January 15, 2015.

CURRICULUM VITAE

Rafail Ostrovsky

HTTP://WWW.CS.UCLA.EDU/~RAFAIL/

MAILING ADDRESS:
UCLA Computer Science Department
3732D Boelter Hall,
Los Angeles, CA, 90095-1596

CONTACT INFORMATION:
Phone: (310) 206-5283
E-mail: RAFAIL@CS.UCLA.EDU

Research Interests

- Cryptography and Computer Security;
- Streaming Algorithms; Routing and Network Algorithms;
- Search and Classification Problems on High-Dimensional Data.

Education

NSF Mathematical Sciences Postdoctoral Research Fellow
Conducted at U.C. Berkeley 1992-95. Host: Prof. Manuel Blum.

Ph.D. in Computer Science, Massachusetts Institute of Technology, 1989-92.

- Thesis titled: "Software Protection and Simulation on Oblivious RAMs", Ph.D. advisor: Prof. Silvio Micali. Final version appeared in Journal of ACM, 1996. Practical applications of thesis work appeared in U.S. Patent No.5,123,045.
- Minor: "Management and Technology", M.I.T. Sloan School of Management.

M.S. in Computer Science, Boston University, 1985-87.

B.A. *Magna Cum Laude* in Mathematics, State University of New York at Buffalo, 1980-84. Department of Mathematics Graduation Honors: *With highest distinction.*

Personal Data

- U.S. citizen, naturalized in Boston, MA, 1986.

Appointments

UCLA Computer Science Department
(2003 – present): Professor of Computer Science.
Recruited in 2003 as a Full Professor with Tenure.

UCLA School of Engineering
(2003 – present): Director, Center for Information and Computation Security. (See http://www.cs.ucla.edu/security/.)

UCLA Department of Mathematics
(2006 – present): Professor of Mathematics (by courtesy).

Appointments (cont.)

Stealth Software Technologies, Inc.

(2008 – present): Serving on the Board of Directors.

Bell Communications Research

(1999 – 2003): Senior Research Scientist;
(1995 – 1999): Research Scientist,
Mathematics and Cryptography Research Group, Applied Research.

Berkeley

(Fall 1992 – August 1995): NSF Mathematical Sciences Postdoctoral Research Fellow. Host: Prof. Manuel Blum.

IBM T.J. Watson Research Center, Hawthorne, New York.

(July – August 1992); (June – September 1991); (July – September 1990): Summer Internship research positions: distributed algorithms, cryptography.

AT&T Bell Laboratories, Murray Hill, New Jersey.

(May – July 1990). Math Research Center. Summer Internship research position: cryptography, distributed and parallel algorithms.

Index Technology Corporation, Cambridge, Massachusetts.

(1987 – 1989). Research Engineer, Product Planning, Architecture and Research Group: algorithm design.

Selected Honors

- Rosalinde and Arthur Gilbert Foundation Research Award, 2014.
- Fellow of International Association of Cryptologic Research (IACR), inducted in 2013.
- Pazy Memorial Research Award, 2012
- Garrick Foundation Award, 2012.
- Invitee to the Third Annual National Security Scholars Conference, 2011 - personal invitation by the Honorable Michael B. Donley, Secretary of the Air Force.
- Quantum Information Processing (QIP) 2011: paper nominated for QIP 2011 plenary talk.
- Plenary Invited Speaker - FBI 2009 conference on cyber security and Law Enforcement.
- Best Paper Award of the 2008 International Conference on Computing and Combinatorics (COCOON-2008);
- Plenary Invited Speaker – Public Key Cryptography international conference, 2007.
- IBM Faculty Award, 2006.
- 2006 Xerox Corporate Innovation Faculty Award.
- 2006 Xerox Corporation Distinguished Lecture Series invited speaker.

Selected Honors (cont.)

- Distinguished Cryptographer of the Year Lecture Series NTT Labs, Kanagawa, Japan, 2005
- B. John Garrick Foundation Research Award, 2005
- 2005 Xerox Corporate Innovation Faculty Award.
- OKAWA Foundation 2004 Research Award.
- SAIC 2002 Publication Prize for Best SAIC-employee Publication in Mathematics and Computer Science (SAIC bought Bellcore in 1997. SAIC was Bellcore Parent company with over 40,000 engineers and scientists at the time of the award).
- SAIC 2001 Publication Prize for Best SAIC-employee Publication in Mathematics and Computer Science.
- SAIC 1999 Publication Prize for Best SAIC-employee Publication in Information and Communications Technology.
- Bellcore prize for excellence in research, 1996.
- Henry H. Taub Prize for the paper "One-Way Functions are Essential for Non-Trivial Zero-Knowledge" 1993.
- NSF Mathematical Sciences Postdoctoral Research Fellowship, 1992-1995.
- IBM Graduate Fellowship, 1990-92.
- SUNY at Buffalo Department of Mathematics Undergraduate Graduation Honors: *With Highest Distinction*, 1984.

Doctoral Students

Listed by Graduation year:

- Alan Roytman (CS Ph.D. 2014, now Postdoc at Tel-Aviv University Computer Science)
- Ran Gelles (CS Ph.D. 2014, now Postdoc at Princeton University Computer Science)
- Silas Richelson (MATH Ph.D. 2014, now Postdoc at UCLA)
- Akshay Wadia (CS Ph.D. 2014, now postdoc EE Department UCLA)
- Chongwon Cho (CS Ph.D. 2013, now Postdoc at HRL)
- Sanjam Garg (CS Ph.D. 2012), now a tenure-track faculty U.C. Berkely. (As my student, Sanjam won 2013 ACM Doctoral Dissertation Award)
- Cheng-Keui Lee (CS Ph.D. 2012, now Security Researcher, LinkedIn)
- Abhishek Jain (CS Ph.D., 2012, now tenure-track faculty at Johns Hopkins University.)
- Hakan Seyalioglu (Math Ph.D., 2012, now researcher at Google.)
- Joshua Baron (Math Ph.D., 2012, now researcher at RAND corporation.)
- Clint Givens (Math Ph.D., 2012, now math instructor in Maine)

Doctoral Students (cont.)

- Vladimir Braverman (C.S. Ph.D. 2011, now C.S. tenure-track faculty at Johns Hopkins University.)
- Nishanth Chandran (C.S. Ph.D. 2011, now researcher at Microsoft Research, India.)
- Omkant Pandey (CS Ph.D., 2010, now Postdoc at UCLA.)
- Brett Hemenway (Math Ph.D., 2010, now tenure-track research professor at U. Penn.)
- Paul Bunn (Math Ph.D., 2010, now researcher at Google.)
- Ryan Moriarty (CS Ph.D., 2010, now entrepreneur in Silicon Valley.)
- Vipul Goyal (CS Ph.D., 2009, now researcher at Microsoft Research, India.)
- Steve Lu (Math Ph.D., 2009, now researcher at UCLA.)
- William Skeith (Math Ph.D., 2007; now CS tenure-track faculty at City College of NY).
- Jonathan Katz (CS Ph.D. 2002, now Professor of CS at U. of Maryland, Director of Maryland Cybersecurity Center (MC2))

Post-Doctoral Fellows

- Dr. Silas Richelson (postdoc 2014 – present)
- Dr. Anat Paskin (postdoc 2012 – 2014) Now tenure-track faculty at Ariel University, Israel.
- Dr. Alessandra Scafuro (postdoc 2012 – 2014) Now Postdoc at Boston Univeristy.
- Dr. Vassilis Zikas (postdoc 2012 – 2014) Now researcher at ETH, Zurich
- Dr. Bhavana Kanukurthi (postodc 2011 –2014) Now tenure-track faculty at IISc, India.
- Dr. Jens Groth (postdoc 2005-2007) now professor at UCL, London.)

Visiting Researchers

- Dr. Steve Lu (researcher at UCLA, 2014-present)
- Dr. Juan Garay (short term visits in 2010, 2011, 2012, 2013, 2014)
- Prof. Yuval Ishai (short term visit in 2012, 2013, 2014)
- Prof. Gepinno Persiano (short term visit in 2012, 2014)
- Prof. Yuval Rabani (short term visits in 2009,2010,2011,2012, 2013, 2014)
- Prof. Eyal Kushulevitz (short term visits in 2008, 2009, 2010, 2011, 2012, 2013, 2014)
- Prof. Ivan Vinsconti (Sabbatical from U. Salerno, 2009-2010 and 2011-2013)
- Dr. Serge Fehr (short term visit in 2011)

Visiting Researchers (cont.)

- Prof. Yuval Ishai (3-year Sabbatical from Technion 2009-2011)
- Claudio Orlandi (6-month visit from Aaharus U. in 2010)
- Prof. Eyal Kushilevitz (6-month sabbatical from Technion, 2010)

Professional Activities

- **Chair of the IEEE Technical Committee on Mathematical Foundations of Computing** 2015–2018. Elected by general voting at FOCS 2014 business meeting. Responsibilities include (among other obligations) selection of Program Committee Chairs for 2016, 2017, 2018 FOCS conferences.
- **Advisory Board Member** UCLA Advisory Board On Privacy and Data Protection 2010–present.
- **Editorial Board member**, Journal of ACM 2014-present.
- **Editorial Board member**, Journal of Cryptology 2006-present.
- **Editorial Board member**, Algorithmica Journal 2005-present.
- **Editorial Board member**, International Journal of Information and Computer Security. 2004-present.
- **Steering Committee member**, Conference on Security and Cryptography for Networks (SCN) 2005-present.
- **Program Committee Chair**, FOCS-2011. 52nd Annual IEEE Symposium on Foundations of Computer Science, October 22-25, 2011 Palm Springs, California
- **Guest Editor** SICOMP Special Issue dedicated to FOCS-2011 best invited papers.
- **UC Privacy and Information Security Steering Committee**, appointed by University of California President, Mark G. Yudof. 2010–2014.
- **Program Committee Chair**, Sixth Conference on Security and Cryptography for Networks Amalfi, September 10-12, 2008. The proceedings of SCN 2008 appeared in LNCS 5229)
- **Program Chair**, IPAM (International Institute of Pure and Applied Mathematics) three month program on Cybersecurity. September trough December 2006 with over fifty participants invited to spend an entire semester in residence at UCLA, and four workshops attracting over 150 participants. (Funded by NSF.)
- **Program Co-chair**, IPAM Workshop Locally decodable codes, PIR, privacy-preserving data-mining, and encryption with special properties. October 25 - 28, 2006, IPAM.
- **Vice-Chair of the IEEE Technical Committee on Mathematical Foundations of Computing** 2012–2014.

