Gilad Asharov

(Last update: September 6, 2022)

Personal Information

Email: Gilad.Asharov@biu.ac.il

Links: [DBLP], [Google Scholar], [Personal Webpage]

Current Position

10/2019 – current **Senior Lecturer**, (aka Assistant Professor), tenure-track, *Bar-Ilan University*

My research concentrates in the field of cryptography, mainly focusing on secure multiparty computation, and privacy-preserving technology . I am also interested in various cryptographic primitives and their interplay: e.g., zero-knowledge proofs, oblivious RAMs, fully-homomorphic encryptions, obfuscations.

Education

2009 – 2014 **Ph.D. in Computer Science**, *Bar-Ilan University*
Field of Research: Cryptography
Thesis Title: Foundations of Secure Computation: Perfect Security and Fairness
Advisor: Prof. Yehuda Lindell
(Thesis submitted: 2014, diploma granted: June 2015.)

2008 – 2009 **M.Sc. in Computer Science,** *Bar-Ilan University*
Advisor: Prof. Yehuda Lindell
summa cum laude

Employment History

07/2020 – 07/2021 **Consultant**, *J.P. Morgan AI Research, NY*
01/2019 – 10/2019 **Vice-President, Cryptography Research Lead**, *J.P. Morgan AI Research, NY*
2015 – 2018 **Postdoctoral Researcher:**
(2017-2018) • *Cornell Tech, NY*. **Simons Foundation Junior Fellow**. Hosted by Rafael Pass
(2016) • *IBM TJ Watson Research Center, NY*, hosted by Tal Rabin
(2015) • *Hebrew University*. **ICORE-algo Fellow**. Hosted by Gil Segev
Summer 2011 **Summer Internship**, *IBM TJ Watson Research Center, Hawthorne, NY*
2005 – 2009 **Software Engineer**, *Mentor Graphics Inc., Israel*

Grants and Fellowships

2022 **JP Morgan Faculty Research Award**.
“FinSec: Secure Analytics over Financial Data". Co-PI: Arpita Patra (IISC, Bangalore)
($110,000, my portion: $55,000)

2021 **JP Morgan Faculty Research Award**,
“Scaling Secure Computation for Data Centers". Co-PI: Ilan Komargodski (Hebrew University)
($90,000; my portion: $45,000)

2020 – 2024 **Israel Science Foundation (ISF): Personal Research Grant**,
“Fundamentals of Oblivious Computation". Including funds for international collaboration and equipment for establishing a lab as a new faculty.
956,000 NIS ($\approx$ $278,000)

2020 – 2024	**Marie Skłodowska-Curie: Individual Fellowship**, *European Commission (Horizon 2020)* "PRIMAL: Private Machine Learning". Reintegration panel (personal grant) ($\approx$€185,000, approximately $\approx$ \$203,000)
2016–2019	**Simons Society of Fellows: Junior Fellow**, The Simons Foundation, NY $\approx$389,000\$ awarded to Cornell University. (https://www.simonsfoundation.org/team/gilad-asharov/)
2014	**ICORE-algo Fellowship**, The Israeli Center of Research Excellence in Algorithms
2010 – 2013	**President's Scholarship for Excellent Ph.D. Students**, *Bar-Ilan University*

Awards and Recognization

2017	**1st Place – iDash Genomic Data Privacy and Security Protection Competition** Track 1: De-duplication for Global Alliance for Genomic Health (GA4GH) (with: Fabrice Benhamouda, Chitchanok Chuengsatiansup, Benny Pinkas, and Tal Rabin)
2016	**1st Place – iDash Genomic Data Privacy and Security Protection Competition** Track 2: Privacy-Preserving Search of Similar Cancer Patients across Organizations (with: Shai Halevi, Shalev Keren, Meital Levy, Yehuda Lindell, and Tal Rabin)
	Excellence Awards, *Bar-Ilan University*
2011	• **Ph.D.:** Rector's Prize for Outstanding Ph.D. Students
2009	• **M.Sc.:** Dean's Outstanding Research Students Award
2002 – 2004	• **B.Sc.:** Dean's Undergraduate List of Excellence

