Arkady Yerukhimovich

January 1, 2018

Contact Information

MIT Lincoln Laboratory
Secure Resilient Systems and Technology Group

arkady5@gmail.com
http://web.mit.edu/arkady5/www/

Education

University of Maryland, College Park, MD USA

Ph.D. Computer Science, August 2011
- Advisor: Prof. Jonathan Katz
- Dissertation Title: *A Study of Separations in Cryptography: New Results and New Models*

M.S. Computer Science, May 2007
- Advisor: Prof. William Gasarch
- Master's Scholarly Paper: *A General Framework for One Database Private Information Retrieval*

Brown University, Providence, RI USA

B.S., Computer Science, May 2003
B.A., Math-Physics, May 2003

Research Experience

MIT Lincoln Laboratory, Lexington, MA USA
Research Scientist in Secure Resilient Systems and Technology Group **2011-present**

Responsibilities include leading medium size research teams, writing proposals for funding, and collaborating on projects inside and outside the laboratory. Recent research topics include secure database search, secure multi-party computation, and analysis of privacy on mobile devices.

University of Maryland, College Park, MD USA
Research Assistant under Prof. Jonathan Katz **2007-2011**

Research primarily focused on the limitations of "black-box" and "nonblack-box" constructions in cryptography. Other topics included secure multi-party computation, byzantine agreement, differential privacy, and zero knowledge proof systems.

The Johns Hopkins University Applied Physics Laboratory Laurel, MD USA
Visiting Scientist under Dr. Jonathan Trostle **Summer 2009**

Research topics included differential privacy for statistical databases and achieving optimal utility for privately answering multiple queries.

Institute for Theoretical Computer Science, Tsinghua University Beijing, China
Visiting Scientist under Dr. Andrej Bogdanov **Summer 2008**

Research topics included pseudorandomness and unconditional cryptographic constructions secure against bounded adversaries.

Brown University, Providence, RI USA
Research Assistant under Prof. John Savage **2002-2003**

Researched techniques for efficient data storage in nanowire arrays. Formally defined and studied complexity of both exact and approximate solutions to related problems.

Publications

Book Chapters

Cryptography for Big Data Security.
A. Hamlin, N. Schear, E. Shen, M. Varia, S. Yakoubov, and A. Yerukhimovich
In *Big Data: Storage, Sharing, and Security*, F. Hu, ed., Taylor & Francis LLC, CRC Press, 2016.
http://eprint.iacr.org/2016/012.pdf

Journals

(Efficient) Universally Composable Oblivious Transfer with a Minimal Number of Stateless Tokens.
S.G. Choi, J. Katz, D. Schröder, A. Yerukhimovich, and H.-S. Zhou.
Accepted to Journal of Cryptology (pending minor revisions).
One of three papers from TCC 2014 invited to this journal.

Authenticated Broadcast with a Partially Compromised Public-Key Infrastructure.
S.D. Gordon, J. Katz, R. Kumaresan, and A. Yerukhimovich
Information & Computation 234: 1725, 2014.
Invited to a special issue of this journal for papers from SSS 2010.

Efficient Data Storage in Large Nanoarrays.
L.-A. Gottlieb, J.E. Savage, and A. Yerukhimovich
Theory of Computing Systems, Vol. 38, pp. 503-536, 2005.

Conferences

SoK: Cryptographically Protected Database Search.
B. Fuller, M. Varia, A. Yerukhimovich, E. Shen, A. Hamlin, V. Gadepally, R. Shay, J.D. Mitchell, and R.K. Cunningham
IEEE Symposium on Security and Privacy, 2017.

Bounded-Collusion Attribute-Based Encryption from Minimal Assumptions
G. Itkis, E. Shen, M. Varia, D. Wilson, and A. Yerukhimovich
International Conference on Practice and Theory of Public-Key Cryptography (PKC), 2017.

SoK: Privacy on Mobile Devices - It's Complicated.
C. Spensky, J. Stewart, A. Yerukhimovich, R. Shay, A. Trachtenberg, R. Housley, and R.K. Cunningham
Privacy Enhancing Technologies Symposium (PETS), 2016.

POPE: Partial Order Preserving Encoding.
D.S. Roche, D. Apon, S.G. Choi, and A. Yerukhimovich
ACM Conference on Computer and Communications Security (CCS), 2016.

Computing on Masked Data to Improve the Security of Big Data.
V. Gadepally, B. Hancock, B. Kaiser, J. Kepner, P. Michaleas, M. Varia, A. Yerukhimovich
IEEE International Symposium on Technologies for Homeland Security (HST), 2015.
`https://arxiv.org/pdf/1504.01287.pdf`

Computing on Masked Data: A High Performance Method for Improving Big Data Veracity.
J. Kepner, V. Gadepally, P. Michaleas, N. Schear, M. Varia, A. Yerukhimovich, and R.K. Cunningham
IEEE High Performance Extreme Computing Conference (HPEC), 2014.

A Survey of Cryptographic Approaches to Securing Big-Data Analytics in the Cloud.
S. Yakoubov, V. Gadepally, N. Schear, E. Shen, and A. Yerukhimovich
IEEE High Performance Extreme Computing Conference (HPEC), 2014.