Professional Activities (cont.)

- **Program Co-chair**, IPAM Workshop Foundations of secure multi-party computation and zero-knowledge and its applications. November 13 - 17, 2006, IPAM.
- **Program Co-chair**, Dagshtul Workshop Anonymous Communication and its Applications October 9-14, 2005.
- **Program Co-chair,** IPAM Workshop Multiscale Geometry and Analysis in High Dimensions October 19-23, 2004.
- **Program Co-chair**, DIMACS Workshop Cryptographic Protocols in Complex Environments May 15-17, 2002.
- Program committee member PODS-2011. ACM SIGMOD/PODS Conference, Athens, Greece
- Program committee member ICALP-2011. The 38th International Colloquium on Automata, Languages and Programming, July 4-8, Zrich, Switzerland.
- Program committee member EUROCRYPT-2011. May 15th-19th, 2011, Tallinn, Estonia
- Program committee member CT-RSA 2011. The Cryptographers' Track (CT-RSA) is a crypto research conference within the RSA 2011 Conference.
- Program committee member TCC-2010: Seventh Theory of Cryptography Conference, 2010.
- Program committee member EUROCRYPT-2009 Cologne, April 26-30, 2009.
- Program committee member Algosensors-2009 5th International Workshop on Algorithmic Aspects of Wireless Sensor Networks 2009.
- Program committee member FOCS-2008 49th Annual IEEE Symposium on Foundations of Computer Science.
- Program committee member PKC-2007: International Workshop on Practice and Theory in Public Key Cryptography, (Apr 17-19 2007, Beijing). China 2007
- Program committee member ACISP-2007: Australian Conference on Information Security and Privacy July 2-6, 2007, Townsville, Queensland, Australia.
- Program committee member ICALP-2006: 33rd International Colloquium on Automata, Languages and Programming, July 9-16, 2006, Venice, Italy.
- Program committee member STOC-2006: Annual ACM Symposium on Theory of Computing, May 2006.

Professional Activities (cont.)

- Program committee member PKC-2006: International Workshop on Practice and Theory in Public Key Cryptography, April 24-26, New York City, USA.
- Program committee member INDOCRYPT-2005 December 10-12, 2005 Indian Institute of Science Bangalore, India, 2005.
- Program committee member Eurocrypt-2005, Aarhus, May 22-26, 2005.
- Program committee member TCC-2005: Second Theory of Cryptography Conference, Feb 2005.
- Program committee member SCN-2004: Security in Communication Networks 2004 (SCN'04) September 8-10, Amalfi, Italy.
- Program committee member PODC-2004: 23rd Annual ACM Symposium on Principles of Distributed Computing, July 2004.
- Program committee member CRYPTO-2004: 24nd Annual IACR/IEEE Conference on Cryptologic Research,
- Program committee member CRYPTO-2003: 23rd Annual IACR/IEEE Conference on Cryptologic Research,
- Program committee member STOC-2003: Annual ACM Symposium on Theory of Computing May of 2003.
- Program committee member CRYPTO-2002: 22nd Annual IACR/IEEE Conference on Cryptologic Research.
- Program committee member RANDOM-2002: The 6th International Workshop on Randomization and Approximation Techniques in Computer Science, September 13-15, 2002.
- Program committee member SCN-2002: Third Workshop on Security in Communication Networks, September 2002, Amalfi, Italy
- Program committee member STOC-2000:Annual ACM Symposium on Theory of Computing, 2000.
- Program committee member SODA-2000: Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms, January 1-9, 2000, San Francisco.
- Program committee member SCN-99: Second Workshop on Security in Communication Networks, September 1999, Amalfi, Italy
- Program committee member CRYPTO-98: 18th Annual IACR/IEEE Conference on Cryptologic Research 1998.
- Program committee member ISTCS-97: 5th ISRAEL Symposium on Theory of Computing and Systems, 1997.

Patents

1. Oded GOLDREICH and Rafail OSTROVSKY "COMPREHENSIVE SOFTWARE PROTECTION SYSTEM" U.S. Patent No.5,123,045.
2. Rafail OSTROVSKY and Eyal KUSHILEVITZ, "METHOD AND APPARATUS FOR PRIVATE INFORMATION RETRIEVAL FROM A SINGLE ELECTRONIC STORAGE DEVICE" U.S. Patent 6,167,392.
3. Rafail OSTROVSKY, Giovanni DI CRESCENZO, And Yuval ISHAI, "METHOD AND SYSTEM FOR NON-MALLEABLE AND NON-INTERACTIVE CRYPTOGRAPHIC COMMITMENT IN A NETWORK" U.S. Patent 6,301,664.
4. Rafail OSTROVSKY And Yuval RABANI, "METHOD AND SYSTEM FOR DETERMINING APPROXIMATE HAMMING DISTANCE AND APPROXIMATE NEAREST NEIGHBORS IN AN ELECTRONIC STORAGE DEVICE" U.S. Patent 6,226,640.
5. William AIELLO, Rafail OSTROVSKY, And Sachin LODHA "A METHOD FOR EFFICIENTLY REVOKING DIGITAL IDENTITIES" U.S. Patent 6,397,329.
6. Rafail OSTROVSKY, Yuval ISHAI, AND Giovanni DI-CRESCENZO, "METHOD AND SYSTEM FOR PRIVATE INFORMATION RETRIEVAL USING COMMODITIES" U.S. Patent 6,216,128.
7. Rafail OSTROVSKY, Yuval ISHAI, AND Giovanni DI-CRESCENZO, "SYSTEM AND METHOD FOR PRIVATE INFORMATION RETRIEVAL USING VERIFIABLE COMMODITIES" U.S. Patent 6,438,554.
8. Giovanni DI-CRESCENZO, AND Rafail OSTROVSKY AND S. RAJAGOPALAN "METHOD AND SYSTEM FOR TIMED-RELEASE PUBLIC-KEY ENCRYPTION" U.S. Patent 6,813,358.
9. Rafail OSTROVSKY AND Yuval RABANI METHOD FOR LOW DISTORTION EMBEDDING OF EDIT DISTANCE TO HAMMING DISTANCE. US Patent 8,060,808.
10. Rafail OSTROVSKY AND William E. SKEITH III METHOD FOR PRIVATE KEYWORD SEARCH ON STREAMING DATA US Patent 8,291,237.
11. Rafail OSTROVSKY APPARATUS, SYSTEM, AND METHOD TO EFFICIENTLY SEARCH AND MODIFY INFORMATION STORED ON REMOTE SERVERS, WHILE HIDING ACCESS PATTERNS US Patent 8,364,979.
12. Yair AMIR AND Paul BUNN and Rafail OSTROVSKY AUTHENTICATED ADVERSARIAL ROUTING (application) US Pat. 12,922,141 - Filed Mar 13, 2009.

Recent Invited Talks (*)

- Invited talk: Distinguished Lecturer of the Year, Johns Hopkins University Computer Science Department, November 13, 2014.
- Invited talk: "Big Thinker Lecture Series" Yahoo Labs, Sunnyvale, California, March 19, 2014.
- Invited talk: Novel Privacy-Enhancing Technologies. UCLA Henry Samueli School of Engineering and Applied Science, 2012 Technology Forum, March 13, 2012.
- Invited talk: NIST Privacy Enhancing Crytpography Meeting By invitation only Workshop for Industry, Governnment and Academia, November 8, 2011.
- Invited talk: Success Stories and Challenges in Cybersecurity September 21, 2011, Institute of Pure and Applied Mathematics, Los Angeles.
- Invited Scholar: U.S. Air Force Third Annual National Security Scholars Conference. April 26, 2011. (Invited by the Honorable Michael B. Donley, Secretary of the Air Force.)
- Invited talk: Mathematics of Information-Theoretic Cryptography IPAM, UCLA, March 3, 2011.
- Invited talk: Trends in Theoretical Cryptography (TTC 2011) January 10-12, 2011, Tsinghua University, Beijing, China.
- Invited talk: MIT CSAIL Theory Colloquium December 7, 2010.
- Invited talk: MIT Quantum Information Processing (QIP) seminar, December 6, 2010.
- Invited talk: Caltech Computing and Mathematical Sciences Lecture Series November 17, 2010.
- Invited talk: Aerospace Corporation Information Assurance Technology Department, Computers and Software Division, Octover 7, 2010.
- Invited talk: 2010 Lockheed-Martin Anti-Tamper Conference, August 26, 2010, Forth Worth, Texas.
- Invited talk: 2009 Workshop on Cryptographic Protocols and Public-Key Cryptography May 24-29 2009, Bertinoro, Italy.
- Distinguished Lecturer Seminar Series, U.C. Irvine Computer Science Department, May 15, 2009.
- Plenary invited speaker at International Conference on Cyber Security 2009 organized by FBI and Fordham university.
- Plenary keynote speaker at PKC-2007 International Workshop on Practice and Theory in Public Key Cryptography, China 2007.

(*) I did not keep detailed notes of my talks prior to September 2005, the ballpark is over a hundred invited talks from 1989 to 2005.

Recent Invited Talks (Since 2005)

- Invited talk: Sun Microsystems, 2007 Distinguished Lecture Series, January 2007, Palo Alto, CA, USA
- Invited tutorial: Series of IPAM lectures on Private Information Retrieval September 2006, Los Angeles, CA, USA.
- Two invited tutorials at Homeland Defense and Security Conference 18-21 Octover 2006, Sorrento, Italy.
- Invited talk: 2006 Xerox Corporation Distinguished Lecture Series Los Angeles, July 2006. USA
- Invited talk: Workshop on Data Surveillance and Privacy Protection Workshop Harvard, June 2006.
- Invited talk: Workshop on classical and quantum information security, Caltech, December 15-18, 2005.
- Invited talk: Interdepartmental Seminar on Algorithmics University of Rome "La Sapienza", Italy. November 21, 2005.
- Invited talk: 2005 Distinguished Cryptographer Lecture Series NTT Labs, Kanagawa, Japan, October 2005.
- Invited talk: Workshop on Cryptography and Information Security 2005 Tokyo, Japan, October 21, 2005.
- Invited talk: IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security Awaji Island, Japan, October 16- 19, 2005.
- Invited talk: Dagshtul Workshop. Germany, October 9-14, 2005.
- Invited talk: Southern California Security and Cryptography Workshop September 24, 2005, Irvine, CA. USA
- Invited talk: Bertinoro Invited one-week course, International PhD School on Mathematical Aspects of Modern Cryptography, Bertinoro, Italy September 4-9, 2005.