Students

Current: *Bar-Ilan University*

- Yehuda Michelson (M.Sc., expected to graduate, September 2023)
- Oren Shochat (M.Sc., expected to graduate, September 2022)
- Hadar Kaner (M.Sc., expected to graduate, Setpember 2022)

Teaching Activities

All in the Department of Computer Science, Bar-Ilan University:

Fall 2019, 2020, 2021	**Lecturer**, Introduction to Cryptography (89-656)
Spring 2020, 2022	**Instructor**, Advances in Cryptography
2019 – 2021	**Organizer** of the Cyber Center Colloquium, Bar-Ilan University
Spring 2021	**Lecturer**, Discrete Math 2 (89-197)
Spring 2010-2015	**Teaching Assistant**, Data Structure (89-120)

Organization of Scientific Meetings

Workshop Organization:

2022	**Co-Organizer** of Privacy-Preserving Machine Learning Workshop. Affiliated events of CRYPTO 2022 (with Polychroniadou and Ostrovsky), hybrid.
2021	**Co-Organizer** of Privacy-Preserving Machine Learning Workshop. Affiliated events of CRYPTO 2021 (with Polychroniadou and Ostrovsky), virtual.
2020	**Co-Organizer** of Privacy-Preserving Machine Learning Workshop. Affiliated events of CRYPTO 2020 (with Polychroniadou and Ostrovsky), virtual.
2019	**Co-Organizer** of Privacy-Preserving Machine Learning Workshop. Affiliated events of CRYPTO 2019 (with Polychroniadou and Ostrovsky), University of California, Santa Barbara.

Program Committee Member:

- TCC 2022 - Theory of Cryptography Conference
- ITC 2022 - Information Theoretic Cryptography

- TCC 2021 - Theory of Cryptography Conference
- ITC 2021 - Information Theoretic Cryptography
- ICAIF 2020 - The 1st ACM International Conference on AI in Finance.
- SCN 2020 - Conference on Security and Cryptography for Networks.
- PKC 2020 - The IACR International Conference on Practice and Theory of Public-Key Cryptography.
- TCC 2019 - Theory of Cryptography Conference
- TCC 2018 - Theory of Cryptography Conference
- EUROCRYPT 2017 - The Annual International Conference on the Theory and Applications of Cryptographic Techniques.
- SCN 2016 - Conference on Security and Cryptography for Networks

Program Committee Member - Workshops:

- CSCML 2022 - International Symposium on Cyber Security Cryptology and Machine Learning
- CSCML 2020 - International Symposium on Cyber Security Cryptology and Machine Learning
- FCS 2019 - Foundations of Computer Security Workshop
- GenoPri 2017 - The 4th International Workshop on Genome Privacy and Security

Institutional Responsibilities

Department of Computer Science, Bar-Ilan University

2021-2022	**Academic advisor** for 2nd year undergraduate students
202-2022	**Member** of the department's committee for graduate studies

Reviewing Activities

Journal Refereeing: SIAM Journal of Computing, ACM Computing Surveys, Journal of Cryptology, Journal of Computer and System Sciences, Distributed Computing, Journal of Cloud Computing, Journal of Mathematical Cryptology, Journal of Applied Mathematics, Theoretical Computer Science.

