Prof. Dalit Naor

Email: dalit.naor@mta.ac.il
Email: dalitnaor@yahoo.com
LinkedIn: Dalit Naor
Mobile: +972-54-6976-425

Summary

I am the *Dean* for the School of Computer Science at the Academic College Tel-Aviv-Yaffo and a *professor* at the school. I joined the college in 2021. Before that I was a *department general manager* of the Hybrid Cloud Department, a *manager* for storage research and a Senior Technical Staff Member (*STSM*) at IBM Research Haifa. My current areas of expertise are Cloud, Big Data and Storage. I also worked on security-related technologies, including internet security, content protection, storage security and cloud security. My past academic research includes bioinformatics and combinatorial optimization. I am teaching academic courses at universities. I am the inventor of 17 patents and the author of 37 academic papers and a book chapter, awarded an IBM Outstanding Innovation & Technical Achievement Awards (OIA, OTAA) and a People Manager of the Year Award.

Education and Academic background

- **B.A** Computer Science, 1985, Technion, Israel Ins. of Technology (*cum laude*)
- **M.Sc**. in Computer Science, 1989, University of California at Davis
  "Performance of Priority Queue Structures in a Virtual Memory Environment".
- **Ph.D.** in Computer Science, 1991, University of California at Davis
  "*The Structure of Minimum Cuts with Applications to Graph-Augmentation*". Thesis Advisor: Prof. Daniel Gusfield.
- Postdoctoral (Computational Biology), 1991-1993, Stanford University
- Postdoctoral (Computer Science), 1993-1996, Tel-Aviv University

Employment

2021-
  Dean, School of Computer Science, Tel-Aviv Yaffo Academic College

2019-2020
  Department General Manager, Hybrid Cloud, IBM Haifa Research Lab. Managing diverse activities that deliver critical components to the infrastructure and platform for clouds, focusing on enterprise mission-critical and data-intensive applications. Emphasis on open source and innovation.

2014-2019
  Senior Manager, Cloud Platforms department, IBM Haifa Research Lab. Senior manager for 40 researchers, engineers and managers. The department activities cover all aspects of Cloud Infrastructure, including Datacenter Networking, Cloud Compute, Cloud Storage, Security and Cloud Data for Analytics. Managing diverse funding sources

including IBM internal projects as well as European funded (H2020), and nurturing ties to the academic community.

2006-2014

Manager, Storage Systems Research group, IBM Haifa Research Lab. People manager of about 15 highly qualified researchers plus students, working on advanced storage systems. Selected the *People Manager of the Year*, 2012. Active in European projects, including a PI in a European FP6 research project on digital preservation (CASPAR), and an IBM-led European FP7 project on cloud Storage (VISION Cloud). Maintained academic ties and taught advanced seminars on topics related to Cloud.

2001-2006

Researcher and team leader at the Storage Systems group at IBM Haifa Lab. Worked on the definition, standardization and prototype of object storage (OSD), a new abstraction for storage devices. Developed technologies for secure storage, for encryption of data-at-rest and for access control. Developed innovative work in the area of storage support for long term digital preservation.

1999-2001

Researcher at the Content Protection group at IBM Almaden Research Center in San Jose. Co-invented, developed and deployed CPRM/CPPM, a technology for Content Protection for Recordable Media and Pre-Recorded Media for DVDs, protecting against illegal copying of content; shipped today in ATA drives and Secure Digital cards, HD-DVD and Blu-ray discs. Responsible for developing optimization algorithms for the assignment of cryptographic keys to compliant devices and other media.
http://en.wikipedia.org/wiki/Advanced_Access_Content_System

1996-1999

Researcher at IBM Haifa Research Lab. Security technologies for the Internet, including proactive security, secure signing of web forms, and trust establishment over the Web.