Funding

- **The Defense Advanced Research Projects Agency (DARPA)**
  - (2011-2015) I20 PROCEED program funded through the U.S. Office of Naval Research under Contract N00014-11-1-0392. “Novel Foundations of Advanced Security Technologies (N-Fast)”.

- **National Science Foundation:**
  - (1992-1995) DMS-9206267;
  - (2004-2009) CNS-0430254;
  - (2007-2012) CNS-0716835;
  - (2007-2012) CNS-0716389;
  - (2008-2013) CNS-0830803;
  - (2009-2014) CCF-0916574
  - (2010-2015) IIS-1065276;
  - (2010-2012) CCF-1016540;
  - (2011-2015) CNS-1118126;
  - (2011-2015) CNS-1136174

- **United States-Israel Binational Science Foundation:**
  - (2012-2016) BSF-2012378;
  - (2008-2012) BSF-2008411;
  - (2002-2008) BSF-2002354;

- **California State Funding**
  - (2007) UC Innovation and Computer Research grant;

- **Foundations and Industry**
  - (2014) Rosalinde and Arthur Gilbert Foundation Award;
  - (2012) Pazy Memorial Award;
  - (2012) Garrick Foundation Award;
  - (2007) Lockheed-Martin Corporation;
  - (2006) IBM Faculty Award;
  - (2006) Xerox Corporate Award;
  - (2005) Garrick Foundation Award;
  - (2005) Teradata Corporate Award;
  - (2004) OKAWA Foundation Award;
  - (2003) Intel Corporation Award;

Publications[1]

Books

[1] Rafail Ostrovsky. Software Protection and Simulation on Oblivious RAMs. Ph.D. Thesis. Massachusetts Institute of Technology Dept. of Electrical Engineering and Computer Science. 1992. *Software protection and simulation on oblivious RAMs.* Thesis (Ph. D.)–Massachusetts Institute of Technology, Dept. of Electrical Engineering and Computer Science, 1992.

Book/Volume Editor

[2] Eli Ben-Sasson and Rafail Ostrovsky (editors). Special issue on the fifty-second IEEE annual symposium on foundations of computer science (FOCS 2011). *SIAM J. Comput.*, 43(2):654, 2014.

[3] Shlomi Dolev, Rafail Ostrovsky, and Andreas Pfitzmann, editors. *Anonymous Communication and its Applications, 09.10. - 14.10.2005*, volume 05411 of *Dagstuhl Seminar Proceedings*. Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany, 2006.

[4] Rafail Ostrovsky, editor. *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011.* IEEE, 2011.

[5] Rafail Ostrovsky, Roberto De Prisco, and Ivan Visconti, editors. *Security and Cryptography for Networks, 6th International Conference, SCN 2008, Amalfi, Italy, September 10-12, 2008. Proceedings*, volume 5229 of *Lecture Notes in Computer Science*. Springer, 2008.

Book Chapters

[6] Allan Borodin, Rafail Ostrovsky, and Yuval Rabani. *In Discrete and Computational Geometry - The Goodman-Pollack Festschrift. Algorithms and Combinatorics Series 3143*, chapter Lower Bounds for High Dimensional Nearest Neighbor Search and Related Problems, pages 255–276. Springer Verlag, Berlin, 2003.

[7] Rafail Ostrovsky and William E. Skeith III. Private Information Retrieval: Single-Database Techniques and Applications. In G. Franceschetti and M. Grossi, editors, *Homeland Security Technology Challenges*, pages 143–176. Artech House Publishing, 2008.

[8] Rafail Ostrovsky, Ramarathnam Venkatesan, and Moti Yung. Fair Games Against an All-Powerful Adversary (full version). In Jin-Yi Cai, editor, *DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Vol. 13*, pages 155–169. AMS, 1993. This

[1] In alphabetical order by publication type.

work was first presented at DIMACS Complexity and Cryptography Workshop, October 1990, Princeton, NJ.

[9] Rafail Ostrovsky and Moti Yung. On necessary conditions for secure distributed computing. In *DIMACS Workshop on Distributed Computing and Cryptography, Feigenbaum and Merritt (eds.), AMS*, pages 229–234. 1990.

Journal Publications

[10] William Aiello, Eyal Kushilevitz, Rafail Ostrovsky, and Adi Rosén. Adaptive packet routing for bursty adversarial traffic. *J. Comput. Syst. Sci.*, 60(3):482–509, 2000.

[11] Yair Amir, Paul Bunn, and Rafail Ostrovsky. Authenticated adversarial routing. *J. Cryptology*, 27(4):636–771, 2014.

[12] Leonid Barenboim, Shlomi Dolev, and Rafail Ostrovsky. Deterministic and energy-optimal wireless synchronization. *TOSN*, 11(1):13, 2014.

[13] Joshua Baron, Karim El Defrawy, Kirill Minkovich, Rafail Ostrovsky, and Eric Tressler. 5pm: Secure pattern matching. *Journal of Computer Security*, 21(5):601–625, 2013.

[14] Joshua Baron, Yuval Ishai, and Rafail Ostrovsky. On linear-size pseudorandom generators and hardcore functions. *Theor. Comput. Sci.*, 554:50–63, 2014.

[15] Nir Bitansky, Alessandro Chiesa, Yuval Ishai, Rafail Ostrovsky, and Omer Paneth. Succinct non-interactive arguments via linear interactive proofs. In *TCC*, pages 315–333, 2013.

[16] Allan Borodin, Rafail Ostrovsky, and Yuval Rabani. Stability preserving transformations: Packet routing networks with edge capacities and speeds. *Journal of Interconnection Networks*, 5(1):1–12, 2004.

[17] Allan Borodin, Rafail Ostrovsky, and Yuval Rabani. Subquadratic approximation algorithms for clustering problems in high dimensional spaces. *Machine Learning*, 56(1-3):153–167, 2004.

[18] Milan Bradonjic, Eddie Kohler, and Rafail Ostrovsky. Near-optimal radio use for wireless network synchronization. *Theor. Comput. Sci.*, 453:14–28, 2012.

[19] Vladimir Braverman, Ran Gelles, and Rafail Ostrovsky. How to catch l_2-heavy-hitters on sliding windows. *Theor. Comput. Sci.*, 554:82–94, 2014.

[20] Vladimir Braverman and Rafail Ostrovsky. Effective computations on sliding windows. *SIAM J. Comput.*, 39(6):2113–2131, 2010.

[21] Vladimir Braverman, Rafail Ostrovsky, and Carlo Zaniolo. Optimal sampling from sliding windows. *J. Comput. Syst. Sci.*, 78(1):260–272, 2012.

[22] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. *SIAM J. Comput.*, 43(1):150–178, 2014.

[23] Ran Canetti, Eyal Kushilevitz, Rafail Ostrovsky, and Adi Rosén. Randomness versus fault-tolerance. *J. Cryptology*, 13(1):107–142, 2000.

[24] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position-based cryptography. *SIAM J. Comput.*, 43(4):1291–1341, 2014.

[25] Nishanth Chandran, Bhavana Kanukurthi, Rafail Ostrovsky, and Leonid Reyzin. Privacy amplification with asymptotically optimal entropy loss. *J. ACM*, 61(5):29, 2014.

[26] Nishanth Chandran, Ryan Moriarty, Rafail Ostrovsky, Omkant Pandey, Mohammad Ali Safari, and Amit Sahai. Improved algorithms for optimal embeddings. *ACM Transactions on Algorithms*, 4(4), 2008.

[27] Julia Chuzhoy, Rafail Ostrovsky, and Yuval Rabani. Approximation algorithms for the job interval selection problem and related scheduling problems. *Math. Oper. Res.*, 31(4):730–738, 2006.

[28] Giovanni Di Crescenzo, Yuval Ishai, and Rafail Ostrovsky. Universal service-providers for private information retrieval. *J. Cryptology*, 14(1):37–74, 2001.

[29] Reza Curtmola, Juan A. Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: Improved definitions and efficient constructions. *Journal of Computer Security*, 19(5):895–934, 2011.

[30] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.*, 38(1):97–139, 2008.

[31] Shlomi Dolev and Rafail Ostrovsky. Xor-trees for efficient anonymous multicast and reception. *ACM Trans. Inf. Syst. Secur.*, 3(2):63–84, 2000.

[32] Matthias Fitzi, Juan A. Garay, Ueli M. Maurer, and Rafail Ostrovsky. Minimal complete primitives for secure multi-party computation. *J. Cryptology*, 18(1):37–61, 2005.

[33] Matthew K. Franklin, Ran Gelles, Rafail Ostrovsky, and Leonard J. Schulman. Optimal coding for streaming authentication and interactive communication. *IEEE Transactions on Information Theory*, 61(1):133–145, 2015.

[34] Juan A. Garay, Clint Givens, and Rafail Ostrovsky. Secure message transmission with small public discussion. *IEEE Transactions on Information Theory*, 60(4):2373–2390, 2014.

[35] Oded Goldreich and Rafail Ostrovsky. Software protection and simulation on oblivious rams. *J. ACM*, 43(3):431–473, 1996.

[36] Oded Goldreich, Rafail Ostrovsky, and Erez Petrank. Computational complexity and knowledge complexity. *SIAM J. Comput.*, 27(4):1116–1141, 1998.

[37] Jens Groth and Rafail Ostrovsky. Cryptography in the multi-string model. *J. Cryptology*, 27(3):506–543, 2014.

[38] Jens Groth, Rafail Ostrovsky, and Amit Sahai. New techniques for noninteractive zero-knowledge. *J. ACM*, 59(3):11, 2012.

[39] Farhad Hormozdiari, Jong Wha J. Joo, Akshay Wadia, Feng Guan, Rafail Ostrovsky, Amit Sahai, and Eleazar Eskin. Privacy preserving protocol for detecting genetic relatives using rare variants. *Bioinformatics*, 30(12):204–211, 2014.

[40] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Zero-knowledge proofs from secure multiparty computation. *SIAM J. Comput.*, 39(3):1121–1152, 2009.

[41] Jonathan Katz, Rafail Ostrovsky, and Moti Yung. Efficient and secure authenticated key exchange using weak passwords. *J. ACM*, 57(1), 2009.

[42] Joe Kilian, Eyal Kushilevitz, Silvio Micali, and Rafail Ostrovsky. Reducibility and completeness in private computations. *SIAM J. Comput.*, 29(4):1189–1208, 2000.

[43] Eyal Kushilevitz, Nathan Linial, and Rafail Ostrovsky. The linear-array conjecture in communication complexity is false. *Combinatorica*, 19(2):241–254, 1999.

