December 17, 2014

Kobbi Nissim - Curriculum Vitae

Contact Information

Phone: 857-400-6137.
e-mail: kobbi@cs.bgu.ac.il, kobbi@seas.harvard.edu.

Research Interests

My research is towards establishing rigorous practices for computer security: identifying problems that result from the collection, sharing, and processing of information, formalizing and studying them towards establishing solid practices and technological solutions. I am particularly interested in intersection points between security and privacy and notions developed in various disciplines within and outside computer science: cryptography, machine learning, game theory, complexity, algorithms, statistics, and databases.

Highlights of Scientific Achievements

Foundations of Privacy:

- Initiated work on theoretical foundations of privacy (PODS 2003). This work received the Alberto O. Mendelzon Test-of-Time Award in 2013.
- Introduced the definition of Differential Privacy (TCC 2006).
- Introduced some of the general constructions of differentially private algorithms: Gaussian/Laplace mechanism, SuLQ framework, smooth sensitivity, sample and aggregate.
- Investigated differential privacy in conjunction with a variety of tasks: machine learning, private data release, mechanism design, and analysis of social networks.
- Since 2011, involved with the Privacy Tools project at Harvard University, developing privacy preserving tools for sharing of social-science data.

Cryptography:

- Presented theoretical work on constructing efficient secure function evaluation (SFE) protocols, including the first communication efficient protocol for Yao's Millionaires' problem (STOC 2001), a generic transformation of computation on RAM machines into SFE protocols, an efficient extension of oblivious transfer - the building block of SFE, and efficient secure protocols for set operations and linear algebra.
- Introduced the BGN cryptosystem (EUROCRYPT 2004), the first homomorphic scheme allowing the evaluating of 2-DNFs on ciphertexts without increasing the ciphertext length.
- Introduced the notions of Private Approximations (ICALP 2001) and Private Search (STOC 2006). Presented efficient private approximations of Hamming distance and some #P-complete functions. Investigated the complexity of private approximation and private search.

Education

B.Sc. EE, 1984–1987

- Dept. of Electrical Engineering, Tel-Aviv University.

M.Sc. CS, 1995–1996

- Dept. of Computer Science and Applied Math, Weizmann Institute of Science. Advisor: Prof. Uri Feige. Thesis Title: "On the Design and Use of Efficient Interactive Proofs".

Ph.D., 1997–2001

- Dept. of Computer Science and Applied Math, Weizmann Institute of Science. Advisor: Prof. Moni Naor. Thesis Title: "On the Construction of Efficient Cryptographic Protocols".

Employment History

2012–present

- Associate Professor (tenured). Department of Computer Science, Ben-Gurion University of the Negev, Israel (on leave of absence).

2012–present

- Visiting Scholar/Professor. Center for Research on Computation and Society (CRCS), Harvard University, Cambridge, Massachusetts. Participating in the *Privacy Tools for*

Sharing Research Data project, `privacytools.seas.harvard.edu/`.

2013–2014
- Visiting Research Professor. Center for Reliable Information Systems and Cyber Security (RISCS), Boston University.

2011–2012
- Visiting Senior Scientist. Cryptography and Security Group, Bar-Ilan University, Israel.

2009–2012
- Senior Lecturer (tenured since April 2009). Department of Computer Science, Ben-Gurion University of the Negev.

2009–2011
- Senior Researcher. Microsoft Audience Intelligence, Israel (while on leave from Ben-Gurion University).

2004–2009
- Lecturer. Department of Computer Science, Ben-Gurion University of the Negev.

2003–2004
- Post Doc Researcher. Microsoft Research, SVC, Mountain View, California.

2001–2002
- Post Doctoral fellow. DIMACS - Center for Discrete Mathematics Theoretical Computer Science, Rutgers University *and* NEC Research Institute (NECI).

Summer 2000
- Internship. Secure Systems Research Department, Shannon Labs, AT&T.

Summer 1998
- Internship. Secure Systems Research Department, Bell Labs, Lucent Technologies.

Professional Activities

Editorial Board

2014–present
- Editorial board, CACM Research Highlights.

2006–present
- Editor, Journal of Privacy and Confidentiality.

2008–2013
- Editorial board, Transactions on Data Privacy.

Conference and Workshop Program Committees

2016
- 35th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS '16)

2015
- The 13th International Conference on Applied Cryptography and Network Security (ACNS 2015) .
- The 16th ACM Conference on Economics and Computation (EC15).

