Yevgeniy Dodis

Courant Institute of Mathematical Sciences,
New York University,
251 Mercer Street, New York, NY 10012.
URL: http://cs.nyu.edu/~dodis

Voice: (212) 998-3084
Fax: (212) 995-4124
Email: dodis@cs.nyu.edu
Citizenship: US

Research Interests

Cryptography, Information Theory and Theoretical Computer Science. Current projects include:

- Random Number Generation and Extraction.
- Key Exposure Protection (aka "Exposure-Resilient Cryptography").
- Cryptography with Imperfect Randomness.
- Cryptography from Biometrics and Other Noisy Data.
- Block Ciphers, Hash Functions and Random Oracle Model.
- Information-Theoretic Cryptography.

My other research interests include digital rights management, authenticated and identity-based encryption, privacy and anonymity, non-malleability, secure distributed computation and concurrent composition of cryptographic protocols. More broadly, I enjoy exploring applications of theoretical computer science to real-life problems.

Education

Massachusetts Institute of Technology. Laboratory for Computer Science. 1998 - 2000
Degree: *Ph.D. in Computer Science.*
Advisor: Professor Madhu Sudan. Thesis topic: "Exposure-Resilient Cryptography".

Massachusetts Institute of Technology. Laboratory for Computer Science. 1996 – 1998
Degree: *Master of Science in Electrical Engineering and Computer Science.*
Master's Thesis: "Space-Time Tradeoffs for Graph Properties".

New York University. College of Arts and Sciences. 1993 – 1996
Degree: *Bachelor of Arts with Honors in Computer Science and Mathematics.*
Overall GPA: 4.0/4.0.

Professional Activities

- Editorial Board Member for Journal of Cryptology (JoC).
- Program co-Chair for the Theory of Cryptography Conference (TCC), 2015.
- Local Arrangements Chair for the Symposium on Theory of Computing (STOC), 2012.
- General Chair for the Theory of Cryptography Conference (TCC), 2008.
- Co-Editor, General and Sponsorship Chair for the Public Key Cryptography (PKC) 2006 International Workshop.
- Program Committees:
  - Symposium on Theory of Computing (STOC), 2017.

  - EuroCrypt Conference, 2016.
  - Theory of Cryptography Conference (TCC), 2015.
  - CRYPTO Conference, 2014.
  - Theory of Cryptography Conference (TCC), 2014.
  - Computer Science Symposium in Russia (CSR), 2013.
  - Innovations in Theoretical Computer Science (ITCS), 2013.
  - CRYPTO Conference, 2012.
  - CRYPTO Conference, 2011.
  - ASIACRYPT Conference, 2010.
  - Security in Communication Networks (SCN), 2010.
  - Behavioral and Quantitative Game Theory (BQGT) Conference, 2010.
  - Foundations of Computer Science (FOCS), 2008.
  - CRYPTO Conference, 2008.
  - International Conference on Information Theoretic Security (ICITS), 2008.
  - Theory of Cryptography Conference (TCC), 2008.
  - CRYPTO Conference, 2007.
  - Symposium on Theory of Computing (STOC), 2007.
  - International Conference on Information Security and Cryptology (ICISC), 2006.
  - EuroCrypt Conference, 2006.
  - RSA Conference, Cryptographers' Track, 2006.
  - International Conference on Information Security and Cryptology (ICISC), 2005.
  - ACM Conference on Computer and Communication Security (CCS), 2005.
  - International Conference on Digital Rights Management: Technologies, Issues, Challenges and Systems (DRMTICS), 2005.
  - EuroCrypt Conference, 2005.
  - CRYPTO Conference, 2004.
  - EuroCrypt Conference, 2003.

- Co-Organizer of the semi-annual IBM/NYU/Columbia Theory Day: `http://cs.nyu.edu/csweb/Calendar/colloquium/theory_day.html`.
- Organizer of NYU Cryptography Seminar: `http://www.cs.nyu.edu/crg/`.
- Editorial Board Member for Advances in Cryptology & Information Security (ACIS) book series.

Funding

- NSF Trustworthy Computing Grant (#1619158), 9/2016-8/2019. "On the Design of Secure Hash Functions and Block Ciphers". Amount: $500,000.
- Google Research Gift on "New Methods for Deriving Keys from Passwords", 2013. Amount: $49,000.
- NSF Trustworthy Computing Grant (#1314568), 8/2013-7/2017. "The Theory and Practice of Key Derivation". Amount: $668,764.
- NSF Trustworthy Computing Grant (#1319051), 8/2013-7/2016. "On Imperfect Randomness and Leakage-Resilient Cryptography". Amount: $500,000.
- VMware Research Gift on "Random Number Generation in Virtualized Environments", 2012. Amount: $97,403.

- NSF Trustworthy Computing Grant (#1065288), 9/2011-8/2015. "Random Number Generation and Use in Virtualized Environments". Amount: $450,000.
- Google Research Gift on "Leakage-Resilient Cryptography", 2010. Amount: $50,000.
- NSF Trustworthy Computing Grant (#1017471), 9/2010-8/2013. "The Design of Secure Hash Functions and Block Ciphers". Amount: $500,000.
- NYU-Poly Seed Fund (with Nitesh Saxena), 9/2009-5/2010. "Fault-Tolerate User-Centric Security Services Exploiting Social Networks". Amount: $23,061.
- NSF CyberTrust Grant (#0831299), 9/2008-8/2011. "On Imperfect Randomness and Exposure-Resilient Cryptography". Amount: $300,000.
- NSF CyberTrust Grant (#0716690, with Victor Shoup), 9/2007-8/2011. "On the Design of Secure Hash Functions and Privacy-Preserving Protocols". Amount: $480,000.
- New York University Research Challenge Fund, Summer 2007. "Enhanced Security Models for Network Protocols". Amount: $6,595.
- IBM Faculty Award, 2005. Amount: $30,000.
- NSF Theory of Computing Grant (#0515121), 9/2005-8/2008. "Rigorous Cryptography from Biometrics and Other Noisy Data". Amount: $100,000.
- NSF Trusted Computing Grant (#0311095), 9/2003-8/2006. "Mitigating the Damaging Effects of Key Exposure". Amount: $180,000.
- New York University Research Challenge Fund, Summer 2003. "Cryptographic Protocols with Imperfect Sources of Randomness". Amount: $7,200.
- NSF Faculty Early Career Development (CAREER) Award (#0133806), 1/2002-12/2006. "Exposure-Resilient Cryptography". Amount: $330,000.

Honors & Awards

- Invited speaker at CISS 2017, TCC 2016 and Indocrypt 2015.
- Winner of 2012 VMware Faculty Award.
- Winner of 2010 and 2013 Google Faculty Award.
- Winner of 2005 IBM Faculty Award.
- Best Paper Award at PKC'2005 conference. See [77].
- The following papers invited to special issues of journals as top 3-5 papers at the corresponding conference: CRYPTO'14 [8], TCC'13 [19], FOCS'11 [29], CRYPTO'11 [31], Asiacrypt'10 [33], TCC'07 [58].
- NSF Faculty Early Career Development (CAREER) Award, 2002-2006.
- Best Contributor Award at ICALP'1999 conference. See [116].
- Winner (Putnam Fellow) of 1995-96 US-Canada PUTNAM Mathematical Competition.

Relevant Professional Experience

New York University. Courant Institute of Mathematical Sciences. 2012-present
Professor in the Department of Computer Science.

UC Berkeley. Simons Institute for Theory of Computing. summer 2015
Visiting Professor for the Cryptography Program.

New York University. Courant Institute of Mathematical Sciences. 2007-2012
Associate Professor in the Department of Computer Science.

Harvard University. School of Engeneering and Applied Sciences. 2007-2008
Visiting Professor in the Center for Research on Computation and Society.

New York University. Courant Institute of Mathematical Sciences. 2001-2006
Assistant Professor in the Department of Computer Science.

Cryptography Consultant. Various positions. 2000-present
Designed, analyzed and supervised the implementation of various cryptographic protocols and evaluation procedures. Performed cryptanalysis of ciphers and other security protocols. Gave tutorials on various aspects of Cryptography and Network Security.

T.J. Watson Research Center. IBM Corporation. Fall of 2000
Postdoctoral Fellow in the Cryptography Group.
Supervisor: Tal Rabin.

T.J. Watson Research Center. IBM Corporation. Summer of 99
Research intern in the Cryptography Group.
Supervisor: Tal Rabin.

Bell Labs. Lucent Technologies. Summers of 98 and 97
Research intern in the Department of Fundamental Mathematics.
Supervisor: Sanjeev Khanna.

Massachusetts Institute of Technology. Laboratory for Computer Science. 1996-2000
Research Assistant. Teaching assistant of the Cryptography class.

Teaching

- Research Seminar in Cryptography (graduate). Every Semester.
- Introduction to Cryptography (graduate). Spring 2012, Fall 2008/2006/2001.
- Advanced Cryptography (graduate). Fall 2009.
- Randomness in Cryptography (graduate). Spring 2014/2013.
- Exposure-Resilient Cryptography (graduate). Spring 2007.
- Cryptography and Imperfect Randomness (graduate). Spring 2006.
- Introduction to Cryptography (undergraduate). Spring 2006/2005, Fall 2002.
- Fundamental Algorithms (graduate). Fall 2016/2015/2014/2013/2012/2011, Spring 2016.
- Basic Algorithms (undergraduate). Spring 2015/2010/2009, Fall 2016/2010.
- Honors Theory of Computation (graduate). Spring 2004/2003/2001.
- Honors Algorithms (undergraduate). Fall 2003.