[44] Eyal Kushilevitz, Rafail Ostrovsky, and Yuval Rabani. Efficient search for approximate nearest neighbor in high dimensional spaces. *SIAM J. Comput.*, 30(2):457–474, 2000.

[45] Eyal Kushilevitz, Rafail Ostrovsky, and Adi Rosén. Log space polynomial end to end communication. *SIAM J. Comput.*, 27(6):1531–1549, 1998.

[46] Eyal Kushilevitz, Rafail Ostrovsky, and Adi Rosén. Characterizing linear size circuits in terms of pricacy. *J. Comput. Syst. Sci.*, 58(1):129–136, 1999.

[47] Eyal Kushilevitz, Rafail Ostrovsky, and Adi Rosén. Amortizing randomness in private multiparty computations. *SIAM J. Discrete Math.*, 16(4):533–544, 2003.

[48] Shay Kutten, Rafail Ostrovsky, and Boaz Patt-Shamir. The las-vegas processor identity problem (how and when to be unique). *J. Algorithms*, 37(2):468–494, 2000.

[49] Steve Lu, Daniel Manchala, and Rafail Ostrovsky. Visual cryptography on graphs. *J. Comb. Optim.*, 21(1):47–66, 2011.

[50] Steve Lu, Rafail Ostrovsky, Amit Sahai, Hovav Shacham, and Brent Waters. Sequential aggregate signatures, multisignatures, and verifiably encrypted signatures without random oracles. *J. Cryptology*, 26(2):340–373, 2013.

[51] Alain J. Mayer, Rafail Ostrovsky, Yoram Ofek, and Moti Yung. Self-stabilizing symmetry breaking in constant space. *SIAM J. Comput.*, 31(5):1571–1595, 2002.

[52] Moni Naor, Rafail Ostrovsky, Ramarathnam Venkatesan, and Moti Yung. Perfect zero-knowledge arguments for *np* using any one-way permutation. *J. Cryptology*, 11(2):87–108, 1998.

[53] Rafail Ostrovsky and William E. Skeith III. Private searching on streaming data. *J. Cryptology*, 20(4):397–430, 2007.

[54] Rafail Ostrovsky and Yuval Rabani. Polynomial-time approximation schemes for geometric min-sum median clustering. *J. ACM*, 49(2):139–156, 2002.

[55] Rafail Ostrovsky and Yuval Rabani. Low distortion embeddings for edit distance. *J. ACM*, 54(5), 2007.

[56] Rafail Ostrovsky, Yuval Rabani, and Leonard J. Schulman. Error-correcting codes for automatic control. *IEEE Transactions on Information Theory*, 55(7):2931–2941, 2009.

[57] Rafail Ostrovsky, Yuval Rabani, Leonard J. Schulman, and Chaitanya Swamy. The effectiveness of lloyd-type methods for the k-means problem. *J. ACM*, 59(6):28, 2012.

Refereed Conference Proceedings

[58] William Aiello, Eyal Kushilevitz, Rafail Ostrovsky, and Adi Rosén. Adaptive packet routing for bursty adversarial traffic. In *STOC*, pages 359–368, 1998.

[59] William Aiello, Eyal Kushilevitz, Rafail Ostrovsky, and Adi Rosén. Dynamic routing on networks with fixed-size buffers. In *SODA*, pages 771–780, 2003.

[60] William Aiello, Sachin Lodha, and Rafail Ostrovsky. Fast digital identity revocation. In *CRYPTO*, pages 137–152, 1998.

[61] Noga Alon, Manuel Blum, Amos Fiat, Sampath Kannan, Moni Naor, and Rafail Ostrovsky. Matching nuts and bolts. In *SODA*, pages 690–696, 1994.

[62] Yair Amir, Paul Bunn, and Rafail Ostrovsky. Authenticated adversarial routing. In *TCC*, pages 163–182, 2009.

[63] Prabhanjan Ananth, Nishanth Chandran, Vipul Goyal, Bhavana Kanukurthi, and Rafail Ostrovsky. Achieving privacy in verifiable computation with multiple servers - without FHE and without pre-processing. In *Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014. Proceedings*, pages 149–166, 2014.

[64] Baruch Awerbuch and Rafail Ostrovsky. Memory-efficient and self-stabilizing network reset. In *PODC*, pages 254–263, 1994.

[65] Leonid Barenboim, Shlomi Dolev, and Rafael Ostrovsky. Deterministic and energy-optimal wireless synchronization. In *DISC*, pages 237–251, 2011.

[66] Joshua Baron, Karim El Defrawy, Joshua Lampkins, and Rafail Ostrovsky. How to withstand mobile virus attacks, revisited. In *ACM Symposium on Principles of Distributed Computing, PODC '14, Paris, France, July 15-18, 2014*, pages 293–302, 2014.

[67] Joshua Baron, Karim El Defrawy, Kirill Minkovich, Rafail Ostrovsky, and Eric Tressler. 5pm: Secure pattern matching. In *SCN*, pages 222–240, 2012.

[68] Joshua Baron, Yuval Ishai, and Rafail Ostrovsky. On linear-size pseudorandom generators and hardcore functions. In *Computing and Combinatorics, 19th International Conference, COCOON 2013, Hangzhou, China, June 21-23, 2013. Proceedings*, pages 169–181, 2013.

[69] Joshua Baron, Rafail Ostrovsky, and Ivan Visconti. Nearly simultaneously resettable black-box zero knowledge. In *ICALP (1)*, pages 88–99, 2012.

[70] Mihir Bellare, Silvio Micali, and Rafail Ostrovsky. Perfect zero-knowledge in constant rounds. In *STOC*, pages 482–493, 1990.

[71] Mihir Bellare, Silvio Micali, and Rafail Ostrovsky. The (true) complexity of statistical zero knowledge. In *STOC*, pages 494–502, 1990.

[72] Eli Ben-Sasson, Serge Fehr, and Rafail Ostrovsky. Near-linear unconditionally-secure multiparty computation with a dishonest minority. In *CRYPTO*, pages 663–680, 2012.

[73] Nir Bitansky, Alessandro Chiesa, Yuval Ishai, Rafail Ostrovsky, and Omer Paneth. Succinct non-interactive arguments via linear interactive proofs. In *TCC*, pages 315–333, 2013.

[74] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In *EUROCRYPT*, pages 506–522, 2004.

[75] Dan Boneh, Shai Halevi, Michael Hamburg, and Rafail Ostrovsky. Circular-secure encryption from decision diffie-hellman. In *CRYPTO*, pages 108–125, 2008.

[76] Dan Boneh, Eyal Kushilevitz, Rafail Ostrovsky, and William E. Skeith III. Public key encryption that allows pir queries. In *CRYPTO*, pages 50–67, 2007.

[77] Allan Borodin, Rafail Ostrovsky, and Yuval Rabani. Lower bounds for high dimensional nearest neighbor search and related problems. In *STOC*, pages 312–321, 1999.

[78] Allan Borodin, Rafail Ostrovsky, and Yuval Rabani. Subquadratic approximation algorithms for clustering problems in high dimensional spaces. In *STOC*, pages 435–444, 1999.

[79] Allan Borodin, Rafail Ostrovsky, and Yuval Rabani. Stability preserving transformations: packet routing networks with edge capacities and speeds. In *SODA*, pages 601–610, 2001.

[80] Xavier Boyen, Yevgeniy Dodis, Jonathan Katz, Rafail Ostrovsky, and Adam Smith. Secure remote authentication using biometric data. In *EUROCRYPT*, pages 147–163, 2005.

[81] Milan Bradonjic, Eddie Kohler, and Rafail Ostrovsky. Near-optimal radio use for wireless network synchronization. In *ALGOSENSORS*, pages 15–28, 2009.

[82] Vladimir Braverman, Kai-Min Chung, Zhenming Liu, Michael Mitzenmacher, and Rafail Ostrovsky. Ams without 4-wise independence on product domains. In *STACS*, pages 119–130, 2010.

[83] Vladimir Braverman, Ran Gelles, and Rafail Ostrovsky. How to catch L_2-heavy-hitters on sliding windows. In *Computing and Combinatorics, 19th International Conference, COCOON 2013, Hangzhou, China, June 21-23, 2013. Proceedings*, pages 638–650, 2013.

[84] Vladimir Braverman, Adam Meyerson, Rafail Ostrovsky, Alan Roytman, Michael Shindler, and Brian Tagiku. Streaming k-means on well-clusterable data. In *SODA*, pages 26–40, 2011.

[85] Vladimir Braverman and Rafail Ostrovsky. Smooth histograms for sliding windows. In *FOCS*, pages 283–293, 2007.

[86] Vladimir Braverman and Rafail Ostrovsky. Measuring independence of datasets. In *STOC*, pages 271–280, 2010.

[87] Vladimir Braverman and Rafail Ostrovsky. Zero-one frequency laws. In *STOC*, pages 281–290, 2010.

[88] Vladimir Braverman and Rafail Ostrovsky. Approximating large frequency moments with pick-and-drop sampling. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques - 16th International Workshop, APPROX 2013, and 17th International Workshop, RANDOM 2013, Berkeley, CA, USA, August 21-23, 2013. Proceedings*, pages 42–57, 2013.

[89] Vladimir Braverman and Rafail Ostrovsky. Generalizing the layering method of indyk and woodruff: Recursive sketches for frequency-based vectors on streams. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques - 16th International Workshop, APPROX 2013, and 17th International Workshop, RANDOM 2013, Berkeley, CA, USA, August 21-23, 2013. Proceedings*, pages 58–70, 2013.

[90] Vladimir Braverman, Rafail Ostrovsky, and Dan Vilenchik. How hard is counting triangles in the streaming model? In *Automata, Languages, and Programming - 40th International Colloquium, ICALP 2013, Riga, Latvia, July 8-12, 2013, Proceedings, Part I*, pages 244–254, 2013.

[91] Vladimir Braverman, Rafail Ostrovsky, and Carlo Zaniolo. Optimal sampling from sliding windows. In *PODS*, pages 147–156, 2009.

[92] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. In *CRYPTO*, pages 429–446, 2011.

[93] Paul Bunn and Rafail Ostrovsky. Secure two-party k-means clusteoring. In *ACM Conference on Computer and Communications Security*, pages 486–497, 2007.

[94] Paul Bunn and Rafail Ostrovsky. Asynchronous throughput-optimal routing in malicious networks. In *ICALP (2)*, pages 236–248, 2010.