Conference Refereeing: External Reviewer
CRYPTO ('10,'11,'12,'13,'14,'15,'16,'17,'18,'19), *TCC* (12',13',15',16',17'), *Eurocrypt* (13',15',16,'18,'19,'20), *STOC* ('14,'16,'19,'20), *SODA* ('20,'21,'23), *FOCS* ('19), *ACM-CCS* ('14,'16,'19,'20), *ITCS* ('19,'21), *DISC* ('14, '15), *Financial Crypto* ('15), *SCN* ('12,'14), *ICITS* ('11,'12), *Asiacrypt* ('13,'20), *ESORICS* ('13), *PKC* ('13,19'), *Inscrypt* ('12), *CANS* ('12), *ICALP* ('12,'18,'19), *CT-RSA* ('11).
PhD Theses reviewer: Bar-Ilan University , Hebrew University
MSc Theses reviewer: Reichman University, Israel
Grants applications reviewer: Israel Science Foundation, European Research Council Consolidator grant

Membership of Scientific Societies

2009 – current	**Member** of International Association of Cryptologic Research	IACR
2017 – current	**Member** of the Association of Computing Machinery	ACM

Publications

Next to each publication we report [R], where R is the rank of the conference/journal according to CORE ranking (conferences and journals) — A*, A, B and C.
A (relatively new) conference that has no CORE ranking is reported with the symbol "X".

Journal Publications

15. Gilad Asharov, Ilan Komargodski, Wei-Kai Lin, Kartik Nayak, Enoch Peserico, Elaine Shi:
OptORAMa: Optimal Oblivious RAM
Journal of the ACM, (accepted) [A*]

14. Ittai Abraham, Gilad Asharov and Avishay Yanai:
Efficient Perfectly Secure Computation with Optimal Resilience
Journal of Cryptology, (accepted) [A*]

13. Gilad Asharov, Naomi Ephraim, Ilan Komargodski and Rafael Pass:
On the Complexity of Compressing Obfuscation
Journal of Cryptology, (accepted) [A*]

12. Gilad Asharov, Hubert Chan, Kartik Nayak, Rafael Pass, Ling Ren and Elaine Shi:
Locality-Preserving Oblivious RAM
Journal of Cryptology 35(2): 6, 2022 [A*]

11. Gilad Asharov, Wei-Kai Lin and Elaine Shi:
Sorting Short Keys in Circuits of Size $o(n \log n)$
SIAM Journal of Computing, 51(3): 424-466, 2022 [A*]

10. Gilad Asharov, Gil Segev and Ido Shahaf:
Tight Tradeoffs in Searchable Symmetric Encryption
Journal of Cryptology, 34(2):9, 2021 [A*]

9. Gilad Asharov, Moni Naor, Gil Segev and Ido Shahaf:
Searchable Symmetric Encryption:
Optimal Locality in Linear Space via Two-Dimensional Balanced Allocations
SIAM Journal of Computing 50(5): 1501-1536, 2021 [A*]

8. Gilad Asharov, Shai Halevi, Yehuda Lindell and Tal Rabin:
Privacy-Preserving Search of Similar Patients in Genomic Data
Proceedings of Privacy Enhanced Technologies (PoPETS) 2018.4: 104-124, 2018 [A]

7. Gilad Asharov and Gil Segev:
On Constructing One-Way Permutations from Indistinguishability Obfuscation
Journal of Cryptology 31(3): 698-736, 2018 [A*]

6. Gilad Asharov, Daniel Demmler, Michael Schapira, Thomas Schneider,
Gil Segev, Scott Shenker and Michael Zohner:
Privacy-Preserving Interdomain Routing at Internet Scale
Proceedings of Privacy Enhanced Technologies (PoPETS) 2017.3: 147-167, 2017 [A]

5. Gilad Asharov, Yehuda Lindell, Thomas Schneider and Michael Zohner:
More Efficient Oblivious Transfer Extensions
Journal of Cryptology 30(3), 805-858, 2017 [A*]

4. Gilad Asharov and Yehuda Lindell:
A Full Proof of the BGW Protocol for Perfectly-Secure Multiparty Computation
Journal of Cryptology 30(1), 58-151, 2017 [A*]

3. Gilad Asharov and Gil Segev:
Limits on the Power of Indistinguishability Obfuscation and Functional Encryption
SIAM Journal of Computing 45(6): 2117-2176, 2016 [A*]