Current Research interest:

- Storage Systems
- Cloud
- BigData Infrastructure

Patents (Issued)

1. *Coincidence-free media key block for content protection for recordable*
   US patent 6883097
2. *Content Insurance*
   US Patent 7389247
3. *Method for broadcast encryption and key revocation of stateless receivers*
   US Patent 7039803
   US Patent 7698551 (a continuation)
   Also issued is China, Belgium, Switzerland, Germany, EP, Spain, France, UK, Ireland, Italy, Netherlands, Sweden, Hong Kong, Taiwan, Korea
4. *Method for tracing traitor receivers in a broadcast encryption system*
   US Patent 7010125
   Also issued in Germany, EP, France, UK, Taiwan
5. *Method for assigning encryption keys*
   US Patent 6888944

6. *Method for assigning encryption keys*
   US Patent 6947563
7. *Method for operating proactively secured applications on an insecure*
   US Patent 7003677
8. *Method for Ensuring Privacy in Electronic Transactions with Session Key Blocks*
   UK Patent 1593100
   Also issued in China, Germany, EP, France, UK
9. *Method for Ensuring Content Protection and Subscription Compliance*
   US Patent 7523307
10. *Method, System and Program Product for Modifying Content Usage Conditions During Content Distribution*
    US Patent 8656178
11. *Preservation Aware Fixity in Digital Preservation*
    US Patent US8046337
12. *Method of a Full Coverage Low Power Mode for Storage Systems Storing Replicated Data Items*
    US Patent 8122217
13. *Estimating Power Consumption in a Computing Environment*
    US Patent 8230238
14. *Estimation of data reduction rate in a data storage system*
    US Patent 8650163
15. *File System Object-based Deduplication*
    US Patent 8660997
16. *Efficient File System Object-Based Deduplication*
    US Patent 8706703
17. *Selective Operation Pushdowns from an Analytics Platform to Bulk Storage*
    US Patent 9569444

Standards

1. IEEE Std 1619-2007 "IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices"
   http://grouper.ieee.org/groups/1619/email/pdf00086.pdf
2. SNIA OSD working group and to the OSD T10 standard "SCSI Object-Based Storage Device Commands (OSD)", 2006
3. Content Protection for Recordable Media (CPRM)
   http://www.4centity.com/specification.aspx
   Adopted by secure digital memory cards, HD-DVD and Blu-ray Discs

Teaching Experience

- Fall 2023. *Seminar: Topics in Cloud-Based Architectures*, Academic College TA
- Fall 2022. *Advanced Storage Systems for Big Data.* Academic College TA
- Spring 2021. *Advanced topics in Storage Systems for Big Data*, Academic College TA

- Spring 2014. *Advanced Topics in Storage Systems for Big Data* at Tel-Aviv University, http://www.eng.tau.ac.il/semcom/
- Spring 2013. *Advanced Topics in Storage Systems* at Tel-Aviv University http://www.eng.tau.ac.il/semcom/2013
- 1997-8. *Internet Security* in Tel-Aviv university
- 1994. *Algorithms for Molecular Biology* in Tel-Aviv university

Awards

- Senior Technical Staff Member (STSM), IBM Research – 2014
  An *expert in advanced storage technologies, with outstanding contributions to IBM storage products*
- People Manager of the Year, IBM Haifa Research Lab - 2012
- IBM Outstanding Technical Achievement Award (OTAA) – 2012
  Impact in Content Protection Standards
- IBM Outstanding Innovation Award (OIA) – 2008
  Contributions in Content Protection
- Sixth Plateau for filing patents - 2016
- Postdoc fellow of the NSF program on Mathematic and Biology – 1991-3

Grants

- Multiple European grants since 2005, starting with FP5, FP7 and currently H2020.
- PI in projects related to Long Term Digital Presentation
  - *APERSEN, ForgetIT , Parse.Insight* and *ENSURE*
- Initiated and led *VISION Cloud*, a large-scale project on Cloud Storage.
- My department executes dozen projects at any given
  - Areas: ICT Cloud, Networking and Security