[95] Ran Canetti, Cynthia Dwork, Moni Naor, and Rafail Ostrovsky. Deniable encryption. In *CRYPTO*, pages 90–104, 1997.

[96] Ran Canetti, Eyal Kushilevitz, Rafail Ostrovsky, and Adi Rosén. Randomness vs. fault-tolerance. In *PODC*, pages 35–44, 1997.

[97] Ran Canetti, Yehuda Lindell, Rafail Ostrovsky, and Amit Sahai. Universally composable two-party and multi-party secure computation. In *STOC*, pages 494–503, 2002.

[98] Ran Canetti and Rafail Ostrovsky. Secure computation with honest-looking parties: What if nobody is truly honest? In *STOC*, pages 255–264, 1999.

[99] Alfonso Cevallos, Serge Fehr, Rafail Ostrovsky, and Yuval Rabani. Unconditionally-secure robust secret sharing with compact shares. In *EUROCRYPT*, pages 195–208, 2012.

[100] Nishanth Chandran, Wutichai Chongchitmate, Juan A. Garay, Shafi Goldwasser, Rafail Ostrovsky, and Vassilis Zikas. Optimally resilient and adaptively secure multi-party computation with low communication locality. In *The 6th Innovations in Theoretical Computer Science (ITCS), Weizmann Institute of Science, Israel, January 11-13, 2015.*

[101] Nishanth Chandran, Juan A. Garay, and Rafail Ostrovsky. Improved fault tolerance and secure computation on sparse networks. In *ICALP (2)*, pages 249–260, 2010.

[102] Nishanth Chandran, Juan A. Garay, and Rafail Ostrovsky. Edge fault tolerance on sparse networks. In *ICALP (2)*, pages 452–463, 2012.

[103] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position based cryptography. In *CRYPTO*, pages 391–407, 2009.

[104] Nishanth Chandran, Vipul Goyal, Rafail Ostrovsky, and Amit Sahai. Covert multi-party computation. In *FOCS*, pages 238–248, 2007.

[105] Nishanth Chandran, Bhavana Kanukurthi, and Rafail Ostrovsky. Locally updatable and locally decodable codes. In *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings*, pages 489–514, 2014.

[106] Nishanth Chandran, Bhavana Kanukurthi, Rafail Ostrovsky, and Leonid Reyzin. Privacy amplification with asymptotically optimal entropy loss. In *STOC*, pages 785–794, 2010.

[107] Nishanth Chandran, Rafail Ostrovsky, and William E. Skeith III. Public-key encryption with efficient amortized updates. In *SCN*, pages 17–35, 2010.

[108] Chongwon Cho, Sanjam Garg, and Rafail Ostrovsky. Cross-domain secure computation. In *Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014. Proceedings*, pages 650–668, 2014.

[109] Chongwon Cho, Chen-Kuei Lee, and Rafail Ostrovsky. Equivalence of uniform key agreement and composition insecurity. In *CRYPTO*, pages 447–464, 2010.

[110] Chongwon Cho, Rafail Ostrovsky, Alessandra Scafuro, and Ivan Visconti. Simultaneously resettable arguments of knowledge. In *TCC*, pages 530–547, 2012.

[111] Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, Muthuramakrishnan Venkitasubramaniam, and Ivan Visconti. 4-round resettably-sound zero knowledge. In *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings*, pages 192–216, 2014.

[112] Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, and Ivan Visconti. Simultaneous resetability from one-way functions. In *54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, 26-29 October, 2013, Berkeley, CA, USA*, pages 60–69, 2013.

[113] Julia Chuzhoy, Rafail Ostrovsky, and Yuval Rabani. Approximation algorithms for the job interval selection problem and related scheduling problems. In *FOCS*, pages 348–356, 2001.

[114] Giovanni Di Crescenzo, Yuval Ishai, and Rafail Ostrovsky. Non-interactive and non-malleable commitment. In *STOC*, pages 141–150, 1998.

[115] Giovanni Di Crescenzo, Yuval Ishai, and Rafail Ostrovsky. Universal service-providers for database private information retrieval. In *PODC*, pages 91–100, 1998.

[116] Giovanni Di Crescenzo, Jonathan Katz, Rafail Ostrovsky, and Adam Smith. Efficient and non-interactive non-malleable commitment. In *EUROCRYPT*, pages 40–59, 2001.

[117] Giovanni Di Crescenzo, Tal Malkin, and Rafail Ostrovsky. Single database private information retrieval implies oblivious transfer. In *EUROCRYPT*, pages 122–138, 2000.

[118] Giovanni Di Crescenzo and Rafail Ostrovsky. On concurrent zero-knowledge with preprocessing. In *CRYPTO*, pages 485–502, 1999.

[119] Giovanni Di Crescenzo, Rafail Ostrovsky, and Sivaramakrishnan Rajagopalan. Conditional oblivious transfer and timed-release encryption. In *EUROCRYPT*, pages 74–89, 1999.

[120] Reza Curtmola, Juan A. Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: improved definitions and efficient constructions. In *ACM Conference on Computer and Communications Security*, pages 79–88, 2006.

[121] Alfredo DeSantis, Giovanni Di Crescenzo, Rafail Ostrovsky, Giuseppe Persiano, and Amit Sahai. Robust non-interactive zero knowledge. In *CRYPTO*, pages 566–598, 2001.

[122] Shlomi Dolev and Rafail Ostrovsky. Efficient anonymous multicast and reception. In *CRYPTO*, pages 395–409, 1997.

[123] Joan Feigenbaum and Rafail Ostrovsky. A note on one-prover, instance-hiding zero-knowledge proof systems. In *ASIACRYPT*, pages 352–359, 1991.

[124] Matthias Fitzi, Juan A. Garay, Ueli M. Maurer, and Rafail Ostrovsky. Minimal complete primitives for secure multi-party computation. In *CRYPTO*, pages 80–100, 2001.

[125] Matthew K. Franklin, Ran Gelles, Rafail Ostrovsky, and Leonard J. Schulman. Optimal coding for streaming authentication and interactive communication. In *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II*, pages 258–276, 2013.

[126] Juan A. Garay, Clint Givens, and Rafail Ostrovsky. Secure message transmission with small public discussion. In *EUROCRYPT*, pages 177–196, 2010.

[127] Juan A. Garay, Clint Givens, and Rafail Ostrovsky. Secure message transmission by public discussion: A brief survey. In *IWCC*, pages 126–141, 2011.

[128] Juan A. Garay, Clint Givens, Rafail Ostrovsky, and Pavel Raykov. Broadcast (and round) efficient verifiable secret sharing. In *Information Theoretic Security - 7th International Conference, ICITS 2013, Singapore, November 28-30, 2013, Proceedings*, pages 200–219, 2013.

[129] Juan A. Garay, Clinton Givens, Rafail Ostrovsky, and Pavel Raykov. Fast and unconditionally secure anonymous channel. In *ACM Symposium on Principles of Distributed Computing, PODC '14, Paris, France, July 15-18, 2014*, pages 313–321, 2014.

[130] Juan A. Garay, Jonathan Katz, Chiu-Yuen Koo, and Rafail Ostrovsky. Round complexity of authenticated broadcast with a dishonest majority. In *FOCS*, pages 658–668, 2007.

[131] Juan A. Garay and Rafail Ostrovsky. Almost-everywhere secure computation. In *EUROCRYPT*, pages 307–323, 2008.

[132] Sanjam Garg, Abishek Kumarasubramanian, Rafail Ostrovsky, and Ivan Visconti. Impossibility results for static input secure computation. In *CRYPTO*, pages 424–442, 2012.

[133] Sanjam Garg, Rafail Ostrovsky, Ivan Visconti, and Akshay Wadia. Resettable statistical zero knowledge. In *TCC*, pages 494–511, 2012.

[134] Ran Gelles, Rafail Ostrovsky, and Alan Roytman. Efficient error-correcting codes for sliding windows. In *SOFSEM 2014: Theory and Practice of Computer Science - 40th International Conference on Current Trends in Theory and Practice of Computer Science, Nový Smokovec, Slovakia, January 26-29, 2014, Proceedings*, pages 258–268, 2014.

[135] Ran Gelles, Rafail Ostrovsky, and Kina Winoto. Multiparty proximity testing with dishonest majority from equality testing. In *ICALP (2)*, pages 537–548, 2012.

[136] Craig Gentry, Shai Halevi, Steve Lu, Rafail Ostrovsky, Mariana Raykova, and Daniel Wichs. Garbled RAM revisited. In *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, pages 405–422, 2014.

[137] Oded Goldreich, Rafail Ostrovsky, and Erez Petrank. Computational complexity and knowledge complexity. In *STOC*, pages 534–543, 1994.

[138] Shafi Goldwasser and Rafail Ostrovsky. Invariant signatures and non-interactive zero-knowledge proofs are equivalent. In *CRYPTO*, pages 228–245, 1992.

[139] Yannai Gonczarowski, Noam Nisan, Rafail Ostrovsky, and Will Rosenbaum. A stable marriage requires communication. In *SODA*, 2015.

[140] S. Dov Gordon, Yuval Ishai, Tal Moran, Rafail Ostrovsky, and Amit Sahai. On complete primitives for fairness. In *TCC*, pages 91–108, 2010.

[141] Vipul Goyal, Abhishek Jain, and Rafail Ostrovsky. Password-authenticated session-key generation on the internet in the plain model. In *CRYPTO*, pages 277–294, 2010.

[142] Vipul Goyal, Abhishek Jain, Rafail Ostrovsky, Silas Richelson, and Ivan Visconti. Concurrent zero knowledge in the bounded player model. In *TCC*, pages 60–79, 2013.

[143] Vipul Goyal, Abhishek Jain, Rafail Ostrovsky, Silas Richelson, and Ivan Visconti. Constant-round concurrent zero knowledge in the bounded player model. In *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I*, pages 21–40, 2013.

[144] Vipul Goyal, Chen-Kuei Lee, Rafail Ostrovsky, and Ivan Visconti. Constructing non-malleable commitments: A black-box approach. In *FOCS*, pages 51–60, 2012.

[145] Vipul Goyal, Ryan Moriarty, Rafail Ostrovsky, and Amit Sahai. Concurrent statistical zero-knowledge arguments for np from any way function. In *ASIACRYPT*, pages 444–459, 2007.

[146] Vipul Goyal, Rafail Ostrovsky, Alessandra Scafuro, and Ivan Visconti. Black-box non-black-box zero knowledge. In *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 515–524, 2014.