2014
- Charles River Workshop on Private Analysis of Social Networks.
- The 5th Innovations in Theoretical Computer Science conference (ITCS '14).

2013
- Integrating Approaches to Privacy across the Research Lifecycle, Center for Research on Computation and Society, Harvard University (Member of planning committee).
- 32th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS '13) (External Review Committee).
- 16th International Conference on Database Theory (ICDT '13).

2011
- 43rd ACM Symposium on Theory of Computing (STOC '11).
- 14th International Conference on Database Theory (ICDT).

2010
- 7th Conference on Security and Cryptography for Networks (SCN).

2009
- 6th IACR Theory of Cryptography Conference (TCC).

2008
- Cryptographers' Track of the RSA Conference, CT-RSA.
- BSF-DyDAn/DIMACS Workshop on Data Privacy. Dimacs, Rutgers University (co-organizer).

2007
- 6th International Workshop on Privacy Aspects of Data Mining.
- 11th International Conference on Database Theory (ICDT '07).

2006
- Locally decodable codes, private information retrieval, privacy-preserving data-mining, and public key encryption with special properties, IPAM, UCLA.
- The 26th Annual International Cryptology Conference (CRYPTO '06).

2005
- Workshop on Privacy and Security Aspects of Data Mining, ICDM.
- The Past, Present and Future of Oblivious Transfer, The Fifth Haifa Workshop on Interdisciplinary Applications of Graph theory, Combinatorics, and Algorithms (co-organizer).
- Financial Cryptography and Data Security (FC '05).

2004
- Workshop on Privacy and Security Aspects of Data Mining, ICDM.
- DIMACS Working Group on Challenges for Cryptographers in Health Data Privacy (co-organizer).

Educational Activities

Courses Taught

Harvard University, 2014:
- Topics in cryptograph and privacy – differential privacy (with Or Sheffet, graduate level).

Ben-Gurion University, 2004–present:
- Graduate level courses: Advanced cryptography, Computational complexity, Advanced seminar, Randomized algorithms and the probabilistic method (with Amos Beimel), Privacy and secure computation (with Amos Beimel), Advanced topics in complexity and algorithms, Advanced topics in privacy and computational learning (with Aryeh Kontorovich).
- Undergraduate level courses: Automata, formal languages and computability, Topics in the frontiers of computer science for honor students, Cryptography.

Stanford University, 2004:
- A Study of perturbation techniques for data privacy (with Cynthia Dwork and Nina Mishra, graduate level).

The Open University, Israel, 1999–2001:
- Advanced algorithms (graduate level), Graph algorithms (undergraduate).

Weizmann Institute of Science, Davidson Institue of Science Education, 1999-2001:
- Coordinator of the Youth Math Circle (a.k.a. *Math by mail*).

Research Students

Renen Hallak
- M.Sc., 2007. Thesis: "Private Approximation of Clustering and Vertex Cover".

Eran Omri
- Post-doc, 2009.

Alex Kantor
- M.Sc., 2010. Thesis: "Attacks on Statistical Databases: The Highly Noisy Case".

Hai Brenner
- M.Sc., 2011. Thesis: "Differential Privacy: Universal Optimality and Bounds on PAC-Learning".

Yuval Mintz
- M.Sc, 2012. Thesis: "Information Ratios of Graph Secret-Sharing Schemes" (co-advised by Prof. Amos Beimel).

Uri Stemmer
- Ph.D. student (co-advised by Prof. Amos Beimel). Research project: "Individuals and Privacy in the Eye of Data Analysis".

Awards

2013
- Alberto O. Mendelzon Test of Time Award for the paper "Revealing Information while Preserving Privacy" (Originally published in PODS 2003).

2006
- (Runner up) PET Award for Outstanding Research in Privacy Enhancing Technologies "Calibrating Noise to Sensitivity in Private Data Analysis".

1998
- Best student paper, USENIX Security Symposium for the paper "Certificate Revocation and Certificate Update".

Scientific Publications

Authors listed in alphabetical order (except for publication [U-6]).

Original Papers in Refereed Journals

[J-1] V. Anupam, A. J. Mayer, K. Nissim, B. Pinkas, and M. K. Reiter. *On the Security of Pay-per-Click and Other Web Advertising Schemes.* Computer Networks, vol. 31, no. 11-16, pp. 1091–1100, 1999, Elsevier.