Graduate Students

Graduated PhD Students:

1. Noah Stephens-Davidowitz. Graduated Summer 2017.
   Thesis Topic: "TBA (on Lattices and Cryptography)".
   First Job: Simons postdoc at Princeton and IAS.
2. Aleksandr (Sasha) Golovnev. Graduated Spring 2017.
   Thesis Topic: "Circuit Complexity: New Techniques and Their Limitations".
   First Job: Yahoo Research.
3. Aristeidis (Aris) Tentes. Graduated Summer 2014.
   Thesis Topic: "Computational Complexity Implications of Secure Coin Flipping Protocols".
   First Job: Goldman Sachs.
4. Adriana Lopez-Alt. Graduated Spring 2014.
   Thesis Topic: "Cryptographic Algorithms for the Secure Delegation of Multiparty Computation".
   First Job: Google.
5. Daniel Wichs. Graduated September 2011.
   Thesis Topic: "Cryptographic Resilience to Continual Information Leakage".
   First job: IBM Watson Research Center (Raviv's postdoc) → Northeastern University.
6. Joel Alwen. Graduated September 2011.
   Thesis Topic: "Collusion Preserving Computation".
   First job: ETH Zurich (postdoc).
7. Sherman Chow (co-adviser Shoup). Graduated September 2010.
   Thesis Topic: "New Privacy-Preserving Techniques for Identity- and Attribute-Base Encryption".
   First job: University of Waterloo (postdoc) → Chinese University of Hong Kong.
8. Carl Bosley. Graduated October 2009.
   Thesis Topic: "On Randomness Requirements for Privacy".
   First job: Stevens Institute (CI postdoc) → Google.
9. Shabsi Walfish. Graduated Fall 2007.
   Thesis Topic: "Enhanced Security Models for Network Protocols".
   First Job: Google.
10. Prashant Puniya. Graduated Summer 2007.
    Thesis Topic: "New Design Criteria for Hash Functions and Block Ciphers".
    First Job: Citigroup.
11. Nelly Fazio. Graduated Spring 2006.
    Thesis Topic: "On Cryptographic Techniques for Digital Rights Management".
    First Job: IBM Almaden Research Center (postdoc) → City University of New York.

Current PhD Students:

- Chaya Ganesh.

Research Mentor and/or Thesis Reader:

- Laura Florescu (NYU). Graduated April 2017.

- Sandro Coretti (ETH, Switzerland). Graduated March 2016.
- Yanquinq Yao (Beihang University, China). Exchange Student in 2012-2014.
- Eric Miles (Northeastern University). Graduated April 2014.
- Yannis Rouselakis (University of Texas at Austin). Graduated August 2013.
- Feng-Hao Liu (Brown University). Graduated April 2013.
- Avradip Mandal (University of Luxembourg). Graduated June 2012.
- Ali Juma (University of Toronto). Graduated April 2011.
- Kris Haralambiev (NYU). Graduated March 2011.
- Yevgeniy Vahlis (University of Toronto). Graduated August 2010.
- Alptekin Kupcu (Brown University). Graduated April 2010.
- Aleksandr Yampolskiy (Yale). Graduated Spring 2006.
- Krzysztof Pietrzak (ETH, Switzerland). Graduated Fall 2005.
- Dae Hyun Yum (POSTECH, Korea). Exchange Student in 2004-2005.
- Roberto Oliveira (NYU). Graduated Spring 2004.
- Anca Ivan (NYU). Graduated Spring 2004.

See [4, 6, 8, 10, 12, 13, 21, 25, 27, 28, 30, 33, 34, 35, 38, 40, 41, 42, 44, 47, 49, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 64, 65, 66, 68, 70, 71, 74, 77, 78, 79, 81, 82, 85, 89, 90, 96, 97, 100, 102] for our joint work.

Postdocs

- Muthu Venkitasubramaniam (Sep. 2010-May 2011)
- Dario Fiore (Jan. 2012-Nov. 2012)
- Divesh Aggraval (Sep. 2012-Aug. 2014)
- Tomasz Kazana (Jan. 2015-Oct. 2015)
- Siyao Guo (Jan. 2016-Dec. 2016)
- Sandro Coretti (Jun. 2016-May 2018)

Invited Journal Papers

- Yevgeniy Dodis, Nelly Fazio, Aggelos Kiayias and Moti Yung. "Scalable Public-Key Tracing and Revoking", Invited paper in the special issue of Journal of Distributed Computing (JoDC), 17(4):323-347, May 2005.
- Ricard Cole, Yevgeniy Dodis and Tim Roughgarden. "How Much Can Taxes Help Selfish Routing?", Invited paper in the special issue of Journal of Computer and System Sciences (JCSS) on Network Algorithms, 72(3):444-467, 2006.
- Yevgeniy Dodis, Pil Joong Lee and Dae Hyun Yum, "Optimistic Fair Exchange in a Multi-User Setting", *Journal of Universal Computer Science*, 14(3):318–346, 2008.

- Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin and Adam Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data", *SIAM Journal of Computing*, 38(1):97–139, 2008.

- Richard Cole, Yevgeniy Dodis and Tim Roughgarden, "Bottleneck Links, Variable Demand, and the Tragedy of the Commons", *Networks*, 60(3):194–203, 2012.

- Yevgeniy Dodis, Bhavana Kanakurthi, Jonathan Katz, Leonid Reyzin and Adam Smith, "Robust Fuzzy Extractors and Authenticated Key Agreement from Close Secrets", *IEEE Transactions on Information Theory*, 58(9):6207–6222, September 2012.

- Yevgeniy Dodis, "The Cost of Cryptography", Nautilus Magazine, Issue 007 ("Waste"), November 2013.

- Yevgeniy Dodis, Xin Li, Trevor D. Wooley, David Zuckerman, "Privacy Amplification and Nonmalleable Extractors Via Character Sums", *SIAM Journal of Computing*, 43(2):800–830, 2014.

- Yevgeniy Dodis, Noah Stephens-Dawidivitz, Adi Shamir and Daniel Wichs, "How to Eat Your Entropy and Have it Too – Optimal Recovery Strategies for Compromised RNGs", special issue of *Algorithmica*, 2016, pp. 1–37.

- Divesh Aggarwal, Yevgeniy Dodis and Shachar Lovett, "Non-malleable Codes from Additive Combinatorics", *SIAM Journal of Computing*, accepted, 2016.

Proceedings and Book Chapters

- Yevgeniy Dodis, Jesper Buus Nielsen. Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part I. Lecture Notes in Computer Science 9014, Springer 2015, ISBN 978-3-662-46493-9.

- Yevgeniy Dodis, Jesper Buus Nielsen. Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part II. Lecture Notes in Computer Science 9015, Springer 2015, ISBN 978-3-662-46496-0.

- "Concealment and Its Applications to Authenticated Encryption", invited chapter in "Practical Signcryption" (edited by A.Dent and Y. Zheng), Springer, 2010.

- "Forward-Secure Hierarchical IBE with Applications to Broadcast Encryption Schemes." (w. Danfeng Yao, Nelly Fazio and Anna Lysyanskaya), *Identity-Based Cryptography*, (special volume edited by Marc Joye and Gregory Neven) , IOS Press Cryptology and Information Security Series, 2008.

- "Fuzzy Extractors" (with Leonid Reyzin and Adam Smith), invited chapter in "Security with Noisy Data" (edited by Pim Tuyls, Boris Skoric, and Tom Kevenaar), Springer, 2007.

- "Cryptography and Game Theory" (with Tal Rabin), invited chapter in "Algorithmic Game Theory" (edited by N. Nisan, T. Roughgarden, E. Tardos, and V. Vazirani), Cambridge University Press, 2007.

- Co-Editor (with Moti Yung, Aggelos Kiayias, Tal Malkin) of "Public Key Cryptography – PKC 2006", 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA, April 24-26, 2006, Proceedings Springer 2006.
- "Signcryption", chapter in the Encyclopedia of Cryptography and Security, Kluwer Academic Publishers (edited by Henk C.A. van Tilborg), 2005.