[147] Jens Groth and Rafail Ostrovsky. Cryptography in the multi-string model. In *CRYPTO*, pages 323–341, 2007.

[148] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Non-interactive zaps and new techniques for nizk. In *CRYPTO*, pages 97–111, 2006.

[149] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Perfect non-interactive zero knowledge for np. In *EUROCRYPT*, pages 339–358, 2006.

[150] Brett Hemenway, Benoit Libert, Rafail Ostrovsky, and Damien Vergnaud. Lossy encryption: Constructions from general assumptions and efficient selective opening chosen ciphertext security. In *ASIACRYPT*, pages 70–88, 2011.

[151] Brett Hemenway, Steve Lu, and Rafail Ostrovsky. Correlated product security from any one-way function. In *Public Key Cryptography*, pages 558–575, 2012.

[152] Brett Hemenway and Rafail Ostrovsky. Public-key locally-decodable codes. In *CRYPTO*, pages 126–143, 2008.

[153] Brett Hemenway and Rafail Ostrovsky. Extended-ddh and lossy trapdoor functions. In *Public Key Cryptography*, pages 627–643, 2012.

[154] Brett Hemenway and Rafail Ostrovsky. On homomorphic encryption and chosen-ciphertext security. In *Public Key Cryptography*, pages 52–65, 2012.

[155] Brett Hemenway and Rafail Ostrovsky. Building lossy trapdoor functions from lossy encryption. In *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part II*, pages 241–260, 2013.

[156] Brett Hemenway, Rafail Ostrovsky, Martin J. Strauss, and Mary Wootters. Public key locally decodable codes with short keys. In *APPROX-RANDOM*, pages 605–615, 2011.

[157] Brett Hemenway, Rafail Ostrovsky, and Mary Wootters. Local correctability of expander codes. In *Automata, Languages, and Programming - 40th International Colloquium, ICALP 2013, Riga, Latvia, July 8-12, 2013, Proceedings, Part I*, pages 540–551, 2013.

[158] Yuval Ishai, Eyal Kushilevitz, Xin Li, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai, and David Zuckerman. Robust pseudorandom generators. In *Automata, Languages, and Programming - 40th International Colloquium, ICALP 2013, Riga, Latvia, July 8-12, 2013, Proceedings, Part I*, pages 576–588, 2013.

[159] Yuval Ishai, Eyal Kushilevitz, and Rafail Ostrovsky. Sufficient conditions for collision-resistant hashing. In *TCC*, pages 445–456, 2005.

[160] Yuval Ishai, Eyal Kushilevitz, and Rafail Ostrovsky. Efficient arguments without short pcps. In *IEEE Conference on Computational Complexity*, pages 278–291, 2007.

[161] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, and Amit Sahai. Efficient non-interactive secure computation. In *EUROCRYPT*, pages 406–425, 2011.

[162] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai, and Jurg Wullschleger. Constant-rate oblivious transfer from noisy channels. In *CRYPTO*, pages 667–684, 2011.

[163] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Batch codes and their applications. In *STOC*, pages 262–271, 2004.

[164] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography from anonymity. In *FOCS*, pages 239–248, 2006.

[165] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Zero-knowledge from secure multiparty computation. In *STOC*, pages 21–30, 2007.

[166] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography with constant computational overhead. In *STOC*, pages 433–442, 2008.

[167] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Extracting correlations. In *FOCS*, pages 261–270, 2009.

[168] Yuval Ishai, Rafail Ostrovsky, and Hakan Seyalioglu. Identifying cheaters without an honest majority. In *TCC*, pages 21–38, 2012.

[169] Yuval Ishai, Rafail Ostrovsky, and Vassilis Zikas. Secure multi-party computation with identifiable abort. In *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part II*, pages 369–386, 2014.

[170] Ari Juels, Michael Luby, and Rafail Ostrovsky. Security of blind digital signatures. In *CRYPTO*, pages 150–164, 1997.

[171] Jonathan Katz, Steven Myers, and Rafail Ostrovsky. Cryptographic counters and applications to electronic voting. In *EUROCRYPT*, pages 78–92, 2001.

[172] Jonathan Katz and Rafail Ostrovsky. Round-optimal secure two-party computation. In *CRYPTO*, pages 335–354, 2004.

[173] Jonathan Katz, Rafail Ostrovsky, and Michael O. Rabin. Identity-based zero knowledge. In *SCN*, pages 180–192, 2004.

[174] Jonathan Katz, Rafail Ostrovsky, and Adam Smith. Round efficiency of multi-party computation with a dishonest majority. In *EUROCRYPT*, pages 578–595, 2003.

[175] Jonathan Katz, Rafail Ostrovsky, and Moti Yung. Efficient password-authenticated key exchange using human-memorable passwords. In *EUROCRYPT*, pages 475–494, 2001.

[176] Jonathan Katz, Rafail Ostrovsky, and Moti Yung. Forward secrecy in password-only key exchange protocols. In *SCN*, pages 29–44, 2002.

[177] Joe Kilian, Silvio Micali, and Rafail Ostrovsky. Minimum resource zero-knowledge proofs. In *FOCS*, pages 474–479, 1989.

[178] Abishek Kumarasubramanian, Rafail Ostrovsky, Omkant Pandey, and Akshay Wadia. Cryptography using captcha puzzles. In *Public-Key Cryptography - PKC 2013 - 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, February 26 - March 1, 2013. Proceedings*, pages 89–106, 2013.

[179] Eyal Kushilevitz, Nathan Linial, and Rafail Ostrovsky. The linear-array conjecture in communication complexity is false. In *STOC*, pages 1–10, 1996.

[180] Eyal Kushilevitz, Steve Lu, and Rafail Ostrovsky. On the (in)security of hash-based oblivious ram and a new balancing scheme. In *SODA*, pages 143–156, 2012.

[181] Eyal Kushilevitz, Silvio Micali, and Rafail Ostrovsky. Reducibility and completeness in multi-party private computations. In *FOCS*, pages 478–489, 1994.

[182] Eyal Kushilevitz and Rafail Ostrovsky. Replication is not needed: Single database, computationally-private information retrieval. In *FOCS*, pages 364–373, 1997.

[183] Eyal Kushilevitz and Rafail Ostrovsky. One-way trapdoor permutations are sufficient for non-trivial single-server private information retrieval. In *EUROCRYPT*, pages 104–121, 2000.

[184] Eyal Kushilevitz, Rafail Ostrovsky, and Yuval Rabani. Efficient search for approximate nearest neighbor in high dimensional spaces. In *STOC*, pages 614–623, 1998.

[185] Eyal Kushilevitz, Rafail Ostrovsky, and Adi Rosén. Log-space polynomial end-to-end communication. In *PODC*, page 254, 1995.

[186] Eyal Kushilevitz, Rafail Ostrovsky, and Adi Rosén. Log-space polynomial end-to-end communication. In *STOC*, pages 559–568, 1995.

[187] Eyal Kushilevitz, Rafail Ostrovsky, and Adi Rosén. Characterizing linear size circuits in terms of privacy. In *STOC*, pages 541–550, 1996.

[188] Eyal Kushilevitz, Rafail Ostrovsky, and Adi Rosén. Amortizing randomness in private multiparty computations. In *PODC*, pages 81–90, 1998.

[189] Shay Kutten, Rafail Ostrovsky, and Boaz Patt-Shamir. The las-vegas processor identity problem (how and when to be unique). In *ISTCS*, pages 150–159, 1993.

[190] Joshua Lampkins and Rafail Ostrovsky. Communication-efficient MPC for general adversary structures. In *Security and Cryptography for Networks - 9th International Conference, SCN 2014, Amalfi, Italy, September 3-5, 2014. Proceedings*, pages 155–174, 2014.

[191] Richard J. Lipton and Rafail Ostrovsky. Micropayments via efficient coin-flipping. In *Financial Cryptography*, pages 1–15, 1998.

[192] Steve Lu, Daniel Manchala, and Rafail Ostrovsky. Visual cryptography on graphs. In *COCOON*, pages 225–234, 2008.

[193] Steve Lu and Rafail Ostrovsky. Distributed oblivious RAM for secure two-party computation. In *TCC*, pages 377–396, 2013.

[194] Steve Lu and Rafail Ostrovsky. How to garble RAM programs. In *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, pages 719–734, 2013.

[195] Steve Lu, Rafail Ostrovsky, Amit Sahai, Hovav Shacham, and Brent Waters. Sequential aggregate signatures and multisignatures without random oracles. In *EUROCRYPT*, pages 465–485, 2006.

[196] Alain J. Mayer, Rafail Ostrovsky, Yoram Ofek, and Moti Yung. Self-stabilizing symmetry breaking in constant-space. In *STOC*, pages 667–678, 1992.

[197] Alain J. Mayer, Rafail Ostrovsky, and Moti Yung. Self-stabilizing algorithms for synchronous unidirectional rings. In *SODA*, pages 564–573, 1996.

[198] Silvio Micali, Joe Kilian, and Rafail Ostrovsky. Minimum resource zero-knowledge proofs. In *CRYPTO*, pages 545–546, 1989.

[199] Moni Naor, Rafail Ostrovsky, Ramarathnam Venkatesan, and Moti Yung. Perfect zero-knowledge arguments for np can be based on general complexity assumptions. In *CRYPTO. Perfect Zero-Knowledge Arguments for NP Can Be Based on General Complexity Assumptions. pages 196-214, 1992.*, pages 196–214, 1992.

[200] Claudio Orlandi, Rafail Ostrovsky, Vanishree Rao, Amit Sahai, and Ivan Visconti. Statistical concurrent non-malleable zero knowledge. In *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings*, pages 167–191, 2014.

[201] Rafail Ostrovsky. Holmes-1, a prolog-based reason maintenance system for collecting information from multiple experts. In *IPMU*, pages 329–336, 1986.

[202] Rafail Ostrovsky. An efficient software protection scheme. In *CRYPTO*, pages 610–611, 1989.

[203] Rafail Ostrovsky. Efficient computation on oblivious rams. In *STOC*, pages 514–523, 1990.

[204] Rafail Ostrovsky. One-way functions, hard on average problems, and statistical zero-knowledge proofs. In *Structure in Complexity Theory Conference*, pages 133–138, 1991.

[205] Rafail Ostrovsky and William E. Skeith III. Private searching on streaming data. In *CRYPTO*, pages 223–240, 2005.

[206] Rafail Ostrovsky and William E. Skeith III. Private searching on streaming data. *IACR Cryptology ePrint Archive*, 2005:242, 2005.