(Efficient) Universally Composable Oblivious Transfer with a Minimal Number of Stateless Tokens.
S.G. Choi, J. Katz, D. Schröder, A. Yerukhimovich, and H.-S. Zhou.
Theory of Cryptography Conference (TCC), 2014.
One of three papers invited to the Journal of Cryptology.

Limits On The Power of Zero-Knowledge Proofs in Cryptographic Constructions.
Z. Brakerski, J. Katz, G. Segev, and A. Yerukhimovich
Theory of Cryptography Conference (TCC), 2011.

On the Impossibility of Blind Signatures From One-Way Permutations.
J. Katz, D. Schröder, and A. Yerukhimovich

Theory of Cryptography Conference (TCC), 2011.

Limits of Computational Differential Privacy in the Client/Server Setting.
A. Groce, J. Katz, and A. Yerukhimovich
Theory of Cryptography Conference (TCC), 2011.

Authenticated Broadcast with a Partially Compromised Public-Key Infrastructure.
S.D. Gordon, J. Katz, R. Kumaresan, and A. Yerukhimovich
International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS), 2010.
Invited to a special issue of Information & Computation.

On the Round Complexity of Zero-Knowledge Proofs Based on One-Way Permutations.
S.D. Gordon, H. Wee, D. Xiao, and A. Yerukhimovich
Latincrypt, 2010.

On Black-Box Constructions of Predicate Encryption from Trapdoor Permutations.
J. Katz and A. Yerukhimovich
Asiacrypt, 2009.

Frequency Independent Flexible Spherical Beamforming via RBF Fitting.
A. Yerukhimovich, R. Duraiswami, N. Gumerov, and D.N. Zotkin
IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 2006.

Technical Reports

CompGC: Efficient Offline/Online Semi-Honest Two-Party Computation.
A. Groce, A. Ledger, A. Malozemoff, A. Yerukhimovich
`https://eprint.iacr.org/2016/458.pdf`

Can Smartphones and Privacy Coexist?
A. Yerukhimovich, R. Balebako, A. Boustead, R.K. Cunningham, W. Welser IV, R. Housley, R. Shay, C. Spensky, K.D. Stanley, J. Stewart, A. Trachtenberg, and Z. Winkelman
RAND Corporation Technical Report, 2016.

A General Framework for One Database Private Information Retrieval.
A. Yerukhimovich
University of Maryland Master's Scholarly Paper, 2007.
`http://web.mit.edu/arkady5/www/papers/pircomp.pdf`

Advising

Massachusetts Institute of Technology, Cambridge, MA USA

Gaurav Singh (Masters of Engineering, co-advised with Prof. Shafi Goldwasser) **2015-2016**
Thesis Title: *FIFE: A Framework for Investigating Functional Encryption*

Teaching Experience

University of Maryland, College Park, MD USA
Computer Science Instructor **Summer 2007**

Designed and taught an advanced undergraduate level algorithms course entitled "Design and Analysis of Computer Algorithms". Responsibilities included designing the syllabus, preparing lecture material and assignments, giving daily lectures, and grading submitted work and exams.

Graduate Teaching Assistant **2004-2006**

Assisted professor for courses entitled "Object Oriented Programming I and II", and "Design and Analysis of Computer Algorithms". Responsibilities included leading semiweekly recitation sections, holding office hours, and grading submitted work.

Brown University, Providence, RI USA
Undergraduate Teaching Assistant **2001-2002**

Assisted professor for course entitled "Models of Computation". Responsibilities included holding

office hours and grading submitted work.

Awards and Honors

- *National Science Foundation: East Asia And Pacific Summer Institutes for U.S. Graduate Students in Science and Engineering (EAPSI) Award*, 2008
- *Magna Cum Laude*, Brown University, 2003
- *Sigma Xi Honor Society* Associate Member, 2003

Service Activities:

- Program Chair: International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS) 2010 – Computer Security and Information Privacy track (co-chair with Prof. Ari Trachtenberg).
- Program Committee: International Conference on Applied Cryptography and Network Security (ACNS) 2015.
- Referee for the following publications: International Conference on Practice and Theory of Public-Key Cryptography (PKC) 2018, 2014, 2013, 2012; USENIX Security Symposium 2017; Theory of Cryptography Conference (TCC) 2017, 2016, 2015, 2012, 2011; ACM Transactions on Database Systems (TODS) 2016; European Symposium on Research in Computer Security (ESORICS) 2016; International Cryptology Conference (Crypto) 2016; Network & Distributed System Security Symposium (NDSS) 2015; International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt) 2014, 2009; IEEE Transactions on Knowledge and Data Engineering (TKDE) 2013; IEEE Symposium on Security and Privacy (IEEE S&P) 2013, 2012; Conference on Cryptographic Hardware and Embedded Systems (CHES) 2013; IEEE Transactions on Computers 2012; Journal of Cryptology 2012; IEEE International Symposium on Network Computing and Applications (NCA) 2012; MILCOM 2012; Symposium on Foundations of Computer Science (FOCS) 2011; ACM Symposium on the Theory of Computing (STOC) 2009; ACM Conference on Computer and Communications Security (CCS) 2009, 2007.