Published Papers (in reverse chronological order)

1. Yevgeniy Dodis, Siyao Guo and Jonathan Katz, "Fixing Cracks in the Concrete: Random Oracles with Auxiliary Input, Revisited", *Advances in Cryptology - EUROCRYPT*, May 2017.
2. Yevgeniy Dodi and Dario Fiore, "Unilaterally-Authenticated Key Exchange", *Financial Cryptography and Data Security Conference*, April 2017.
3. Yevgeniy Dodis, Shai Halevi, Ron D. Rothblum and Daniel Wichs, "Spooky Encryption and its Applications", *Advances in Cryptology - CRYPTO*, August 2016.
4. Yevgeniy Dodis, Ilya Mironov and Noah Stephens-Dawidivitz, "Message Transmission with Reverse Firewalls–Secure Communication on Corrupted Machines", *Advances in Cryptology - CRYPTO*, August 2016.
5. Yevgeniy Dodis, Tianren Liu, Martijn Stam and John Steinberger, "Indifferentiability of Confusion-Diffusion Networks", *Advances of Cryptology — EUROCRYPT*, May 2016.
6. Sandro Coretti, Yevgeniy Dodis, Bjorn Tackmann and Daniele Venturi, "Non-Malleable Encryption: Simpler, Shorter, Stronger", *Theory of Cryptography Conference (TCC)*, January 2016.
7. Allison Bishop and Yevgeniy Dodis, "Interactive Coding for Interactive Proofs", *Theory of Cryptography Conference (TCC)*, January 2016.
8. Yevgeniy Dodis and Yanquing Yao, "Privacy with Imperfect Randomness", *Advances in Cryptology - CRYPTO*, August 2015.
9. Divesh Aggarwal, Yevgeniy Dodis, Tomasz Kazana and Maciej Obremski, "Non-malleable Reductions and Applications", *Symposium on Theory of Computing (STOC)*, June 2015.
10. Yevgeniy Dodis, Chaya Ganesh, Alexander Golovnev, Ari Juels and Thomas Ristenpart, "A Formal Treatment of Backdoored Pseudorandom Generators", *Advances of Cryptology — EUROCRYPT*, April 2015.
11. Yevgeniy Dodis and Dario Fiore, "Interactive Encryption and Message Authentication", *Conference on Security in Communication Networks*, September 2014.
12. Yevgeniy Dodis, Noah Stephens-Dawidivitz, Adi Shamir and Daniel Wichs, "How to Eat Your Entropy and Have it Too – Optimal Recovery Strategies for Compromised RNGs", *Advances in Cryptology - CRYPTO*, August 2014. Invited to special CRYPTO'14 issue of *Algorithmica* as one of best papers.

13. Divesh Aggarwal, Yevgeniy Dodis, Zahra Jafargholi, Eric Miles and Leonid Reyzin, "Amplifying Privacy in Privacy Amplification", *Advances in Cryptology - CRYPTO*, August 2014.

14. Divesh Aggarwal, Yevgeniy Dodis and Shachar Lovett, "Non-malleable Codes from Additive Combinatorics", *Symposium on Theory of Computing (STOC)*, June 2014.

15. Yevgeniy Dodis, Krzysztof Pietrzak and Daniel Wichs, "Key Derivation Without Entropy Waste", *Advances of Cryptology — EUROCRYPT*, May 2014.

16. Shweta Agrawal, Yevgeniy Dodis, Vinod Vaikuntanathan and Daniel Wichs, "On Continual Leakage of Discrete Log Representations", *Advances in Cryptology - ASIACRYPT*, December 2013.

17. Yevgeniy Dodis, David Pointcheval, Sylvain Ruhault, Damien Vergnaud and Daniel Wichs, "Security Analysis of Pseudo-Random Number Generators with Input: /dev/random is not Robust", *ACM Conference on Computer and Communication Security (CCS)*, November 2013.

18. Elena Andreeva, Andrey Bogdanov, Yevgeniy Dodis, Bart Mennink and John P. Steinberger, "On the Indifferentiability of Key-Alternating Ciphers", *Advances in Cryptology - CRYPTO*, August 2013.

19. Yevgeniy Dodis and Yu Yu, "Overcoming Weak Expectations", *Theory of Cryptography Conference (TCC)*, March 2013. Invited to *Journal of Cryptology* as one of best papers.

20. Yevgeniy Dodis and Yu Yu, "Overcoming Weak Expectations" (invited paper), *Information Theory Workshop (ITW)*, September 2012.

21. Yevgeniy Dodis, Adriana Lopez-Alt, Ilya Mironov and Salil Vadhan, "Differential Privacy with Imperfect Randomness", *Advances in Cryptology - CRYPTO*, August 2012.

22. Yevgeniy Dodis, Tom Ristenpart, John Steinberger and Stefano Tessaro, "To Hash or Not to Hash Again? (In)differentiability Results for H^2 and HMAC", *Advances in Cryptology - CRYPTO*, August 2012.

23. Yevgeniy Dodis, "Shannon Impossibility, Revisited", *International Conference on Information Theoretic Security (ICITS)*, August 2012.

24. Yevgeniy Dodis, Weiliang Luo, Shouhuai Xu and Moti Yung, "Key-Insulated Symmetric Key Cryptography and Mitigating Attacks against Cryptographic Cloud Software", *ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, May 2012.

25. Yevgeniy Dodis, Eike Kiltz, Krzysztof Pietrzak and Daniel Wichs, "Message Authentication, Revisited", *Advances of Cryptology — EUROCRYPT*, April 2012.

26. Yevgeniy Dodis, Thomas Ristenpart and Salil Vadhan, "Randomness Condensers for Efficiently Samplable, Seed-Dependent Sources", *Theory of Cryptography Conference (TCC)*, March 2012.

27. Yevgeniy Dodis, Abhishek Jain, Tal Moran and Daniel Wichs, "Counterexamples to Hardness Amplification Beyond Negligible", *Theory of Cryptography Conference (TCC)*, March 2012.

28. Yevgeniy Dodis, Iftach Haitner and Aris Tentes, "On the Instantiability of Hash-and-Sign RSA Signatures", *Theory of Cryptography Conference (TCC)*, March 2012.

29. Yevgeniy Dodis, Xin Li, Trevor D. Wooley, and David Zuckerman, "Privacy Amplification and Non-Malleable Extractors Via Character Sums", *Foundations of Computer Science (FOCS)*, October 2011. Invited to special issue of *SICOMP*.

30. Yevgeniy Dodis, Allison Lewko, Brent Waters and Daniel Wichs, "Storing Secrets on Continually Leaky Devices", *Foundations of Computer Science (FOCS)*, October 2011.

31. Boaz Barak, Yevgeniy Dodis, Hugo Krawczyk, Olivier Pereira, Krzysztof Pietrzak, Francois-Xavier Standaert and Yu Yu, "Leftover Hash Lemma, Revisited", *Advances in Cryptology - CRYPTO*, August 2011. Invited to *Journal of Cryptology* as one of best papers.

32. Yevgeniy Dodis and John Steinberger, "Domain Extension for MACs beyond the Birthday Barrier", *Advances of Cryptology — EUROCRYPT*, May 2011.

33. Yevgeniy Dodis, Kristiyan Haralambiev, Adriana Lopez-Alt and Daniel Wichs, "Efficient Public-Key Cryptography in the Presence of Key Leakage", *Advances in Cryptology - ASIACRYPT*, December 2010. Invited to *Journal of Cryptology* as one of best papers.

34. Yevgeniy Dodis, Kristiyan Haralambiev, Adriana Lopez-Alt and Daniel Wichs, "Cryptography Against Continuous Memory Attacks", *Foundations of Computer Science (FOCS)*, October 2010.

35. Sherman Chow, Yevgeniy Dodis, Yannis Rouselakis and Brent Waters, "Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions", *ACM Conference on Computer and Communication Security (CCS)*, October 2010.

36. Yevgeniy Dodis and Krzysztof Pietrzak, "Leakage-Resilient Pseudorandom Functions and Side-Channel Attacks on Feistel Networks", *Advances in Cryptology - CRYPTO*, August 2010.

37. Yevgeniy Dodis, Mihai Patrascu and Mikkel Thurup, "Changing Base Without Losing Space", *ACM Symposium on Theory of Computing (STOC)*, June 2010.

38. Joel Alwen, Yevgeniy Dodis, Moni Naor, Gil Segev, Shabsi Walfish and Daniel Wichs, "Public-Key Encryption in the Bounded-Retrieval Model", *Advances of Cryptology — EUROCRYPT*, May 2010.

39. Yevgeniy Dodis, Shafi Goldwasser, Yael Kalai, Chris Peikert and Vinod Vaikuntanathan "Public-key Encryption Schemes with Auxiliary Inputs" *Theory of Cryptography Conference (TCC)*, February 2010.

40. Jean-Sebastien Coron, Yevgeniy Dodis, Avradip Mandal and Yannick Seurin, "A Domain Extender for the Ideal Cipher" *Theory of Cryptography Conference (TCC)*, February 2010.

41. Joel Alwen, Yevgeniy Dodis and Daniel Wichs, "Leakage-Resilience and the Bounded Retrieval Model" (invited paper), *International Conference on Information Theoretic Security (ICITS)*, December 2009.

42. Joel Alwen, Yevgeniy Dodis and Daniel Wichs, "Leakage-Resilient Public-Key Cryptography in the Bounded-Retrieval Model", *Advances of Cryptology — CRYPTO*, August 2009.

43. Yevgeniy Dodis and John Steinberger, "Message Authentication Codes from Unpredictable Block Ciphers", *Advances of Cryptology — CRYPTO*, August 2009.

44. Yevgeniy Dodis and Daniel Wichs, "Non-malleable Extractors and Symmetric Key Cryptography from Weak Secrets", *ACM Symposium on Theory of Computing (STOC)*, May 2009.