[207] Rafail Ostrovsky and William E. Skeith III. A survey of single-database private information retrieval: Techniques and applications. In *Public Key Cryptography*, pages 393–411, 2007.

[208] Rafail Ostrovsky and William E. Skeith III. Communication complexity in algebraic two-party protocols. In *CRYPTO*, pages 379–396, 2008.

[209] Rafail Ostrovsky, Omkant Pandey, and Amit Sahai. Private locally decodable codes. In *ICALP*, pages 387–398, 2007.

[210] Rafail Ostrovsky, Omkant Pandey, and Ivan Visconti. Efficiency preserving transformations for concurrent non-malleable zero knowledge. In *TCC*, pages 535–552, 2010.

[211] Rafail Ostrovsky, Anat Paskin-Cherniavsky, and Beni Paskin-Cherniavsky. Maliciously circuit-private FHE. In *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*, pages 536–553, 2014.

[212] Rafail Ostrovsky and Boaz Patt-Shamir. Optimal and efficient clock synchronization under drifting clocks. In *PODC*, pages 3–12, 1999.

[213] Rafail Ostrovsky, Giuseppe Persiano, and Ivan Visconti. Constant-round concurrent non-malleable zero knowledge in the bare public-key model. In *ICALP (2)*, pages 548–559, 2008.

[214] Rafail Ostrovsky, Giuseppe Persiano, and Ivan Visconti. Simulation-based concurrent non-malleable commitments and decommitments. In *TCC*, pages 91–108, 2009.

[215] Rafail Ostrovsky, Giuseppe Persiano, and Ivan Visconti. On input indistinguishable proof systems. In *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part I*, pages 895–906, 2014.

[216] Rafail Ostrovsky and Yuval Rabani. Universal o(congestion + dilation + $\log^{(1+\epsilon)} n$) local control packet switching algorithms. In *STOC*, pages 644–653, 1997.

[217] Rafail Ostrovsky and Yuval Rabani. Polynomial time approximation schemes for geometric k-clustering. In *FOCS*, pages 349–358, 2000.

[218] Rafail Ostrovsky and Yuval Rabani. Low distortion embeddings for edit distance. In *STOC*, pages 218–224, 2005.

[219] Rafail Ostrovsky, Yuval Rabani, and Leonard J. Schulman. Error-correcting codes for automatic control. In *FOCS*, pages 309–316, 2005.

[220] Rafail Ostrovsky, Yuval Rabani, Leonard J. Schulman, and Chaitanya Swamy. The effectiveness of lloyd-type methods for the k-means problem. In *FOCS*, pages 165–176, 2006.

[221] Rafail Ostrovsky, Charles Rackoff, and Adam Smith. Efficient consistency proofs for generalized queries on a committed database. In *ICALP*, pages 1041–1053, 2004.

[222] Rafail Ostrovsky, Sridhar Rajagopalan, and Umesh V. Vazirani. Simple and efficient leader election in the full information model. In *STOC*, pages 234–242, 1994.

[223] Rafail Ostrovsky, Vanishree Rao, Alessandra Scafuro, and Ivan Visconti. Revisiting lower and upper bounds for selective decommitments. In *TCC*, pages 559–578, 2013.

[224] Rafail Ostrovsky, Vanishree Rao, and Ivan Visconti. On selective-opening attacks against encryption schemes. In *Security and Cryptography for Networks - 9th International Conference, SCN 2014, Amalfi, Italy, September 3-5, 2014. Proceedings*, pages 578–597, 2014.

[225] Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-based encryption with non-monotonic access structures. In *ACM Conference on Computer and Communications Security*, pages 195–203, 2007.

[226] Rafail Ostrovsky, Alessandra Scafuro, Ivan Visconti, and Akshay Wadia. Universally composable secure computation with (malicious) physically uncloneable functions. In *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, pages 702–718, 2013.

[227] Rafail Ostrovsky and Victor Shoup. Private information storage. In *STOC*, pages 294–303, 1997.

[228] Rafail Ostrovsky, Ramarathnam Venkatesan, and Moti Yung. Fair Games Against an All-Powerful Adversary (preliminary version). In Renato M. Capocelli, Alfredo De Santis, and Ugo Vaccaro, editors, *Sequences II: Communication, Security, and Computer Science*, pages 418–429. Springer-Verlag, 1991. From International Advanced Workshop. Sequences II, Positano, Italy, June 1991. Prior to Positano, this work was first presented at DIMACS Complexity and Cryptography Workshop, October 1990, Princeton, NJ.

[229] Rafail Ostrovsky, Ramarathnam Venkatesan, and Moti Yung. Secure commitment against a powerful adversary. In *STACS*, pages 439–448, 1992.

[230] Rafail Ostrovsky, Ramarathnam Venkatesan, and Moti Yung. Interactive hashing simplifies zero-knowledge protocol design. In *EUROCRYPT*, pages 267–273, 1993.

[231] Rafail Ostrovsky and Avi Wigderson. One-way functions are essential for non-trivial zero-knowledge. In *ISTCS*, pages 3–17, 1993.

[232] Rafail Ostrovsky and Daniel Wilkerson. Faster computation on directed networks of automata. In *PODC*, pages 38–46, 1995.

[233] Rafail Ostrovsky and Moti Yung. How to withstand mobile virus attacks. In *PODC*, pages 51–59, 1991.

Technical Reports

[234] Yair Amir, Paul Bunn, and Rafail Ostrovsky. Authenticated adversarial routing. *IACR Cryptology ePrint Archive*, 2008:448, 2008.

[235] Yair Amir, Paul Bunn, and Rafail Ostrovsky. Optimal-rate coding theorem for adversarial networks in the public-key setting. *CoRR*, abs/0808.0156, 2008.

[236] Leonid Barenboim, Shlomi Dolev, and Rafail Ostrovsky. Deterministic and energy-optimal wireless synchronization. *CoRR*, abs/1010.1112, 2010.

[237] Joshua Baron, Karim El Defrawy, Joshua Lampkins, and Rafail Ostrovsky. How to withstand mobile virus attacks, revisited. *IACR Cryptology ePrint Archive*, 2013:529, 2013.

[238] Eli Ben-Sasson, Serge Fehr, and Rafail Ostrovsky. Near-linear unconditionally-secure multiparty computation with a dishonest minority. *IACR Cryptology ePrint Archive*, 2011:629, 2011.

[239] Nir Bitansky, Alessandro Chiesa, Yuval Ishai, Rafail Ostrovsky, and Omer Paneth. Succinct non-interactive arguments via linear interactive proofs. *IACR Cryptology ePrint Archive*, 2012:718, 2012.

[240] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. *IACR Cryptology ePrint Archive*, 2003:195, 2003.

[241] Dan Boneh, Eyal Kushilevitz, Rafail Ostrovsky, and William E. Skeith III. Public key encryption that allows pir queries. *IACR Cryptology ePrint Archive*, 2007:73, 2007.

[242] Milan Bradonjic, Eddie Kohler, and Rafail Ostrovsky. Near-optimal radio use for wireless network synchronization. *CoRR*, abs/0810.1756, 2008.

[243] Vladimir Braverman, Ran Gelles, and Rafail Ostrovsky. How to catch l2-heavy-hitters on sliding windows. *CoRR*, abs/1012.3130, 2010.

[244] Vladimir Braverman and Rafail Ostrovsky. Measuring \$k\$-wise independence of streaming data. *CoRR*, abs/0806.4790, 2008.

[245] Vladimir Braverman and Rafail Ostrovsky. Measuring independence of datasets. *CoRR*, abs/0903.0034, 2009.

[246] Vladimir Braverman and Rafail Ostrovsky. Recursive sketching for frequency moments. *CoRR*, abs/1011.2571, 2010.

[247] Vladimir Braverman and Rafail Ostrovsky. Approximating large frequency moments with pick-and-drop sampling. *CoRR*, abs/1212.0202, 2012.

[248] Vladimir Braverman, Rafail Ostrovsky, and Yuval Rabani. Rademacher chaos, random eulerian graphs and the sparse johnson-lindenstrauss transform. *CoRR*, abs/1011.2590, 2010.

[249] Vladimir Braverman, Rafail Ostrovsky, and Alan Roytman. Universal streaming. *CoRR*, abs/1408.2604, 2014.

[250] Vladimir Braverman, Rafail Ostrovsky, and Dan Vilenchik. How hard is counting triangles in the streaming model. *CoRR*, abs/1304.1458, 2013.

[251] Vladimir Braverman, Rafail Ostrovsky, and Carlo Zaniolo. Succinct sampling on streams. *CoRR*, abs/cs/0702151, 2007.

[252] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. *CoRR*, abs/1009.2490, 2010.

[253] Paul Bunn and Rafail Ostrovsky. Throughput in asynchronous networks. *CoRR*, abs/0910.4572, 2009.

[254] Paul Bunn and Rafail Ostrovsky. Throughput-optimal routing in unreliable networks. *IACR Cryptology ePrint Archive*, 2010:231, 2010.

[255] Paul Bunn and Rafail Ostrovsky. Secure end-to-end communication with optimal throughput in unreliable networks. *CoRR*, abs/1304.2454, 2013.

[256] Nishanth Chandran, Wutichai Chongchitmate, Juan A. Garay, Shafi Goldwasser, Rafail Ostrovsky, and Vassilis Zikas. Optimally resilient and adaptively secure multi-party computation with low communication locality. *IACR Cryptology ePrint Archive*, 2014:615, 2014.

[257] Nishanth Chandran, Juan A. Garay, and Rafail Ostrovsky. Almost-everywhere secure computation with edge corruptions. *IACR Cryptology ePrint Archive*, 2012:221, 2012.

[258] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position based cryptography. *IACR Cryptology ePrint Archive*, 2009:364, 2009.

[259] Nishanth Chandran, Bhavana Kanukurthi, and Rafail Ostrovsky. Locally updatable and locally decodable codes. *IACR Cryptology ePrint Archive*, 2013:520, 2013.

[260] Nishanth Chandran, Bhavana Kanukurthi, Rafail Ostrovsky, and Leonid Reyzin. Privacy amplification with asymptotically optimal entropy loss. *IACR Cryptology ePrint Archive*, 2012:501, 2012.

[261] Nishanth Chandran, Ryan Moriarty, Rafail Ostrovsky, Omkant Pandey, and Amit Sahai. Improved algorithms for optimal embeddings. *Electronic Colloquium on Computational Complexity (ECCC)*, 13(110), 2006.