2. Gilad Asharov, Ran Canetti and Carmit Hazay:
Towards a Game Theoretic View of Secure Computation
Journal of Cryptology 29(4): 879-926, 2016 [A*]

1. Gilad Asharov and Yehuda Lindell:
Utility Dependence in Correct and Fair Rational Secret Sharing
Journal of Cryptology 24(1), 157–202, 2011 [A*]

Publications in Highly Refereed Conferences

34. Ittai Abraham, Gilad Asharov, Shravani Patil, Arpita Patra:
Asymptotically Free Broadcast in Constant Expected Time via Packed VSS
TCC 2022 [A]

33. Gilad Asharov, Koki Hamada, Dai Ikarashi, Ryo Kikuchi, Ariel Nof, Benny Pinkas, Katsumi Takahashi, Junichi Tomida:
Efficient Secure Three-Party Sorting with Applications to Data Analysis and Heavy Hitters
ACM CCS 2022 [A*]

32. Ittai Abraham, Gilad Asharov:
Gradecast in Synchrony and Reliable Broadcast in Asynchrony with Optimal Resilience, Efficiency, and Unconditional Security
PODC 2022 [A*]

31. Gilad Asharov, Elaine Shi, Ke Wu:
A Complete Characterization of Game-Theoretically Fair, Multi-Party Coin Toss
EUROCRYPT 2022 [A*]

30. Gilad Asharov, Ran Cohen, Oren Shochat:
Static vs. Adaptive in Perfect MPC: A Separation and the Adaptive Security of BGW
ITC – Information Theoretic Cryptography 2022 [X]

29. Gilad Asharov, Ilan Komargodski, Wei-Kai Lin, Elaine Shi:
Optimal Oblivious Parallel RAM
SODA 2022: 2459-2521 [A*]

28. Gilad Asharov, Ilan Komargodski, Wei-Kai Lin, Elaine Shi:
Oblivious RAM with Worst-Case Logarithmic Overhead
CRYPTO 2021: (4) 610-640 [A*]

27. Prabhanjan Ananth, Gilad Asharov, Hila Dahari, Vipul Goyal:
Towards Accountability in CRS Generation
EUROCRYPT 2021: (3): 278-308 [A*]

26. Gilad Asharov, Wei-Kai Lin, Elaine Shi:
Sorting Short Keys in Circuits of Size $o(nlogn)$
SODA 2021: 2249-2268 [A*]

25. Ittai Abraham, Gilad Asharov, Avishay Yanai:
Efficient Perfectly Secure Computation with Optimal Resilience
TCC 2021: (2) 2021: 66-96 [A]

24. Gilad Asharov, Tucker Balch, Antigoni Polychroniadou:
Privacy-Preserving Portfolio Pricing
ICAIF 2021 - ACM International Conference on AI in Finance: (accepted) [X]

23. Gilad Asharov, Ilan Komargodski, Wei-Kai Lin, Kartik Nayak, Enoch Peserico, Elaine Shi:
OptORAMa: Optimal Oblivious RAM
EUROCRYPT 2020: (2) 403-432 [A*]

22. Gilad Asharov, Ilan Komargodski, Wei-Kai Lin, Enoch Peserico, Elaine Shi:
Oblivious Parallel Tight Compaction
ITC - Information Theoretic Cryptography 2020, 11:1-11:23 [X]

21. Gilad Asharov, Tucker Hybinette Balch, Antigoni Polychroniadou, Manuela Veloso:
Privacy-Preserving Dark Pools
AAMAS 2020 (extended abstract): 1747-1749 [A*]

20. Gilad Asharov, T.-H. Hubert Chan, Kartik Nayak, Rafael Pass, Ling Ren, Elaine Shi:
Bucket Oblivious Sort: An Extremely Simple Oblivious Sort
SOSA 2020: 8-14 [X]

19. Gilad Asharov, Hubert Chan, Kartik Nayak, Rafael Pass, Ling Ren and Elaine Shi:
Locality-Preserving Oblivious RAM
EUROCRYPT 2019: 214-243 [A*]

