/007. Available: <http://eprint.iacr.org/1996/007/>
144. M. Naor, *Verification of a human in the loop or Identification via the Turing Test*, Available: http://www.wisdom.weizmann.ac.il/~naor/PAPERS/human_abs.html
145. O. Goldreich, Y. Lustig and M. Naor, *On Chosen Ciphertext Security of Multiple Encryptions* IACR's Cryptology ePrint Archive, 2002/089, available: <http://eprint.iacr.org/2002/089/>