Publications

A. Cloud, Storage and Big Data

1. Too Big to Eat: Boosting Analytics Data Ingestion from Object Stores with Scoop, by Yosef Moatti, Eran Rom et al. In ICDE 2017: 309-320
2. Security intelligence for cloud management infrastructures, by Stefan Berger, et al. IBM Journal of Research and Development 60(4): 11 (2016)
3. Iostack: Software-defined object storage, by R Gracia-Tinedo et al, IEEE Internet Computing 20 (3), 10-18. (2016).
4. SDGen: Mimicking Datasets for Content Generation in Storage Benchmarks, by Raúl Gracia-Tinedo, Danny Harnik, Dalit Naor, Dmitry Sotnikov, Sivan Toledo and Aviad Zuck. In FAST 2015.
5. Estimation of deduplication ratios in large data sets, by Danny Harnik, Oded Margalit, Dalit Naor, Dmitry Sotnikov and Gil Vernik. IEEE 28th Symposium on Mass Storage Systems and Technologies (MSST) 2012: 1-11.
6. A Cloud Environment for Data-intensive Storage Services, by E.K. Kolodner et al. CloudCom 2011: 357-366.
7. Data-intensive storage services on clouds: Limitations, challenges and enablers E.K. Kolodner et al. In 2nd Workshop on Software Services: Cloud Computing and Applications based on Software Services, 2011.
8. Low Power Mode in Cloud Storage Systems, by Danny Harnik, Dalit Naor and Itai Segall, The Fifth International Workshop on System Management Techniques, Processes, and Services (SMTPS 2009), Special Focus on Cloud Computing.
9. Storage Modeling for Power Estimation, by Miriam Allalouf, Yuriy Arbitman, Michael Factor, Ronen Kat, Kalman Meth and Dalit Naor, SYSTOR 2009.
10. Authenticity and Provenance in Long Term Digital Preservation: Modeling and Implementation in Preservation Aware Storage. Michael Factor, Ealan Henis, Dalit Naor, Simona Rabinovici-Cohen, Petra Reshef, Shahar Ronen, Giovanni Michetti, Maria Guercio. Workshop on the Theory and Practice of Provenance, 2009.
11. Preservation DataStores: New storage paradigm for preservation environments. Simona Rabinovici-Cohen, Michael Factor, Dalit Naor, Leeat Ramati, Petra Reshef, Shahar Ronen, Julian Satran, David L. Giaretta. IBM Journal of Research and Development 52(4-5): 389-400 (2008).
12. Towards knowledge in the cloud. Davide Cerri et al. In OTM Confederated International Conferences "On the Move to Meaningful Internet Systems", pp. 986-995, 2008.
13. The ANSI T10 object-based storage standard and current implementations. David Nagle, Michael Factor, Sami Iren, Dalit Naor, Erik Riedel, Ohad Rodeh, Julian Satran. IBM Journal of Research and Development 52(4-5): 401-412 (2008).
14. Capability based Secure Access Control to Networked Storage Devices. Michael Factor, Dalit Naor, Eran Rom, Julian Satran, Sivan Tal. MSST 2007: 114-128.
15. Preservation datastores: Architecture for preservation aware storage. Michael Factor, Dalit Naor, Simona Rabinovici-Cohen, Leeat Ramati, Petra Reshef, Julian Satran, David L Giaretta. MSST 2007, pp. 3-15.
16. The need for preservation aware storage: a position paper. Michael Factor, Dalit Naor, Simona Rabinovici-Cohen, Leeat Ramati, Petra Reshef, Julian Satran. Operating Systems Review 41(1): 19-23 (2007)).
17. Toward Securing Untrusted Storage without Public-Key Operations. Dalit Naor, Amir Shenhav, Avishai Wool. StorageSS 2005: 51-56.