18. Liang Wang, Gilad Asharov, Rafael Pass, Abhi Shelat and Thomas Ristenpart:
Blind Certificate Authorities
IEEE Security & Privacy 2019: 107-124 [A*]

17. Gilad Asharov, Naomi Ephraim, Ilan Komargodski and Rafael Pass:
On the Complexity of Compressing Obfuscation
CRYPTO 2018: 407-436 [A*]

16. Gilad Asharov, Gil Segev and Ido Shahaf:
Tight Tradeoffs in Searchable Symmetric Encryption
CRYPTO 2018: 753-783 [A*]

15. Gilad Asharov, Francesco Bonchi, David Garcia-Soriano and Tamir Tassa:
Secure Centrality Computation Over Multiple Networks
WWW 2017: 957-966 [A*]

14. Gilad Asharov, Moni Naor, Gil Segev and Ido Shahaf:
Searchable Symmetric Encryption: Optimal Locality in Linear Space via Two-Dimensional Balanced Allocations
STOC 2016: 1101-1114 [A*]

13. Gilad Asharov and Gil Segev:
On Constructing One-Way Permutations from Indistinguishability Obfuscation
TCC 2016-A: 512–541 [A]

12. Gilad Asharov and Gil Segev:
Limits on the Power of Indistinguishability Obfuscation and Functional Encryption
FOCS 2015, 191–209 [A*]

11. Gilad Asharov, Yehuda Lindell, Thomas Schneider and Michael Zohner:
More Efficient Oblivious Transfer Extensions with Security for Malicious Adversaries
EUROCRYPT 2015, 673–701 [A*]

10. Gilad Asharov, Amos Beimel, Nikolaos Makriyannis and Eran Omri:
Complete Characterization of Fairness in Secure Two-Party Computation of Boolean Functions
TCC 2015, 199–228 [A]

9. Gilad Asharov:
Towards Characterizing Complete Fairness in Secure Two-Party Computation
TCC 2014: 291–316 [A]

8. Gilad Asharov, Yehuda Lindell, Thomas Schneider and Michael Zohner:
More Efficient Oblivious Transfer and Extensions for Faster Secure Computation
ACM CCS 2013, 535–548 [A*]

7. Gilad Asharov, Yehuda Lindell and Hila Zarosim:
Fair and Efficient Secure Multiparty Computation with Reputation Systems
ASIACRYPT 2013, 201-220 [A]

6. Gilad Asharov, Yehuda Lindell and Tal Rabin:
A Full Characterization of Functions that Imply Fair Coin Tossing and Ramifications to Fairness
TCC 2013, 243-262 [A]

5. Gilad Asharov and Claudio Orlandi:
Calling Out Cheaters: Covert Security With Public Verifiability
ASIACRYPT 2012, 681-698 [A]

4. Gilad Asharov, Abhishek Jain, Adriana López-Alt, Eran Tromer, Vinod Vaikuntanathan and Daniel Wichs:
Multiparty Computation with Low Communication, Computation and Interaction via Threshold FHE
EUROCRYPT 2012: 483–501 [A*]

3. Gilad Asharov, Yehuda Lindell and Tal Rabin:
Perfectly-Secure Multiplication for any t $<$ n/3
CRYPTO 2011, 240–258 [A*]

2. Gilad Asharov, Ran Canetti and Carmit Hazay:
Towards a Game Theoretic View of Secure Computation
EUROCRYPT 2011, 426–445 [A*]

1. Gilad Asharov and Yehuda Lindell:
Utility Dependence in Correct and Fair Rational Secret Sharing
CRYPTO 2009, 559–576 [A*]

Book Chapters

1. Gilad Asharov and Yehuda Lindell:
The BGW Protocol for Perfectly-Secure Multiparty Computation
Secure Multi-Party Computation, IOS Press 2013, 120-167

Manuscripts

1. Gilad Asharov, Naomi Ephraim, Ilan Komargodski, Rafael Pass:
On Perfect Correctness without Derandomization
IACR ePrint 2019: 1025

Others

John Pavlus:
Seeking the Limits of Encryption: Q&A with Gilad Asharov.
Simons Foundation, https://www.simonsfoundation.org/2019/05/17/seeking-the-limits-of-encryption/.