[J-2] M. Naor and K. Nissim. *Certificate Revocation and Certificate Update.* IEEE Journal on Selected Areas in Communications, vol. 18, no. 4, pp. 561–570, 2000, IEEE.

[J-3] U. Feige, R. Krauthgamer, and K. Nissim. *On cutting a few vertices from a graph.* Discrete Applied Mathematics, vol. 127, no. 3, pp. 643–649, 2003, Elsevier.

[J-4] Y. Bartal, A.J. Mayer, K. Nissim, and A. Wool. *Firmato: A Novel Firewall Management Toolkit.* ACM Transactions on Computer Systems (TOCS), vol. 22, no. 4, pp. 381–420, 2004, ACM.

[J-5] J. Feigenbaum, Y. Ishai, T. Malkin, K. Nissim, M. Strauss, and R.N. Wright. *Secure Multiparty Computation of Approximations.* ACM Transactions on Algorithms (TALG), vol. 2, no. 3, pp. 435–472, 2006, Springer.

[J-6] P. Harsha, Y. Ishai, J. Kilian, K. Nissim, and S. Venkatesh. *Communication Versus Computation.* Computational Complexity, vol. 16, no. 1, pp. 1-33, 2007, Springer.

[J-7] A. Beimel, P. Carmi, K. Nissim, and E. Weinreb. *Private Approximation of Search Problems.* Siam Journal on Computing, vol. 38, no. 5, pp. 1728–1760, 2008, SIAM.

[J-8] A. Beimel, R. Hallak, and K. Nissim. *Private Approximation of Clustering and Vertex Cover.* Computational Complexity, vol. 18, no. 3, pp. 435-494, 2009, Springer.

[J-9] A. Beimel, T. Malkin, K. Nissim, and E. Weinreb. *How should we solve search problems privately?* Journal of Cryptology, vol. 23, no. 2, pp. 344–371, 2010, Springer.

[J-10] S. Kasiviswanathan, H.K. Lee, K. Nissim, S. Raskhodnikova, and A. Smith. *What Can We Learn Privately?* Invited to FOCS 2008 special issue. Siam Journal of Computing, vol. 40, no. 3, pp. 793–826, 2011, SIAM.

[J-11] C. Hazay and K. Nissim. *Efficient Set Operations in the Presence of Malicious Adversaries.* Journal of Cryptology, vol. 25, no. 2, pp. 383-433, 2012, Springer.

[J-12] A. Kantor and K. Nissim. *Attacks on Statistical Databases: The Highly Noisy Case.* Information Processing Letters, Vol. 113, No. 12, pp. 409-413, 2013.

[J-13] K. Kenthapadi, N. Mishra, and K. Nissim. *Denials Leak Information: Simulatable Auditing.* Journal of Computer and System Sciences Vol. 79, pp. 1322–1340, 2013.

[J-14] H. Brenner, A. Beimel, S.P. Kasiviswanathan, and K. Nissim. *Bounds on the Sample Complexity for Private Learning and Private Data Release.* Journal of Machine Learning Vol. 94, No. 3, pp. 401–437, 2014.

[J-15] C. Hazay, M.J. Freedman, K. Nissim, and B. Pinkas. *Efficient Private Matching and Set Intersection.* Accepted for publication. Journal of Cryptology.

[J-16] H. Brenner and K. Nissim. *Impossibility of Differentially Private Universally Optimal Mechanisms.* SIAM Journal of Computing 43(5): 1513-1540 (2014)

[J-17] A. Beimel, K. Nissim, and U. Stemmer. *Private Learning and Sanitization: Pure vs. Approximate Differential Privacy.* Accepted for publication. Special issue of *Theory of Computing* journal dedicated to APPROX/RANDOM 2013.

Original Papers in Refereed Conference Proceedings

[C-1] M. Naor and K. Nissim. *Certificate Revocation and Certificate Update.* Proceedings of the 7th USENIX Security Symposium, 1998, pp. 217–228. Earlier version of J-2.

[C-2] Y. Bartal, A. Mayer, K. Nissim, and A. Wool. *Firmato: A novel firewall management toolkit.* Proceedings of the 1999 IEEE Symposium on Security and Privacy, pp. 17–31, 1999, IEEE. Earlier version of J-4.