18. One-time signatures revisited: Have they become practical? Dalit Naor, Amir Shenhav, Avishai Wool. IACR Cryptol. ePrint Arch. 2005.
19. Object storage: The future building block for storage systems. Michael Factor, Kalman Meth, Dalit Naor, Ohad Rodeh, Julian Satran. MSST 2005, pp. 119-123.
20. The OSD Security Protocol. Michael Factor, David Nagle, Dalit Naor, Erik Riedel, Julian Satran. IEEE Security in Storage Workshop 2005: 29-39.
21. Towards an object store. A. Azagury et al.   MSST 2003.
22. A two-layered approach for securing an object store network. Alain Azagury, Ran Canetti, Michael Factor, Shai Halevi, Ealan Henis, Dalit Naor, Noam Rinetzky, Ohad Rodeh, Julian Satran. First International IEEE Security in Storage Workshop, 2002, pp. 10-23.

B. Content Protection and Security

23. Revocation and Tracing Schemes for Stateless Receivers. Dalit Naor, Moni Naor, Jeffery Lotspiech. CRYPTO 2001: 41-62.
24. Protecting Cryptographic Keys: The Trace-and-Revoke Approach. Dalit Naor, Moni Naor. IEEE Computer 36(7): 47-53 (2003).
25. Clock synchronization with faults and recoveries. Boaz Barak, Shai Halevi, Amir Herzberg, and Dalit Naor. PODC, pp. 133-142, 2000.
26. Access Control Meets Public Key Infrastructure, Or: Assigning Roles to Strangers. Amir Herzberg, Yosi Mass, Joris Mihaeli, Dalit Naor, Yiftach Ravid. IEEE Symposium on Security and Privacy 2000: 2-14.
27. The Proactive Security Toolkit and Applications. Boaz Barak, Amir Herzberg, Dalit Naor, Eldad Shai. ACM Conference on Computer and Communications Security 1999: 18-27.
28. Proactive Security: Long-Term Protection Against Break-Ins, Ran Canetti, Rosario Gennaro, Amir Herzberg and Dalit Naor. Cryptobytes, the technical newsletter of RSA Labs, Vol. 3, number 1 - Spring 1997.
29. Surf'N'Sign: Client Signatures on Web Documents, Amir Herzberg, Dalit Naor. IBM Systems Journal 37(1): 61-71 (1998).

C. Bioinformatics

30. Interchanges of spatially neighboring residues in structurally conserved environments. Einat Azarya-Sprinzak, Dalit Naor, Haim Wolfson and Ruth Nussinov. Protein Engineering, Vol 10. pp. 1109--1123 (1997).
31. Amino Acid Pair Interchanges at Spatially Conserved Locations. Dalit Naor, Daniel Fischer, Robert L. Jernigan, Haim J. Wolfson and Ruth Nussinov. Journal of Molecular Biology, Volume 256, Issue 5, 15 March 1996, Pages 924-938.
32. On Near-Optimal Alignments of Biological Sequences. Dalit Naor, Douglas L. Brutlag. Journal of Computational Biology 1(4): 349- (1994).
33. Parametric Optimization of Sequence Alignment. Dan Gusfield, K. Balasubramanian, Dalit Naor. Algorithmica 12(4/5): 312-326 (1994).

34. On suboptimal alignments of biological sequences. Dalit Naor, Douglas Brutlag. Annual Symposium on Combinatorial Pattern Matching, (1993).
35. A Lower Bound on the Number of Solutions to the Probed Partial Digest Problem. Lee Newberg and Dalit Naor. Advances in Applied Mathematics, 14, pp. 172-183 (1993).

D. Combinatorial Optimization

36. A Fast Algorithm for Optimally Increasing the Edge Connectivity. Dalit Naor, Dan Gusfield, Charles Martel. FOCS 1990: 698-707. Also, in SIAM J. Comput. 26(4): 1139-1165 (1997).
37. Extracting Maximal Information About Sets of Minimum Cuts. Dan Gusfield, Dalit Naor. Algorithmica 10(1): 64-89 (1993).
38. Representing and enumerating edge connectivity cuts in RNC. Dalit Naor, Vijay V Vazirani. Workshop on Algorithms and Data Structures (1991)
39. Efficient Algorithms for Generalized Cut Trees. Dan Gusfield, Dalit Naor. SODA 1990: 422-433.
40. Performance of Priority Queue Structures in a Virtual Memory Environment. Dalit Naor, Charles U. Martel, Norman S. Matloff. The Computer Journal 34(5): 428-437 (1991).