Talks

Some of the talks were filmed and are available online. The PDF document provides links.

Tutorials:

- **Oblivious Computation (ORAM):**
As part of The 12th Bar-Ilan Winter School (2022) – Advanced in Secure Computation:
  1. Part I: Introduction to ORAM, lower bounds and tree-based ORAMs.
  2. Part II: Oblivious sorts, Oblivious compaction, and sorting circuits.
  3. Part III: Hierarchical Framework and OptORAMa.
- **Secret sharing, verifiable secret sharing and the BGW protocol:**
As part of the The 10th Bar-Ilan Winter School (2020) — Information Theoretic Cryptography.
  1. Part I: Threshold secret sharing (an introduction to secret sharing).
  2. Part II: Verifiable secret sharing.
  3. Part III: Secure computation: The BGW protocol.

Talks in conferences, workshops and seminars:

- **Static vs. Adaptive in Perfect MPC: A Separation and the Adaptive Security of BGW:**

1. ITC 2022 – MIT, Cambridge, MA. July, 2022 (in person). [video]

- **Efficient Perfectly Secure Computation with Optimal Resilience:**
  1. TCC 2021 (virtual) [video]
  2. A series of online talks in China, Shanghai key laboratory for privacy-preserving computation, November, 2021. [video]
  3. CMU crypto seminar. April, 2021 (Virtual).
- **Oblivious RAM with Worst-Case Logarithmic Overhead:**
  1. Crypto 2021 (virtual). [video]
- **Optimal Oblivious Parallel RAM:**
  1. TPMPC 2020: Theory and Practice of Multi-Party Computation Workshop, Aarhus university, Denmark. (Virtual) May, 2020. [video]
- **Sorting Short Keys in Circuits of Size $o(n \log n)$:**
  1. Hebrew University Theory Seminar, May 2021.
- **OptORAMa: Optimal Oblivious RAM**
  1. Eurocrypt 2020, virtual, May 2020. [video,online session]
  2. GTACS: Greater Tel-Aviv Area Cryptography Seminar, IDC Hertzeliya, Israel. October 2019.
  3. Charles River cryptoday, MIT. March, 2019.
  4. NYC Crypto cryptoday, January 2019.
  5. Washington D.C. area cryptoday, University of Maryland, College Park. December 2018.
- **Oblivious Computation with Data Locality**
  1. Invited speaker at TPMPC 2018 - Theory and Practice of Multi-Party Computation Workshop. Aarhus university, Denmark, May 2018. [video]
  2. IBM TJ Watson Research Center, NY. July, 2017.
  3. DIMACS Workshop on Outsourcing Computation Securely, Rutgers University, NJ. July, 2017.
- **Privacy-Preserving Search of Similar Patients in Genomic Data**
  1. *Real-World Crypto*, Zurich, Switzerland. January, 2018.
  2. *NYC Crypto Day*, Columbia University, NY, February 2017.
  3. *iDash Genomic Data Privacy and Security Workshop*, Chicago, November 2016. [video]
- **Searchable Symmetric Encryption: Optimal Locality in Linear Space via Two-Dimensional Balanced Allocations**
  1. *Crypto Breakfast*, Cornell Tech, NYC, September 2016.
  2. *DIMACS Workshop on Cryptography for the RAM Model of Computation, MIT*, Cambridge, MA. June, 2016.
- **On Constructing One-Way Permutations from Indistinguishability Obfuscation.**
  1. *NYC Crypto Day*, NYU. January, 2016.
  2. *TCC 2016A*, Tel-Aviv. January, 2016.[video]
  3. *IBM Research Cryptography Seminar*, NY. December, 2015.
  4. *GTACS - The Greater Tel-Aviv Area Cryptography Symposium*. IDC, Herzeliya. November, 2015.
- **Limits on the Power of Indistinguishability Obfuscation and Functional Encryption**
  1. FOCS 2015 – UC Berkeley, October, 2015. [video]
  2. GTACS - The Greater Tel-Aviv Area Cryptography Symposium. Bar-Ilan University, May, 2015.
- **Complete Characterization of Fairness in Secure Two-Party Computation of Boolean Functions.**
  1. Cryptography meeting, the Weizmann institute of science. May, 2015.
  2. The Hebrew University Theory Seminar, March, 2015.
- **More Efficient Oblivious Transfer Extensions with Security for Malicious Adversaries**
  1. *Eurocrypt 2015*, Sofia, Bulgaria. April, 2015.