45. Yevgeniy Dodis, Yael Tauman Kalai and Shachar Lovett, "On Cryptography with Auxiliary Input", *ACM Symposium on Theory of Computing (STOC)*, May 2009.

46. Yevgeniy Dodis, Thomas Ristenpart and Thomas Shrimpton, "Salvaging Merkle-Damgard for Practical Applications", *Advances in Cryptology - EUROCRYPT*, April 2009.

47. Yevgeniy Dodis, Salil Vadhan and Daniel Wichs, "Proofs of Retrievability via Hardness Amplification", *Theory of Cryptography Conference (TCC)*, March 2009.

48. Yevgeniy Dodis, Russell Impagliazzo, Ragesh Jaiswal and Valentine Kabanets, "Security Amplification for Interactive Cryptographic Primitives", *Theory of Cryptography Conference (TCC)*, March 2009.

49. Yevgeniy Dodis, Jonathan Katz, Adam Smith and Shabsi Walfish, "Composability and On-Line Deniability of Authentication", *Theory of Cryptography Conference (TCC)*, March 2009.

50. Yevgeniy Dodis, Leonid Reyzin, Ronald Rivest and Emily Shen, "Indifferentiability of Permutation-Based Compression Functions and Tree-Based Modes of Operation, with Applications to MD6", *Workshop on Fast Software Encryption (FSE)*, February 2009.

51. Yevgeniy Dodis, Victor Shoup and Shabsi Walfish, "Efficient Constructions of Composable Commitments and Zero-Knowledge Proofs", *Advances of Cryptology — CRYPTO*, August 2008.

52. Yevgeniy Dodis and Prashant Puniya, "Getting the Best Out of Existing Hash Functions or What if We Are Stuck with SHA?", *Applied Cryptography and Network Security (ACNS) Conference*, June 2008.

53. Yevgeniy Dodis, Krzysztof Pietrzak and Prashant Puniya, "A New Mode of Operation for Block Ciphers and Length-Preserving MACs", *Advances in Cryptology - EUROCRYPT*, April 2008.

54. Ronald Cramer, Yevgeniy Dodis, Serge Fehr, Carles Padro and Daniel Wichs, "Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors", *Advances in Cryptology - EUROCRYPT*, April 2008.

55. Yevgeniy Dodis and Prashant Puniya, "Feistel Networks made Public, and Applications", *Advances in Cryptology — EUROCRYPT*, May 2007.

56. Yevgeniy Dodis, Pil Joong Lee and Dae Hyun Yum, "Optimistic Fair Exchange in a Multi-User Setting", *Workshop on Public Key Cryptography (PKC)*, April 2007.

57. Yevgeniy Dodis and Krzysztof Pietrzak, "Improving the Security of MACs via Randomized Message Preprocessing", *Workshop on Fast Software Encryption (FSE)*, March 2007.

58. Carl Bosley and Yevgeniy Dodis, "Does Privacy Require True Randomness?", *Theory of Cryptography Conference (TCC)*, February 2007. Invited to *Journal of Cryptology* as one of best papers.

59. Ran Canetti, Yevgeniy Dodis, Rafael Pass and Shabsi Walfish, "Universally Composable Security with Global Setup", *Theory of Cryptography Conference (TCC)*, February 2007.

60. David Cash, Yan Zong Ding, Yevgeniy Dodis, Wenke Lee, Richard Lipton and Shabsi Walfish, "Intrusion-Resilient Key Exchange in the Bounded Retrieval Model", *Theory of Cryptography Conference (TCC)*, February 2007.

61. Yevgeniy Dodis, Jonathan Katz, Leonid Reyzin and Adam Smith, "Robust Fuzzy Extractors and Authenticated Key Agreement from Close Secrets", *Advances of Cryptology — CRYPTO*, August 2006.

62. Yevgeniy Dodis and Renato Renner, "On the Impossibility of Extracting Classical Randomness Using a Quantum Computer", *International Colloquium on Automata, Languages and Programming (ICALP)*, July 2006.

63. Dario Catalano, Yevgeniy Dodis and Ivan Visconti, "Mercurial Commitments: Minimal Assumptions and Efficient Constructions", *Theory of Cryptography Conference (TCC)*, March 2006.

64. Yevgeniy Dodis, Krzysztof Pietrzak and Bartosz Przydatek "Separating Sources for Encryption and Secret-Sharing", *Theory of Cryptography Conference (TCC)*, March 2006.

65. Yevgeniy Dodis and Prashant Puniya, "On the Relation between the Ideal Cipher and the Random Oracle Models", *Theory of Cryptography Conference (TCC)*, March 2006.

66. Yevgeniy Dodis, Aleksandr Yampolskiy and Moti Yung, "Threshold and Proactive Pseudorandom Permutations", *Theory of Cryptography Conference (TCC)*, March 2006.

67. Richard Cole, Yevgeniy Dodis and Tim Roughgarden, "Bottleneck Links, Variable Demand, and the Tragedy of the Commons", *ACM/SIAM Symposium on Discrete Algorithms (SODA)*, January 2006.

68. Jean-Sebastian Coron, Yevgeniy Dodis, Cecile Malinaud and Prashant Puniya, "A New Design Criteria for Hash-Functions", *NIST Cryptographic Hash Workshop*, November 2005.

69. Yevgeniy Dodis, "On Extractors, Error-Correction and Hiding All Partial Information" (invited paper), *Information Theory Workshop (ITW)*, October 2005.

70. Yevgeniy Dodis, Roberto Oliveira and Krzysztof Pietrzak, "On the Generic Insecurity of the Full Domain Hash", *Advances of Cryptology — CRYPTO*, August 2005.

71. Jean-Sebastian Coron, Yevgeniy Dodis, Cecile Malinaud and Prashant Puniya, "Merkle-Damgard Revisited : how to Construct a Hash Function", *Advances of Cryptology — CRYPTO*, August 2005.

72. Yevgeniy Dodis and Adam Smith, "Correcting Errors Without Leaking Partial Information", *ACM Symposium on Theory of Computing (STOC)*, May 2005.

73. Xavier Boyen, Yevgeniy Dodis, Jonathan Katz, Rafail Ostrovsky and Adam Smith, "Secure Remote Authentication Using Biometrics", *Advances in Cryptology — EUROCRYPT*, May 2005.

74. Yevgeniy Dodis and Dae Hyun Yum, "Time Capsule Signature", *Financial Cryptography and Data Security Conference (FC)*, March 2005.

75. Yevgeniy Dodis and Adam Smith, "Entropic Security and the Encryption of High-Entropy Messages", *Theory of Cryptography Conference (TCC)*, February 2005.

76. Yevgeniy Dodis and Jonathan Katz, "Chosen Ciphertext Security For Multiple Encryption", *Theory of Cryptography Conference (TCC)*, February 2005.

77. Yevgeniy Dodis and Aleksandr Yampolskiy, "A Verifiable Random Function With Short Proofs and Keys", *Workshop on Public Key Cryptography (PKC)*, January 2005. Winner of *Best Paper Award*.

78. Danfeng Yao, Nelly Fazio, Yevgeniy Dodis and Anna Lysyanskaya, "ID-Based Encryption for Complex Hierarchies with Applications to Forward Security and Broadcast Encryption", *ACM Conference on Computer and Communication Security (CCS)*, October 2004.

79. Yevgeniy Dodis, Michael J. Freedman, Stanislaw Jarecki and Shabsi Walfish, "Versatile Padding Schemes for Joint Signature and Encryption", *ACM Conference on Computer and Communication Security (CCS)*, October 2004.

80. Yevgeniy Dodis, Shien Jin Ong, Manoj Prabhakaran and Amit Sahai, "On the (Im)possibility of Cryptography with Imperfect Randomness", *Foundations of Computer Science (FOCS)*, October 2004.

81. Yevgeniy Dodis, Rafael Pass and Shabsi Walfish, "Fully-Simulatable Multiparty Computation", Preliminary announcement of future work, published in *Workshop on Secure Multiparty Protocols (SMP 2004)*, October 2004.

82. Yevgeniy Dodis, Ariel Elbaz, Roberto Oliveira and Ran Raz, "Improved Randomness Extraction from Two Independent Sources", *International Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM)*, August 2004.

83. Yevgeniy Dodis, Rosario Gennaro, Johan Hastad, Hugo Krawczyk and Tal Rabin, "Randomness Extraction and Key Derivation Using the CBC, Cascade and HMAC Modes", *Advances in Cryptology — CRYPTO*, August 2004.

84. Andris Ambainis, Harry Buhrman, Yevgeniy Dodis and Hein Röhrig, "Multiparty Quantum Coin Flipping", *Conference on Computational Complexity (CCC)*, June 2004.

85. Yevgeniy Dodis, Aggelos Kiayias, Antonio Nicolosi and Victor Shoup, "Anonymous Identification in Ad-hoc Groups", *Advances in Cryptology — EUROCRYPT*, May 2004.

86. Yevgeniy Dodis, Leonid Reyzin and Adam Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data", *Advances in Cryptology — EUROCRYPT*, May 2004.