[262] Nishanth Chandran, Rafail Ostrovsky, and William E. Skeith III. Public-key encryption with efficient amortized updates. *IACR Cryptology ePrint Archive*, 2008:429, 2008.

[263] Chongwon Cho, Chen-Kuei Lee, and Rafail Ostrovsky. Equivalence of uniform key agreement and composition insecurity. *Electronic Colloquium on Computational Complexity (ECCC)*, 16:108, 2009.

[264] Reza Curtmola, Juan A. Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: Improved definitions and efficient constructions. *IACR Cryptology ePrint Archive*, 2006:210, 2006.

[265] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *IACR Cryptology ePrint Archive*, 2003:235, 2003.

[266] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *CoRR*, abs/cs/0602007, 2006.

[267] Shlomi Dolev, Andreas Pfitzmann, and Rafail Ostrovsky. 05411 abstracts collection – anonymous communication and its applications. In *Anonymous Communication and its Applications, Schloss Dagstuhl, Germany*, 2005.

[268] Mattew Franklin, Ran Gelles, Rafail Ostrovsky, and Leonard J. Schulman. Optimal coding for streaming authentication and interactive communication. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:104, 2012.

[269] Juan A. Garay, Clint Givens, and Rafail Ostrovsky. Broadcast-efficient secure multiparty computation. *IACR Cryptology ePrint Archive*, 2012:130, 2012.

[270] Juan A. Garay and Rafail Ostrovsky. Almost-everywhere secure computation. *IACR Cryptology ePrint Archive*, 2007:394, 2007.

[271] Sanjam Garg, Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography with one-way communication. *IACR Cryptology ePrint Archive*, 2014:914, 2014.

[272] Sanjam Garg, Abishek Kumarasubramanian, Rafail Ostrovsky, and Ivan Visconti. Impossibility results for static input secure computation. *IACR Cryptology ePrint Archive*, 2012:433, 2012.

[273] Sanjam Garg, Steve Lu, Rafail Ostrovsky, and Alessandra Scafuro. Garbled RAM from one-way functions. *IACR Cryptology ePrint Archive*, 2014:941, 2014.

[274] Sanjam Garg, Rafail Ostrovsky, Ivan Visconti, and Akshay Wadia. Resettable statistical zero knowledge. *IACR Cryptology ePrint Archive*, 2011:457, 2011.

[275] Ran Gelles, Rafail Ostrovsky, and Kina Winoto. Multiparty proximity testing with dishonest majority from equality testing. *IACR Cryptology ePrint Archive*, 2012:378, 2012.

[276] Oded Goldreich, Rafail Ostrovsky, and Erez Petrank. Computational complexity and knowledge complexity. *Electronic Colloquium on Computational Complexity (ECCC)*, 1(7), 1994.

[277] Vipul Goyal, Ryan Moriarty, Rafail Ostrovsky, and Amit Sahai. Concurrent statistical zero-knowledge arguments for np from one way functions. *IACR Cryptology ePrint Archive*, 2006:400, 2006.

[278] Vipul Goyal, Rafail Ostrovsky, Alessandra Scafuro, and Ivan Visconti. Black-box non-black-box zero knowledge. *IACR Cryptology ePrint Archive*, 2014:390, 2014.

[279] Jens Groth and Rafail Ostrovsky. Cryptography in the multi-string model. *IACR Cryptology ePrint Archive*, 2006:407, 2006.

[280] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Perfect non-interactive zero knowledge for np. *Electronic Colloquium on Computational Complexity (ECCC)*, (097), 2005.

[281] Brett Hemenway, Benoit Libert, Rafail Ostrovsky, and Damien Vergnaud. Lossy encryption: Constructions from general assumptions and efficient selective opening chosen ciphertext security. *IACR Cryptology ePrint Archive*, 2009:88, 2009.

[282] Brett Hemenway, Steve Lu, and Rafail Ostrovsky. Correlated product security from any one-way function and the new notion of decisional correlated product security. *IACR Cryptology ePrint Archive*, 2010:100, 2010.

[283] Brett Hemenway and Rafail Ostrovsky. Public key encryption which is simultaneously a locally-decodable error-correcting code. *IACR Cryptology ePrint Archive*, 2007:83, 2007.

[284] Brett Hemenway and Rafail Ostrovsky. Lossy trapdoor functions from smooth homomorphic hash proof systems. *Electronic Colloquium on Computational Complexity (ECCC)*, 16:127, 2009.

[285] Brett Hemenway and Rafail Ostrovsky. Homomorphic encryption over cyclic groups implies chosen-ciphertext security. *IACR Cryptology ePrint Archive*, 2010:99, 2010.

[286] Brett Hemenway, Rafail Ostrovsky, Martin Strauss, and Mary Wootters. Public key locally decodable codes with short keys. *ECCC*, 18:118, 2011.

[287] Brett Hemenway, Rafail Ostrovsky, and Mary Wootters. Local correctability of expander codes. *CoRR*, abs/1304.8129, 2013.

[288] Yuval Ishai, Eyal Kushilevitz, Xin Li, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai, and David Zuckerman. Robust pseudorandom generators. *IACR Cryptology ePrint Archive*, 2013:671, 2013.

[289] Yuval Ishai, Eyal Kushilevitz, Xin Li, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai, and David Zuckerman. Robust pseudorandom generators. *IACR Cryptology ePrint Archive*, 2013:671, 2013.

[290] Abhishek Jain, Rafail Ostrovsky, Silas Richelson, and Ivan Visconti. Concurrent zero knowledge in the bounded player model. *IACR Cryptology ePrint Archive*, 2012:279, 2012.

[291] Jonathan Katz, Rafail Ostrovsky, and Moti Yung. Efficient password-authenticated key exchange using human-memorable passwords. *IACR Cryptology ePrint Archive*, 2001:31, 2001.

[292] Abishek Kumarasubramanian, Rafail Ostrovsky, Omkant Pandey, and Akshay Wadia. Cryptography using CAPTCHA puzzles. *IACR Cryptology ePrint Archive*, 2012:689, 2012.

[293] Eyal Kushilevitz, Steve Lu, and Rafail Ostrovsky. On the (in)security of hash-based oblivious ram and a new balancing scheme. *IACR Cryptology ePrint Archive*, 2011:327, 2011.

[294] Joshua Lampkins and Rafail Ostrovsky. Communication-efficient MPC for general adversary structures. *IACR Cryptology ePrint Archive*, 2013:640, 2013.

[295] Steve Lu and Rafail Ostrovsky. Multi-server oblivious ram. *IACR Cryptology ePrint Archive*, 2011:384, 2011.

[296] Steve Lu and Rafail Ostrovsky. How to garble RAM programs. *IACR Cryptology ePrint Archive*, 2012:601, 2012.

[297] Steve Lu and Rafail Ostrovsky. Garbled RAM revisited, part II. *IACR Cryptology ePrint Archive*, 2014:83, 2014.

[298] Silvio Micali, Joe Kilian, and Rafail Ostrovsky. Minimum resource zero-knowledge proofs. In *CRYPTO*, pages 545–546, 1989.

[299] Claudio Orlandi, Rafail Ostrovsky, Vanishree Rao, Amit Sahai, and Ivan Visconti. Statistical concurrent non-malleable zero knowledge. *IACR Cryptology ePrint Archive*, 2014:143, 2014.

[300] Rafail Ostrovsky and William E. Skeith III. Algebraic lower bounds for computing on encrypted data. *IACR Cryptology ePrint Archive*, 2007:64, 2007.

[301] Rafail Ostrovsky and William E. Skeith III. Algebraic lower bounds for computing on encrypted data. *Electronic Colloquium on Computational Complexity (ECCC)*, 14(022), 2007.

[302] Rafail Ostrovsky and William E. Skeith III. A survey of single database pir: Techniques and applications. *IACR Cryptology ePrint Archive*, 2007:59, 2007.

[303] Rafail Ostrovsky, Omkant Pandey, and Amit Sahai. Private locally decodable codes. *IACR Cryptology ePrint Archive*, 2007:25, 2007.

[304] Rafail Ostrovsky and Anat Paskin-Cherniavsky. Locally decodable codes for edit distance. *IACR Cryptology ePrint Archive*, 2014:260, 2014.

[305] Rafail Ostrovsky, Anat Paskin-Cherniavsky, and Beni Paskin-Cherniavsky. Maliciously circuit-private FHE. *IACR Cryptology ePrint Archive*, 2013:307, 2013.

[306] Rafail Ostrovsky, Giuseppe Persiano, and Ivan Visconti. Concurrent non-malleable witness indistinguishability and its applications. *Electronic Colloquium on Computational Complexity (ECCC)*, 13(095), 2006.

[307] Rafail Ostrovsky, Giuseppe Persiano, and Ivan Visconti. Impossibility results for leakage-resilient zero knowledge and multi-party computation. *IACR Cryptology ePrint Archive*, 2014:865, 2014.

[308] Rafail Ostrovsky, Charles Rackoff, and Adam Smith. Efficient consistency proofs for generalized queries on a committed database. *IACR Cryptology ePrint Archive*, 2004:170, 2004.

[309] Rafail Ostrovsky, Vanishree Rao, Alessandra Scafuro, and Ivan Visconti. Revisiting lower and upper bounds for selective decommitments. *IACR Cryptology ePrint Archive*, 2011:536, 2011.

[310] Rafail Ostrovsky and Will Rosenbaum. Fast distributed almost stable marriages. *CoRR*, abs/1408.2782, 2014.

[311] Rafail Ostrovsky and Will Rosenbaum. It's not easy being three: The approximability of three-dimensional stable matching problems. *CoRR*, abs/1412.1130, 2014.

[312] Rafail Ostrovsky and Will Rosenbaum. On the communication complexity of finding an (approximate) stable marriage. *CoRR*, abs/1406.1273, 2014.

[313] Rafail Ostrovsky, Alessandra Scafuro, and Muthuramakrishnan Venkitasubramaniam. Resettably sound zero-knoweldge arguments from owfs - the (semi) black-box way. *IACR Cryptology ePrint Archive*, 2014:284, 2014.

[314] Rafail Ostrovsky, Alessandra Scafuro, Ivan Visconti, and Akshay Wadia. Universally composable secure computation with (malicious) physically uncloneable functions. *IACR Cryptology ePrint Archive*, 2012:143, 2012.

[315] Rafail Ostrovsky and Ivan Visconti. Simultaneous resettability from collision resistance. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:164, 2012.

[316] Rafail Ostrovsky and Arman Yousefi. Improved approximation algorithms for earth-mover distance in data streams. *CoRR*, abs/1404.6287, 2014.