2. *The 5th Bar-Ilan Winter School*, Advances in Practical Multiparty Computation, February 2015.[video]

- **Towards Characterizing Complete Fairness in Secure Two-Party Computation.**
  1. *Theory Lunch*, computer science department, Technion, Israel. March, 2014.
  2. *TCC 2014*, University of California, San-Diego (UCSD), CA. February, 2014. [video]
  3. *MIT Cryptography and Information Security Seminar*, MIT CSAIL, Cambridge, MA. February 2014.
  4. *Boston University Cryptography Seminar*, Boston, MA. February 2014.
  5. *NYU Cryptography Seminar*, New-York University, NY. February, 2014.
  6. *GTACS – The Greater Tel-Aviv Area Cryptographic Seminar*, IDC, Israel. December, 2013.

- **A Full Characterization of Functions that Imply Fair Coin Tossing and Ramifications to Fairness.**
  1. *Theory Lunch*, Computer Science Department, Technion, Israel. March, 2013.
  2. *TCC 2013*, The University of Tokyo, Tokyo, Japan. March, 2013.
  3. *GTACS – The Greater Tel-Aviv Area Cryptographic Seminar*, IDC, Herzliya, Israel. February, 2013.

- **Calling Out Cheaters: Covert Security with Public Verifiability.**
  1. *Asiacrypt 2012*, Beijing, China. December, 2012.

- **Multiparty Computation with Low Communication, Computation and Interaction via Threshold FHE.**
  1. *Eurocrypt 2012*, The University of Cambridge, England. April, 2012. [video]
  2. *GTACS – The Greater Tel-Aviv Area Cryptographic Seminar*, Tel-Aviv University, March, 2012.
  3. *Computer Science Seminar*, Ben-Gurion University, Israel. February, 2012.

- **Perfectly-Secure Multiplication for any t < n/3.**
  1. *Computer Science Theory Seminar*, The Hebrew University of Jerusalem, Israel. November, 2011.
  2. *CRYPTO 2011*, Santa Barbara, California, USA. August, 2011.[video]
- **Towards a Game Theoretic View of Secure Computation.**
  1. *Eurocrypt 2011*, Tallinn, Estonia. May, 2011.
  2. *IBM Research*, T. J. Watson Research Center, New-York, USA. March, 2011.
  3. *GTACS – The Greater Tel-Aviv Area Cryptographic Seminar*, Bar-Ilan University, March, 2011.
- **Utility Dependence in Correct and Fair Rational Secret Sharing.**
  1. *Computer Science Seminar*, The Open–University, Israel. March, 2011.
  2. Guest lecturer at Cryptography and Game Theory course, Tel-Aviv University, Israel, December, 2009. Instructors: Ran Canetti and Alon Rosen.
  3. *CRYPTO 2009*, Santa Barbara, California, USA. August, 2009.
  4. *Computer Science Seminar*, Ben-Gurion University, Israel. June, 2009.
  5. *Tel-Aviv – Weizmann Cryptography Reading Group*, Tel-Aviv University, Israel. April, 2009.