87. Yevgeniy Dodis, Matt Franklin, Jonathan Katz, Atsuko Miyaji and Moti Yung, "A Generic Construction for Intrusion-Resilient Public-Key Encryption", *RSA Conference, Cryptography Track (CT-RSA)*, February 2004.

88. Yevgeniy Dodis and Leonid Reyzin, "Breaking and Repairing Optimistic Fair Exchange from PODC 2003", *ACM Workshop on Digital Rights Management*, October 2003.

89. Yevgeniy Dodis and Roberto Oliveira, "On Extracting Private Randomness over a Public Channel", *Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM)*, August 2003.

90. Yevgeniy Dodis, Nelly Fazio, Aggelos Kiayias and Moti Yung, "Fully Scalable Public-Key Traitor Tracing", *Principles of Distributed Computing (PODC)*, July 2003.

91. Richard Cole, Yevgeniy Dodis and Tim Roughgarden, "Pricing Network Edges for Heterogeneous Selfish Users", *ACM Symposium on Theory of Computing (STOC)*, June 2003.

92. Richard Cole, Yevgeniy Dodis and Tim Roughgarden, "The Cost of Taxes for Selfish Routing", *ACM Conference on Electronic Commerce (EC)*, June 2003.

93. Richard Cole, Yevgeniy Dodis and Tim Roughgarden, "Pricing Networks with Selfish Routing" (survey), *Workshop on Economics of Peer-to-Peer Systems*, June 2003.

94. Yevgeniy Dodis and Jee Hea An, "Concealment and Its Applications to Authenticated Encryption", *Advances in Cryptology — EUROCRYPT*, May 2003.

95. Yevgeniy Dodis, Matt Franklin, Jonathan Katz, Atsuko Miyaji and Moti Yung, "Intrusion-Resilient Public-Key Encryption", *RSA Conference, Cryptography Track (CT-RSA)*, April 2003.

96. Antonio Nicolosi, Max Krohn, Yevgeniy Dodis and David Mazières, "Proactive Two-party Signatures for User Authentication", *Network and Distributed System Security Symposium (NDSS)*, February 2003.

97. Anca Ivan and Yevgeniy Dodis, "Proxy Cryptography Revisited", *Network and Distributed System Security Symposium (NDSS)*, February 2003.

98. Yevgeniy Dodis, "Efficient Construction of (Distributed) Verifiable Random Functions", *Workshop on Public Key Cryptography (PKC)*, January 2003.

99. Yevgeniy Dodis, Jonathan Katz, Shouhuai Xu and Moti Yung, "Strong Key-Insulated Signature Schemes", *Workshop on Public Key Cryptography (PKC)*, January 2003.

100. Yevgeniy Dodis and Nelly Fazio, "Public Key Trace and Revoke Scheme Secure against Adaptive Chosen Ciphertext Attack", *Workshop on Public Key Cryptography (PKC)*, January 2003.

101. Yevgeniy Dodis and Moti Yung, "Exposure-Resilience for Free: the Case of Hierarchical ID-based Encryption", *IEEE International Security In Storage Workshop (SISW)*, December 2002.

102. Yevgeniy Dodis and Nelly Fazio, "Public Key Broadcast Encryption for Stateless Receivers", *ACM Workshop on Digital Rights Management*, November 2002.

103. Yevgeniy Dodis and Joel Spencer, "On the (non)Universality of the One-Time Pad", *Foundations of Computer Science Conference (FOCS)*, November 2002.

104. Yevgeniy Dodis and Leonid Reyzin, "On the Power of Claw-Free Permutations", *Conference on Security in Communication Networks*, July 2002.

105. Jee Hea An, Yevgeniy Dodis and Tal Rabin, "On the Security of Joint Signature and Encryption", *Advances in Cryptology — EUROCRYPT*, May 2002.

106. Yevgeniy Dodis, Jonathan Katz, Shouhuai Xu, and Moti Yung, "Key-Insulated Public Key Cryptosystems", *Advances in Cryptology — EUROCRYPT*, May 2002.

107. Yevgeniy Dodis and Shai Halevi, "Incremental Codes", *Workshop on Approximation Algorithms for Combinatorial Optimization Problems (APPROX)*, August 2001.

108. Yevgeniy Dodis, "New Imperfect Random Source with Applications to Coin-Flipping", *International Colloquium on Automata, Languages and Programming (ICALP)*, July 2001. Preliminary version appeared in *Electronic Colloquium on Computational Complexity*, technical report TR00-039, 2000.

109. Yevgeniy Dodis, Amit Sahai and Adam Smith, "On Perfect and Adaptive Security in Exposure-Resilient Cryptography", *Advances in Cryptology — EUROCRYPT*, May 2001.

110. Yevgeniy Dodis and Peter Winkler, "Universal Configurations in Light-Flipping Games" (Short Form), *ACM/SIAM Symposium on Discrete Algorithms (SODA)*, January 2001.

111. **PhD Thesis**, "Exposure-Resilient Cryptography", *Massachusetts Institute of Technology*, September 2000.

112. Yevgeniy Dodis and Silvio Micali, "Parallel Reducibility for Information-Theoretically Secure Computation", *Advances in Cryptology — CRYPTO*, August 2000.

113. Yevgeniy Dodis, Shai Halevi and Tal Rabin, "A Cryptographic Solution to a Game Theoretic Problem", *Advances in Cryptology — CRYPTO*, August 2000.

114. Ran Canetti, Yevgeniy Dodis, Shai Halevi, Eyal Kushilevitz and Amit Sahai, "Exposure-Resilient Functions and All-Or-Nothing Transforms", *Advances in Cryptology — EUROCRYPT*, May 2000.

115. Yevgeniy Dodis, Oded Goldreich, Eric Lehman, Sofya Raskhodnikova, Dana Ron, and Alex Samorodnitsky, "Improved Testing Algorithms for Monotonicity", *Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM)*, August 1999. Also available at *Electronic Colloquium on Computational Complexity*, technical report TR99-017, 1999.

116. Yevgeniy Dodis and Sanjeev Khanna, "Space-Time Tradeoffs for Graph Properties", *International Colloquium on Automata, Languages and Programming (ICALP)*, July 1999.

117. Yevgeniy Dodis and Silvio Micali, "Lower Bounds for Oblivious Transfer Reductions", *Advances in Cryptology — EUROCRYPT*, May 1999.

118. Yevgeniy Dodis and Sanjeev Khanna, "Designing Networks with Bounded Pairwise Distance", *ACM Symposium on Theory of Computing (STOC)*, May 1999.

119. Yevgeniy Dodis, Venkatesan Guruswami and Sanjeev Khanna, "The 2-Catalog Segmentation Problem" (Short Form), *ACM/SIAM Symposium on Discrete Algorithms (SODA)*, January 1999.

120. **Master's Thesis**, "Space-Time Tradeoffs for Graph Properties", *Massachusetts Institute of Technology*, May 1998.

121. Yevgeniy Dodis, "Geodesics on Orbifolds", undergraduate research project, *Geometry Center Research Report*, summer 1994. Visit `http://www.geom.umn.edu/apps/pinball` for more information.

Invited Talks at Special Events (in reverse chronological order)

- "Basing Cryptography on Biometrics and Other Noisy Data", plenary speaker at Conference on Information Sciences and Systems, Baltimore, MD, March 2017.
- "Randomness in Cryptography", Mini-Course at Special Semester of Pseudorandomness, Simons Institute for the Theory of Computing, Berkeley, CA, February 2017.
- "Random Oracle and Non-uniformity: Fixing cracks in the concrete", Theory at UBC Mini-Symposium, Vancouver, Canada, February 2017.
- "Randomness in Cryptography", COST-IACR School on Randomness in Cryptography, Pompeu Fabra University, Barcelona, Spain, November 2016.
- "Randomness in Cryptography", Tutorial on Mathematics of Information-Theoretic Cryptography, Institute for Mathematical Sciences, Singapore, September 2016.
- "Spooky Encryption and its Applications", Special Workshop on Coding-Theoretic Methods for Network Security, DIMACS Workshop on Cryptography and its Interactions: Learning Theory, Coding Theory, and Data Structures, Piscataway, NJ, July 2016.
- "Non-malleable Codes", distinguished speaker at the 2016 Capital Area Theory Day, Johns Hopkins University, Baltimore, MD, May 26 2016.
- "Non-malleable Codes", Nexus of Information and Computation Theories, Secrecy and Privacy Theme, Paris, France, March 2016.
- "Non-malleable Codes", invited talk at Theory of Cryptography Conference (TCC'16), Tel Aviv, Israel, January 2016.
- "Backdoorless Cryptography", Second Desert Workshop in Cryptography, Sde Boker Field School, Sde Boker, Israel, January 2016.
- "Randomness in Cryptography", invited talk at Indocrypt'15, Indian Institute of Science, Bangalore, India, December 2015.
- "Backdoorless Cryptography", Special Workshop on Cryptography for Big Data, Columbia University, New York, NY, December 2015.
- "Randomness in Cryptography", Special Workshop on Foundations of Randomness, Stellenbosch Institute for Advanced Study, Stellenbosch, South Africa, October 2015.
- "Non-malleable Codes in the Split-State Model", Special Workshop on The Mathematics of Modern Cryptography, Simons Institute for the Theory of Computing, Berkeley, CA, July 2015.