[C-3] R. Canetti, T. Malkin, and K. Nissim. *Efficient Communication-Storage Tradeoffs for Multicast Encryption.* Advances in Cryptology–EUROCRYPT'99, pp. 459–474, 1999, Springer.

[C-4] U. Feige, R. Krauthgamer, and K. Nissim. *Approximating the minimum bisection size.* Proceedings of the thirty-second annual ACM symposium on Theory of computing, STOC, pp. 530–536, 2000, ACM.

[C-5] U. Feige, M. Langberg, and K. Nissim. *On the hardness of approximating NP witnesses.* Proceedings of third International Workshop Approximation Algorithms for Combinatorial Optimization, APPROX, pp. 120–131, 2000, Springer.

[C-6] J. Feigenbaum, Y. Ishai, T. Malkin, K. Nissim, M. Strauss, and R.N. Wright. *Secure Multiparty Computation of Approximations.* Proceedings of the 28th International Colloquium on Automata, Languages and Programming, ICALP, pp. 927–938, 2001, Springer. Earlier version of J-5.

[C-7] M. Naor and K. Nissim. *Communication Preserving Protocols for Secure Function Evaluation.* Proceedings of the thirty-third annual ACM symposium on Theory of computing, STOC, pp. 590–599, 2001, ACM.

[C-8] S. Halevi, E. Kushilevitz, R. Krauthgamer, and K. Nissim. *Private approximations of NP-hard functions.* Proceedings of the thirty-third annual ACM symposium on Theory of computing, STOC, pp. 550–559, 2001, ACM.

[C-9] Y. Ishai, J. Kilian, K. Nissim, and E. Petrank. *Extending Oblivious Transfer Efficiently.* Advances in Cryptology–CRYPTO 2003, pp. 145–161, 2003, Springer.

[C-10] I. Dinur and K. Nissim. *Revealing Information while Preserving Privacy.* Proceedings of the twenty-second ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems, pp. 202–210, 2003, ACM. Receiver of the ACM PODS Alberto O. Mendelzon Test-of-Time Award, PODS, 2013.

[C-11] P. Harsha, Y. Ishai, J. Kilian, K. Nissim, and S. Venkatesh. *Communication Versus Computation.* Proceedings of the 31st International Colloquium on Automata, Languages and Programming, ICALP, pp. 745–756, 2004. Earlier version of J-6.

[C-12] M.J. Freedman, K. Nissim, B. Pinkas. *Efficient Private Matching and Set Intersection.* Advances in Cryptology–EUROCRYPT 2004, pp. 1–19, 2004, Springer. Earlier version of J-15.

[C-13] C. Dwork and K. Nissim. *Privacy-Preserving Datamining on Vertically Partitioned Databases.* Advances in Cryptology–CRYPTO 2004, pp. 134–138, 2004, Springer.

[C-14] D. Boneh, E. Goh, and K. Nissim. *Evaluating 2-DNF Formulas on Ciphertexts.* Theory of Cryptography, TCC, pp. 325–341, 2005, Springer.

[C-15] K. Kenthapadi, N. Mishra, and K. Nissim. *Simulatable Auditing.* Proceedings of the twenty-fourth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems, PODS, pp. 118–127, 2005, ACM. Earlier version of J-13.

[C-16] A. Blum, C. Dwork, F. McSherry, and K. Nissim. *Practical Privacy: The SuLQ Framework.* Proceedings of the twenty-fourth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems, PODS, pp. 128–138, 2005, ACM.

[C-17] K. Nissim and R. Zivan. *Secure DisCSP Protocols - From Centralized Towards Distributed Solutions.* Proceedings of the 6th Distributed Constraint Reasoning (DCR), 2005.

[C-18] C. Dwork, F. McSherry, K. Nissim, and A. Smith. *Calibrating Noise to Sensitivity in Private Data Analysis.* Theory of Cryptography, TCC, pp. 265–284, 2006.

[C-19] K. Nissim and E. Weinreb. *Communication Efficient Secure Linear Algebra.* Theory of Cryptography, TCC, pp. 522–541, 2006.

[C-20] A. Beimel, P. Carmi, K. Nissim, and E. Weinreb. *Private Approximation of Search Problems.* Proceedings of the thirty-eighth annual ACM symposium on Theory of computing, STOC, pp. 119–128, 2006, ACM. Earlier version of J-7.