Publications in non-refereed workshops, conferences and journals

1. Data-intensive storage services on clouds: Limitations, challenges and enablers. E.K. Kolodner et al. In 2nd Workshop on Software Services: Cloud Computing and Applications based on Software Services, 2011.
2. Authenticity and Provenance in Long Term Digital Preservation: Modeling and Implementation in Preservation Aware Storage. Michael Factor, Ealan Henis, Dalit Naor, Simona Rabinovici-Cohen, Petra Reshef, Shahar Ronen, Giovanni Michetti, Maria Guercio. Workshop on the Theory and Practice of Provenance (TAPP), 2009.
3. Towards knowledge in the cloud. Davide Cerri et al. In OTM Confederated International Conferences "On the Move to Meaningful Internet Systems", pp. 986-995, 2008.
4. One-time signatures revisited: Have they become practical? Dalit Naor, Amir Shenhav, Avishai Wool. IACR Cryptol. ePrint Arch. 2005.
5. Benchmarking and Testing OSD for Correctness and Compliance. Dalit Naor, Petra Reshef, Ohad Rodeh, Allon Shafrir, Adam Wolman, Eitan Yaffe: Haifa Verification Conference 2005: pp. 158-176
6. Enforcing Confinement in Distributed Storage and a Cryptographic Model for Access Control. Shai Halevi, Paul A. Karger, Dalit Naor. IACR Cryptol. ePrint Arch. 2005: 169.
7. Revocation and Tracing Schemes for Stateless Receivers. Dalit Naor, Moni Naor and Jeffrey Lotspiech. IACR Cryptol. ePrint Arch. 2001: 59 (2001), and ECCC 043, 2002.
8. Proactive Security: Long-Term Protection Against Break-Ins, Ran Canetti, Rosario Gennaro, Amir Herzberg and Dalit Naor. Cryptobytes, the technical newsletter of RSA Labs, Vol. 3, number 1 - Spring 1997.
9. Deductive Databases for Genomic Mapping (Extended Abstract). Shalom Tsur, Frank Olken, Dalit Naor. Workshop on Deductive Databases 1990

Chapters

- Dalit Naor: *Broadcast Encryption*. In Encyclopedia of Cryptography and Security, 2005; and Encyclopedia of Cryptography and Security (2nd Ed.) 2011, pp. 171-174
- Dalit Naor, Ron Shamir: Lecture notes on "*Algorithms for Molecular Biology*", Tel Aviv University, 1994-5, the basis for lecture notes 2002, (~400 pages) http://www.cs.tau.ac.il/~rshamir/algmb.html

Editorial

- Dalit Naor, Gernot Heiser, Idit Keidar. Proceedings of the 8th ACM International Systems and Storage Conference, SYSTOR 2015, Haifa, Israel, May 26-28, 2015

Student Committees:

- Roei Kisous (M.Sc., Technion, 2022)
- Aviv Nachman (M.Sc., Technion, 2020)
- Raúl Gracia-Tinedo, (URV, Spain)
- Roye Rozov (TAU)
- Amir Shenhav (TAU)

Community Activities & Talks

FAST 2023	Conference Co-Chair
HotStorage 2023	Program Committee
FAST 2022	Program Committee
HotStorage 2022	Program Committee
FAST 2021	Program Committee
FAST 2020	Program committee
ATC 2020	External Reviewer
IISWC 2020	Program committee
Systor 2016 – today	Steering Committee Chair
Systor 2015	General Chair
Future of AI 2018	Panel speaker
IBM Interconnect 2017	Speaker
IBM Insight 2014	Speaker
TRANSISTOR 2010	Invited speaker
TRANSISTOR 2009	Invited speaker