- "Basing Cryptography on Biometrics and Other Noisy Data", workshop on "Crypto-powered Disruptive Technologies", Yahoo Research, Sunnyvale, CA, July 2015.
- "Non-malleable Codes in the Split-State Model", Special Workshop on Coding-Theoretic Methods for Network Security, DIMACS Center for Discrete Mathematics and Theoretical Computer Science, Piscataway, NJ, April 2015.
- "Random Number Generation, Revisited", New York City BSD User group. New York, NY, April 2014.
- "Random Number Generation, Revisited", Real World Cryptography Workshop. New York, NY, January 2014.
- "Key Derivation Without Entropy Waste", Celebration of the work of Shafi Goldwasser and Silvio Micali. Rehovot, Israel, December 2013.
- "Random Number Generation, Revisited", VMware Labs Academic Symposium. Palo Alto, CA, July 2013.
- "Key Derivation Without Entropy Waste", Workshop on Leakage, Tampering and Viruses. Warsaw, Poland, June 2013.
- "Key Derivation Without Entropy Waste", International State of the Art in Cryptography - Security, Athens, Greece, May 2013,
- "Key Derivation Without Entropy Waste", Special Workshop on Current Trends in Cryptology, AT&T Building, New York, NY, May 2013.
- "Overcoming Weak Expectations", Special Workshop on Information-Theoretic Network Security, DIMACS Center for Discrete Mathematics and Theoretical Computer Science, Piscataway, NJ, November 2012.
- "Overcoming Weak Expectations", Special Workshop on Privacy-Oriented Cryptography, International Conference and Research Center for Computer Science, Dagstuhl, Germany, September, 2012.
- "Overcoming Weak Expectations", Special Cryptography and Complexity Day, Ecole Normale Superieure (ENS), Paris, France, June 2012.
- "Overcoming Weak Expectations", Workshop on "Formal and Computational Cryptographic Proofs", Newton Institute for Mathematical Sciences, Cambridge, England, April 2012.
- "Getting Results under Weak Expectations", Crypto Day, New York, NY, January, 2012.
- "Getting Results under Weak Expectations", Special Workshop on Symmetric-Key Cryptography, International Conference and Research Center for Computer Science, Dagstuhl, Germany, January, 2012.
- "Leftover Hash Lemma, Revisited", Special Workshop on Public-Key Cryptography, International Conference and Research Center for Computer Science, Dagstuhl, Germany, September, 2011.

- "On the (In)Security of RSA Signatures", Special Workshop on Public-Key Cryptography, International Conference and Research Center for Computer Science, Dagstuhl, Germany, September, 2011.
- "Leftover Hash Lemma, Revisited", Special Workshop on Mathematics of Information-Theoretic Cryptography, Institute of Pure and Applied Mathematics, UCLA, Los Angeles, CA, March 2011.
- "Recent Progress in Leakage-Resilient Cryptography", Trends in Theretical Cryptography Conference, Tsinghua University, Beijing, China, January 2011.
- "Recent Progress in Leakage-Resilient Cryptography", Security and Privacy Day, Columbia University, New York, NY, December 2010.
- "Cryptography Against Continuous Memory Attacks", Workshop on Cloud Cryptography, Microsoft Research, Redmond, CA, August 2010.
- "Leakage-Resilience and the Bounded Retrieval Model", Workshop on Provable Security against Physical Attacks. Leiden, Netherlands, February 2010.
- "Leakage-Resilience and the Bounded Retrieval Model", International Conference on Information Theoretic Security, Shizuoka, Japan, December 2009.
- "Leakage-Resilient Cryptography in the Bounded Retrieval Model", Crypto in the Clouds Workshop, MIT, Cambridge, MA, August 2009.
- "Leakage-Resilient Cryptography in the Bounded Retrieval Model", Special Workshop on Cryptographic Protocols, University Residential Center, Bertinoro, Italy, May 2009.
- "Round-Optimal Authenticated Key Agreement from Weak Secrets", Special Workshop on Cryptography, International Conference and Research Center for Computer Science, Dagstuhl, Germany, December 2008.
- "Message Authentication Codes from Unpredictable Block Ciphers", Special Workshop on Cryptography, International Conference and Research Center for Computer Science, Dagstuhl, Germany, December 2008.
- "Game Theory and Cryptography", Invited Course at the Summer School on Game Theory in Computer Science, University Residential Center, Bertinoro, Italy, June 2008.
- "Deniable Authentication", Special Workshop on Data Privacy, DIMACS Center for Discrete Mathematics and Theoretical Computer Science, Piscataway, NJ, February 2008.
- "Does Privacy Require True Randomness?", Special Workshop on Cryptography, International Conference and Research Center for Computer Science, Dagstuhl, Germany, September 2007.
- "Universally Composable Security with Global Setup", Special Workshop on Cryptographic Protocols, University Residential Center, Bertinoro, Italy, March 2007.
- "Does Privacy Require True Randomness?", Special Workshop on Foundations of Secure Multi-Party Computation, Zero-Knowledge and its Applications, Institute of Pure and Applied Mathematics, UCLA, Los Angeles, CA, November 2006.

- "Provable Cryptography Based on Biometrics and Other Noisy Data", Various Faces of Cryptography Conference, Center for Algorithms and Interactive Scientific Software (CAISS), The City College of New York, New York, NY, November 2006.
- "Game Theory and Cryptography", Invited Course at the Summer School on Game Theory in Computer Science, Aarhus University, Denmark, June 2006.
- "On Extractors, Error-Correction and Hiding All Partial Information", Workshop on Cryptography and Information Security (WCIS), Tokyo, Japan, October 2005.
- "On Extractors, Error-Correction and Hiding All Partial Information", Information Theory Workshop (ITW), Awaji Island, Japan, October 2005.
- "On Extractors, Error-Correction and Hiding All Partial Information", Special Workshop on Cryptography, International Conference and Research Center for Computer Science, Dagstuhl, Germany, October 2005.
- "Pairing-Based Verifiable Random Functions", International Workshop on Pairings in Cryptography (PIC), Dublin, Ireland, June 2005.
- "Fully Simulatable Multiparty Computation", Special Workshop on Cryptography, International Center for Mathematical Research, Luminy, France, November 2004.
- "Provable Cryptography Based on Biometrics and Other Noisy Data", Special Workshop on Provable Security, Versailles, France, November 2004.
- "Fully Simulatable Multiparty Computation", Special Workshop on Secure Multiparty Protocols (SMP), Amsterdam, Netherlands, October 2004.
- "On Tolerant and Secure Biometric Technologies; or How to Use Your Fingerprints?", International Conference on Advanced Technologies for Homeland Security (ICATHS), University of Connecticut, Storrs, CT, August 2004.
- "Basing Cryptography on Biometrics and Other Noisy Data", Selected Areas in Cryptography (SAC), University of Waterloo, Waterloo, Ontario, Canada, August 2004.
- "Efficient Construction of (Distributed) Verifiable Random Functions", Special Workshop on Cryptography, International Conference and Research Center for Computer Science, Dagstuhl, Germany, September 2002.
- "Key-Insulated Public Key Cryptosystems", Special Workshop on Cryptographic Protocols, DIMACS Center for Discrete Mathematics and Theoretical Computer Science, Piscataway, NJ, May 2002.
- "Incremental Codes", Special Workshop on Asymptotic and Computational Aspects of Coding Theory, Institute of Advanced Study, Princeton, NJ, March 2001.
- "Exposure-Resilient Cryptography", Special Workshop on Cryptographic Protocols, Centro Stefano Franscini, Monte Verita, Switzerland, March 2001.
- "A Cryptographic Solution to a Game-Theoretic Problem", Special Workshop on Cryptography and Intractability, DIMACS Center for Discrete Mathematics and Theoretical Computer Science, Piscataway, NJ, March 2000.

Other Invited Talks (in reverse chronological order)

- "Random Oracle and Non-uniformity: Fixing cracks in the concrete", Theory Lunch, UB Berkeley, Berkeley, CA, February 2017.
- "Spooky Encryption and its Applications", Departmental Colloquium, Dipartimento di Informatica e Sistemistica, Universita' di Roma "La Sapienza", Italy, October 2016.
- "Non-malleable Codes", Cryptography Seminar, NYU, New York, NY, April 2016.
- "Backdoorless Cryptography", Florida Atlantic University, Boca Raton, FL, November 2015.
- "Non-malleable Codes in the Split-State Model", Algorithms and Complexity Seminar, University of Pennsylvania, Philadelphia, PA, September 2015.
- "Fuzzy Extractors", AT&T Security Conference, Sunnyvale, CA, July 2015.
- "Random Number Generation, Revisited", Cryptography Seminar, Aarhus University, Aarhus, Denmark, May 2014.
- "Random Number Generation, Revisited", Computer Science Colloquium, Georgetown University, Washington, DC, May 2014.
- "Random Number Generation, Revisited", Cornell NYC, New York, NY, March 2014.
- "Key Derivation Without Entropy Waste", Theory Seminar, Rutgers University, Piscataway, NJ, September 2013.
- "Random Number Generation, Revisited", Security Seminar, MIT, Cambridge, MA, September 2013.
- "Key Derivation Without Entropy Waste", Security Seminar, Stanford University, Stanford, CA, July 2013.
- "Key Derivation Without Entropy Waste", Departmental Colloquium, Northeastern University, Boston, MA, May 2013.
- "Key Derivation Without Entropy Waste", Cryptography and Information Security Seminar, MIT, Cambridge, MA, May 2013.
- "Overcoming Weak Expectations", Theory Seminar, Northeastern University, Boston, MA, March 2013.
- "Overcoming Weak Expectations", Security Seminar, Boston University, Boston, MA, March 2013.
- "Overcoming Weak Expectations", Theory Seminar, Penn State University, State College, PA, October 2012.
- "Recent Progress in Leakage-Resilient Cryptography", Cryptography Seminar, University of Luxembourg, Luxembourg, June 2012.
- "Randomness Condensers for Efficiently Samplable, Seed-Dependent Sources", Cryptography Seminar, Ecole Normale Superieure (ENS), Paris, France, June 2012.
- "Recent Progress in Leakage-Resilient Cryptography", Cryptography Seminar, Ecole Normale Superieure (ENS), Paris, France, June 2012.
- "Privacy Amplification Against Active Attackers", Cryptography Seminar, University of Warsaw, Warsaw, Poland, May 2012.