[C-21] I. Mironov, A. Mityagin, and K. Nissim. *Hard Instances of the Constrained Discrete Logarithm Problem.* Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS-VII, pp. 582–598, 2006, Springer.

[C-22] A. Beimel, R. Hallak, and K. Nissim. *Private Approximation of Clustering and Vertex Cover.* Proceedings of the 4th Theory of Cryptography Conference, TCC, pp. 383–403 ,2007, Springer. Earlier version of J-8.

[C-23] K. Nissim, S. Raskhodnikova, and Adam Smith. *Smooth Sensitivity and Sampling in Private Data Analysis.* roceedings of the 39th Annual ACM Symposium on Theory of Computing, STOC, pp. 75–84, 2007, ACM.

[C-24] A. Beimel, T. Malkin, K. Nissim, and E. Weinreb. *How Should We Solve Search Problems Privately?* Advances in Cryptology–CRYPTO 2007, pp. 31–49, 2007, Springer. Earlier version of J-9 .

[C-25] A. Beimel, K. Nissim, and E. Omri. *Distributed Private Data Analysis: Simultaneously Solving How and What.* Advances in Cryptology–CRYPTO 2008, pp. 451–468, 2008, Springer.

[C-26] S. P. Kasiviswanathan, H. K. Lee, K. Nissim, S. Raskhodnikova, and A. Smith. *What Can We Learn Privately?* IEEE 49th Annual IEEE Symposium on Foundations of Computer Science, FOCS'08, pp. 531–540, 2008, IEEE. Earlier version of J-10.

[C-27] D. Feldman, A. Fiat, H. Kaplan, and K. Nissim. *Private Coresets.* Proceedings of the 41st annual ACM symposium on Theory of computing, STOC, pp. 361–370, 2009, ACM.

[C-28] A. Beimel, S. P. Kasiviswanathan, and K. Nissim. *Bounds on the Sample Complexity for Private Learning and Private Data Release.* Theory of Cryptography, TCC, pp. 437–454, 2010, Springer. Earlier version of J-14.

[C-29] C. Hazay and K. Nissim. *Efficient Set Operations in the Presence of Malicious Adversaries.* Public Key Cryptography–PKC 2010, pp. 312–331, 2010, Springer. Earlier version of J-11.

[C-30] H. Brenner and K. Nissim. *Impossibility of Differentially Private Universally Optimal Mechanisms.* 51st Annual IEEE Symposium on Foundations of Computer Science (FOCS), pp. 71–80, 2010, IEEE. Earlier version of J-16.

[C-31] K. Nissim, R. Smorodinsky, and M. Tennenholtz. *Approximately Optimal Mechanism Design via Differential Privacy.* Innovations of Theoretical Computer Science (ITCS), pp. 203–213, 2012.

[C-32] K. Nissim, C. Orlandi, and R. Smorodinsky. *Privacy-Aware Mechanism Design.* ACM Conference on Electronic Commerce (EC), pp. 774–789A, 2012.

[C-33] A. Beimel, K. Nissim, and U. Stemmer. *Characterizing the Sample Complexity of Private Learners.* Innovations of Theoretical Computer Science (ITCS) 2013, pp. 97–110.

[C-34] S. Kasiviswanathan, K. Nissim, S. Raskhodnikova, and A. Smith. *Analyzing Graphs with Node Differential Privacy.* Theory of Crptography Conference (TCC) 2013, pp. 457–476.

[C-35] A. Beimel, K. Nissim, and U. Stemmer. *Private Learning and Sanitization: Pure vs. Approximate Differential Privacy.* Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (RANDOM) 2013, pp. 363–378. Earlier version of J-17. Invited to the special issue of *Theory of Computing* journal dedicated to APPROX/RANDOM 2013.

[C-36] Y. Lindell, K. Nissim, and C. Orlandi. *Hiding the Input-Size in Secure Two-Party Computation.* Advances in Cryptology (ASIACRYPT) 2013, pp. 421–440.

[C-37] K. Nissim, S. Vadhan, and D. Xiao. *Redrawing the Boundaries on Purchasing Data from Privacy-Sensitive Individuals.* Innovations in Theoretical Computer Science (ITCS) 2014, pp. 411–422.

[C-38] A. Beimel, K. Nissim, and U. Stemmer. *Learning Privately with Labeled and Unlabeled Examples.* Accepted for publication, SODA 2015.