- "Overcoming Weak Expectations", Cryptography Seminar, University of Warsaw, Warsaw, Poland, May 2012.
- "Randomness Condensers for Efficiently Samplable, Seed-Dependent Sources", Cryptography Seminar, University of Warsaw, Warsaw, Poland, May 2012.
- "Randomness Condensers for Efficiently Samplable, Seed-Dependent Sources", Cryptography Seminar, New York University, New York, NY, March 2012.
- "Leftover Hash Lemma, Revisited", Departmental Colloquium, Dipartimento di Informatica e Sistemistica, Universita' di Roma "La Sapienza", Italy, March 2012.
- "Leftover Hash Lemma, Revisited", Cryptography Seminar, New York University, New York, NY, December 2011.
- "Leftover Hash Lemma, Revisited", Theory Colloquium, Brown University, Providence, RI, December 2011.
- "Leftover Hash Lemma, Revisited", Algorithms and Complexity Seminar, University of Pennsylvania, Philadelphia, PA, November 2011.
- "Leftover Hash Lemma, Revisited", Cryptography Seminar, Ecole Normale Superieure (ENS), Paris, France, September 2011.
- "Leftover Hash Lemma, Revisited", Microsoft Research Cryptography Seminar, Microsoft Research, Mountain View, CA, August 2011.
- "On the (In)Security of RSA Signatures", Cryptography and Security Seminar, Stanford University, Stanford, CA, August 2011.
- "Leftover Hash Lemma, Revisited", Microsoft Research Cryptography Seminar, Microsoft Research, Redmond, WA, June 2011.
- "Leftover Hash Lemma, Revisited", Cryptography and Security Seminar, Stanford University, Stanford, CA, June 2011.
- "Leftover Hash Lemma, Revisited", Theory Seminar, University of Chicago, Chicago, IL, May 2011.
- "Leftover Hash Lemma, Revisited", Theory Seminar, Northwestern University, Evanston, IL, May 2011.
- "Leftover Hash Lemma, Revisited", Theory Seminar, University of Southern California, Los Angeles, CA, April 2011.
- "Leftover Hash Lemma, Revisited", Theory Seminar, California Institute of Technology, Pasadena, CA, April 2011.
- "Leftover Hash Lemma, Revisited", Theory Seminar, UC San Diego, San Diego, CA, April 2011.
- "Leftover Hash Lemma, Revisited", Theory of Computation Seminar, Harvard University, Cambridge, MA, March 2011.
- "Cryptography Againt Continuous Memory Attacks", Theory Seminar, University of Chicago, Chicago, IL, October 2010.
- "Recent Progress in Leakage-Resilient Cryptography", Theory Seminar, Northwestern University, Evanston, IL, October 2010.
- "Leakage-Resilience and the Bounded Retrieval Model", Microsoft Research Cryptography Seminar, Microsoft Research, Redmond, WA, August 2010.

- "Leakage-Resilience and the Bounded Retrieval Model", Departmental Colloquium, Dipartimento di Informatica e Sistemistica, Universita' di Roma "La Sapienza", Italy, May 2010.
- "Message Authentication Codes from Unpredictable Block Ciphers", NYU Cryptography Seminar, NYU, New York, NY, October 2009.
- "Adding Robustness to Information-Theoretic Primitives", Departmental Colloquium, Dipartimento di Informatica e Sistemistica, Universita' di Roma "La Sapienza", Italy, May 2009.
- "Non-malleable Extractors and Symmetric-Key Cryptography from Weak Secrets", CMU Theory Seminar, Pittburgh, PA, April 2009.
- "Non-malleable Extractors and Symmetric-Key Cryptography from Weak Secrets", MIT/Microsoft Cryptograpjhy Seminar, Cambridge, MA, April 2009.
- "Non-malleable Extractors and Symmetric-Key Cryptography from Weak Secrets", IBM T.J. Watson Research Center, Hawthorne, NY, March 2009.
- "Non-malleable Extractors and Symmetric-Key Cryptography from Weak Secrets", Theory Colloquium, Brown University, Providence, RI, March 2009.
- "Non-malleable Extractors and Symmetric-Key Cryptography from Weak Secrets", Theory Colloquium, Algorithms and Randomness Center, Georgia Tech Institute of Technology, Atlanta, GA, February 2009.
- "Cryptography from Biometrics and Other Noisy Data", Center for Applied Cybersecurity Speaker Series, Indiana University, Bloomington, Indiana, November 2008.
- "Deniable Authentication", Microsoft Research Cryptography Seminar, Microsoft Research, Redmond, WA, October 2008.
- "Deniable Authentication", Theory Seminar, Cornell University, Ithaca, NY, October 2008.
- "On Extractors, Error-Correction and Hiding All Partial Information", Theory Seminar, New York University, New York, NY, September 2008.
- Series of tutorials in Cryptography (various topics), NTT Labs, Tokyo, Japan, July 2008.
- "Cryptography from Biometrics and Other Noisy Data", Departmental Colloquium, University of Lugano, Lugano, Italy, June 2008.
- "Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors", Cryptography Seminar, University of Salerno, Salerno, Italy, June 2008.
- "Does Privacy Require True Randomness?", Security Seminar, Stanford University, Palo Alto, CA, May 2008.
- " On UC Security, Deniability and Global Setup", Cryptography and Information Security Seminar, MIT, Cambridge, MA, November 2007.
- "Does Privacy Require True Randomness?", Theory Seminar, Harvard University, Cambridge, MA, October 2007.
- "Robust Fuzzy Extractors and Authenticated Key Agreement from Close Secrets", Cryptography Seminar, New York University, New York, NY, May 2007.
- "Does Privacy Require True Randomness?", Cryptography and Information Security Seminar, MIT, Cambridge, MA, April 2007.

- "On Extractors, Error-Correction and Hiding All Partial Information", Departmental Colloquium, University of Connecticut, Storrs, CT, October 2006.
- "On Extractors, Error-Correction and Hiding All Partial Information", 2 lectures at Cryptography Seminar, Aarhus University, Denmark, July 2006.
- "On Extractors, Error-Correction and Hiding All Partial Information", Cryptography Seminar, Ecole Normale Superieure (ENS), Paris, France, June 2006.
- "On Extractors, Error-Correction and Hiding All Partial Information", Cryptography and Information Security Seminar, MIT, Cambridge, MA, March 2006.
- "On Extractors, Error-Correction and Hiding All Partial Information", IBM T.J. Watson Research Center, Hawthorne, NY, Febtuary 2006.
- "On Extractors, Error-Correction and Hiding All Partial Information", Departmental Colloquium, Swiss Federal Institute of Technology (ETH), Zurich, Switzerland, December 2005.
- 4-day Tutorial on "Randomness Extraction and Basing Cryptography On Imperfect Randomness", NTT Labs, Yokosuka R&D Center, Yokosuka, Japan, October 2005.
- "On Extractors, Error-Correction and Hiding All Partial Information", Department of Computer Science, University of California at San Diego (UCSD), San Diego, CA, September 2005.
- "On Extractors, Error-Correction and Hiding All Partial Information", Department of Computer Science, Stanford University, Palo Alto, CA, September 2005.
- "Provable Cryptography Based on Biometrics and Other Noisy Data", Departmental Colloquium, University of Rochester, Rochester, NY, May 2005.
- "Provable Cryptography Based on Biometrics and Other Noisy Data", GEMPLUS, Paris, France, March 2005.
- "Provable Cryptography Based on Biometrics and Other Noisy Data", Departmental Colloquium, University of Rennes, Rennes, France, March 2005.
- "Provable Cryptography Based on Biometrics and Other Noisy Data", Departmental Colloquium, Dipartimento di Informatica e Sistemistica, Universita' di Roma "La Sapienza", Italy, March 2005.
- "Basing Cryptography on Imperfect Randomness", Theory Seminar, New York University, New York, NY, February 2005.
- "Exposure-Resilient Cryptography (Survey)", Departmental Colloquium, Boston University, Boston, MA, December 2004.
- "Fully Simulatable Multiparty Computation", Cryptography and Information Security Seminar, MIT, Cambridge, MA, December 2004.
- "Provable Cryptography Based on Biometrics and Other Noisy Data", Departmental Colloquium, Swiss Federal Institute of Technology (ETH), Zurich, Switzerland, October 2004.
- "Fully Simulatable Multiparty Computation", Departmental Colloquium, Swiss Federal Institute of Technology (ETH), Zurich, Switzerland, October 2004.
- "Provable Cryptography Based on Biometrics and Other Noisy Data", Departmental Colloquium, National Research Institute for Mathematics and Computer Science (CWI), Amsterdam, Netherlands, October 2004.