[C-39] Y. Chen, K. Nissim, and B. Waggoner. *Fair Information Sharing for Treasure Hunting.* Accepted for publication, AAAI 2015.

Invited Book Chapters

[B-1] K. Nissim. *Private Data Analysis via Output Perturbation.* In Privacy-Preserving Data Mining: Models and Algorithms. Editors: C. Aggarwal and Philip Yu. pp. 383-413, 2008.

Patents

[P-1] M. Naor and K. Nissim. *Method for authentication item.* US Patent no. 6226743, 2001.

[P-2] C. Dwork, K. Nissim. *Preserving privacy when statistically analyzing a large database.* US Patent no. 7653615, 2010.

[P-3] A. Blum, C. Dwork, F. McSherry, and K. Nissim. *Private clustering and statistical queries while analyzing a large database.* US Patent no. 7676454, 2010.

[P-4] A. Mityagin, I. Mironov, and K. Nissim. *Systems and methods for generating random addition chains.* US Patent no. 7657029, 2010.

Unrefereed Publications

[U-1] U. Feige and K. Nissim. *On the use of interactive proofs for formal program verification*, 1997.

[U-2] C. Dwork, M. Langberg, M. Naor, K. Nissim, O. Reingold. *Succinct proofs for NP and spooky interactions*, circa 2000.

[U-3] N. Mishra and K. Nissim. *How Auditors May Inadvertently Compromise Your Privacy.* PORTIA Workshop on Sensitive Data in Medical, Financial, and Content-Distribution Systems, Stanford University, July 8-9, 2004.

[U-4] C. Dwork, F. McSherry, K. Nissim, and A. Smith. *Differential privacy – a primer for the perplexed.* Joint United Nations Economic Commission for Europe (UN-ECE)/Statistical Office of the European Union (EUROSTAT) work session on statistical data confidentiality. Topic (iv): Balancing data quality and data confidentiality, 2011.

[U-5] K. Nissim. *Differential Privacy.* MIT Big Data initiative at CSAIL, Member Workshop #2: Big Data Privacy, Exploring the Future Role of Technology in Protecting Privacy, June 19th, 2013.

[U-6] A. Wood, D. O'Brien, M. Altman, A. Karr, U. Gasser, M. Bar-Sinai, K. Nissim, J. Ullman, S. Vadhan, and M. J. Wojcik. *Integrating Approaches to Privacy across the Research Lifecycle: Long-term Longitudinal Studies.* Berkman Center Research Publication, 2014.

In Preparation/Submission

[IP-1] K. Nissim, S. Vadhan, and D. Xiao. *Individualized Differential Privacy.*

[IP-2] S. Kemara, G. Kollios, K. Nissim, and X. Meng. *GRECS: Graph Encryption for Approximate Shortest Distance Queries.*

[IP-3] K. Nissim, R. Smorodinsky, and M. Tennenholtz. *Segmentation.*

[IP-4] M. Bar-Sinai and K. Nissim *What is Replicability? From Repeatability to Extensibility.*

[IP-5] M. Bun, K. Nissim, U. Stemmer, and S. Vadhan. *Differentially Private Release and Learning of Threshold Functions.*

Research Grants

Privacy Aware Mechanism Design.

- One-year research award from the Sapir Center for Development, Tel-Aviv University. With Rann Smorodinsky, the Technion. 2012–2013. NIS48,000.

Privacy, Equilibrium, and Markets.

- Israel Science Foundation (ISF) grant 2761/12. With Rann Smorodinsky, the Technion. 4 years starting 2012.

Privacy in Mechanism Design.

- One-year research award from the Sapir Center for Development, Tel-Aviv University. With Rann Smorodinsky, the Technion. 2011-2012. NIS48,000.

Towards Foundations for Data Privacy.

- Israel Science Foundation (ISF) grant 860/06. With Benny Pinkas, Haifa University. 4 years (2006–2011). $75,000/year.

Interdisciplinary Workshop on Data Privacy.

- BSF supported workshop. With Benny Pinkas and Rebecca Wright. 3 out of 63 proposals approved. 2007. $30,000

Mentions in Media

- *Israel's 'anonymous' statistics surveys aren't so anonymous.* Amitai Ziv, Haaretz-TheMarker, TechNation, Jan 7th, 2013.