- "Provable Cryptography Based on Biometrics and Other Noisy Data", Departmental Colloquium, University College London (UCL), London, United Kingdom, September 2004.
- "Provable Cryptography Based on Biometrics and Other Noisy Data", Departmental Colloquium, New York University, New York, NY, September 2004.
- "Breaking and Repairing Optimistic Fair Exchange from PODC 2003", Cryptography Seminar, New York University, New York, NY, May 2004.
- "Exposure-Resilient Cryptography (Survey)", Departmental Colloquium, Swiss Federal Institute of Technology (ETH), Zurich, Switzerland, May 2004.
- "Basing Cryptography on Imperfect Randomness", Cryptography Seminar, Swiss Federal Institute of Technology (ETH), Zurich, Switzerland, May 2004.
- "How to Fool an Unbounded Adversary with a Short Key", Theory Seminar, Princeton University, Princeton, NJ, November 2003.
- "Exposure-Resilient Cryptography (Survey)", Theory Seminar, Columbia University, New York, NY, November 2003.
- "Exposure-Resilient Cryptography (Survey)", Departmental Colloquium, Rutgers University, Piscataway, NJ, November 2003.
- "Exposure-Resilient Cryptography (Survey)", Security Seminar, Stevens Institute of Technology, Hoboken, NJ, September 2003.
- "Basing Cryptography on Imperfect Randomness", Departmental Colloquium, University of California at San Diego, San Diego, CA, June 2003.
- "Basing Cryptography on Imperfect Randomness", Theory Seminar, Princeton University, Princeton, NJ, April 2003.
- "Signcryption: whats, whys and hows", Cryptography and Information Security Seminar, MIT, Cambridge, MA, March 2003.
- "Basing Cryptography on Imperfect Randomness", Theory of Computation Seminar, Harvard University, Cambridge, MA, March 2003.
- "Recent Advances in Broadcast Encryption", Departmental Colloquium, Boston University, Boston, MA, March 2003.
- "Key-Insulated Public Key Cryptosystems", Cryptography and Information Security Seminar, Cryptography Seminar, New York University, February 2003.
- "Efficient Construction of (Distributed) Verifiable Random Functions", Cryptography Seminar, New York University, November 2002.
- "On the Power of Claw-Free Permutations", Cryptography Seminar, New York University, New York, NY, August 2002.
- "Key-Insulated Public Key Cryptosystems", Cryptography and Information Security Seminar, MIT, Cambridge, MA, March 2002.
- "Key-Insulated Public Key Cryptosystems", Departmental Colloquium, University of California at San Diego, San Diego, CA, January 2002.
- "New Imperfect Random Source with Applications to Coin-Flipping", NEC Research Institute, Princeton, NJ, August 2001.
- "Exposure-Resilient Cryptography", Theory Seminar, Princeton University, Princeton, NJ, February 2001.

- "New Imperfect Random Source with Applications to Coin-Flipping", DIMACS Center for Discrete Mathematics and Theoretical Computer Science, Piscataway, NJ, November 2000.
- "Exposure-Resilient Cryptography", PhD Thesis Defense, Massachusetts Institute of Technology, Boston, MA, June 2000.
- "Exposure-Resilient Cryptography", Computer Science Colloquium, New York University, New York, NY, May 2000.
- "A Cryptographic Solution to a Game-Theoretic Problem", Department of Economics, MIT, Cambridge, MA, May 2000.
- "Optimal Lower Bound for Perfect All-Or-Nothing Transforms", Complexity Seminar, MIT, Cambridge, MA, April 2000.
- "Parallel Reducibility for Information Theoretically Secure Computation", Multiparty Computation Seminar, MIT, Cambridge, MA, March 2000.
- "Fault-Tolerant Leader Election and Coin-Flipping — Survey and Recent Developments", Area Exam Defense, MIT, Cambridge, MA, January 2000.
- "Algorithms for Testing Monotonicity", Combinatorics Seminar, MIT, Cambridge, November 1999.
- "Lower Bounds for Oblivious Transfer Reductions", Cryptography Group, IBM Zürich Research Center, Zürich, Switzerland, July 1999.
- "Space-Time Tradeoffs for Graph Properties", Information Security and Cryptography Group, Swiss Federal Institute of Technology (ETH), Zürich, Switzerland, July 1999.
- "Lower Bounds for Oblivious Transfer Reductions", Cryptography and Information Security Seminar, MIT, Cambridge, MA, March 1999.
- "Space-Time Tradeoffs for Graph Properties", Department of Computer Science, Stanford University, Palo Alto, CA, November 1998.
- "Designing Networks with Bounded Pairwise Distance", Algorithms Seminar, MIT, Cambridge, October 1998.
- "Space-Time Tradeoffs for Graph Properties", Cryptography Group, IBM T.J. Watson Research Center, Hawthorne, NY, September 1998.
- "Space-Time Tradeoffs for Graph Properties", Department of Fundamental Mathematics, Bell Labs, Murray Hill, NJ, August 1998.

Conference Talks (in reverse chronological order)

- "Fixing Cracks in the Concrete: Random Oracles with Auxiliary Input, Revisited", EuroCrypt, Paris, France, May 2017.
- 'Interactive Coding for Interactive Protocols", TCC'16, Tel Aviv, Israel, January 2016.
- "Privacy with Imperfect Randomness", CRYPTO, Santa Barbara, CA, August 2015.
- "Key Derivation Without Entropy Waste", EuroCrypt, Copenhagen, Denmark, May 2014.
- "Overcoming Weak Expectations", TCC, Tokyo, Japan, March 2013.
- "Randomness Condensers for Efficiently Samplable, Seed-Dependent Sources", TCC, Taormina, Italy, March 2012.

- "Leftover Hash Lemma, Revisited", CRYPTO, Santa Barbara, CA, August 2011.
- "Public-Key Encryption Schemes with Auxiliary Inputs", TCC, Zurich, Switzerland, February 2010.
- "Robust Fuzzy Extractors and Authenticated Key Agreement from Close Secrets", CRYPTO, Santa Barbara, CA, August 2006.
- "On the Impossibility of Extracting Classical Randomness Using a Quantum Computer", International Colloquium on Automata, Languages and Programming (ICALP), Venice, Italy, July 2006.
- "On the Generic Insecurity of the Full Domain Hash", CRYPTO, Santa Barbara, CA, August 2005.
- "Chosen Ciphertext Security of Multiple Encryption", Theory of Cryptography Conference (TCC), Boston, MA, February 2005.
- "Fuzzy Extractors: How to Generate Strong Keys From Biometrics and Other Noisy Data", EuroCrypt, Interlaken, Switzerland, May 2004.
- "Concealment and its Applications to Authenticated Encryption", EuroCrypt, Warsaw, Poland, May 2003.
- "Efficient Construction of (Distributed) Verifiable Random Functions", International Workshop on Public Key Cryptography (PKC), Miami, Florida, January 2003.
- "On the (non)Universality of the One-Time Pad", Foundations of Computer Science Conference (FOCS), Vancouver, Canada, November 2002.
- "On the Security of Joint Signature and Encryption", EuroCrypt, Amsterdam, Netherlands, May 2002.
- "Incremental Codes", Workshop on Approximation Algorithms for Combinatorial Optimization Problems (APPROX), Berkeley, CA, August 2001.
- "New Imperfect Random Source with Applications to Coin-Flipping", International Colloquium on Automata, Languages and Programming (ICALP), Heraklion (Crete), Greece, July 2001.
- "Universal Configurations in Light-Flipping Games", ACM/SIAM Symposium on Discrete Algorithms (SODA), Washington, DC, January 2001.
- "A Cryptographic Solution to a Game-Theoretic Problem", CRYPTO, Santa Barbara, CA, August 2000.
- "Parallel Reducibility for Information Theoretically Secure Computation", CRYPTO, Santa Barbara, CA, August 2000.
- "Exposure-Resilient Functions and All-Or-Nothing Transforms", EuroCrypt, Brugge, Belgium, May 2000.
- "Space-Time Tradeoffs for Graph Properties", International Colloquium on Automata, Languages and Programming (ICALP), Prague, Czech Republic, July 1999.
- "Designing Networks with Bounded Pairwise Distance", Symposium on Theory of Computing (STOC), Atlanta, GA, May 1999.
- "The 2-Catalog Segmentation Problem", Symposium on Discrete Algorithms (SODA), Baltimore, MD, January 1999.
