Arkady Yerukhimovich

August 16, 2023

Contact Information

George Washington University
Department of Computer Science

arkady@gwu.edu
https://www2.seas.gwu.edu/~arkady/

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

Employment History

The George Washington University, Washington, DC USA
Assistant Professor **2018-Present**

MIT Lincoln Laboratory, Lexington, MA USA
Research Scientist in Secure Resilient Systems and Technology Group **2011-2018**

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

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

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

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

Conferences:

Noiseless Differentially-Private Jaccard Index Estimation via Min-hash Sketching
M. Liang, L. Liu, S.G. Choi, D. Dachman-Soled, and A. Yerukhimovich
In Submission, 2023.

Secure Sampling with Sublinear Communication
S.G. Choi, D. Dachman-Soled, S.D. Gordon, L. Liu, and A. Yerukhimovich
Theory of Cryptography Conference (TCC), 2022.

When Frodo Flips: End-to-End Key Recovery on FrodoKEM via Rowhammer
M. Fahr, H. Kippen, A. Kwong, T. Dang, J. Lichtinger, D. Dachman-Soled, D. Genkin, A. Nelson, R. Perlner, A. Yerukhimovich, and D. Apon
ACM Conference on Computer and Communications Security (CCS), 2022.
Recipient of Best Paper Honorable Mention Award.

Fighting Fake News in Encrypted Messaging with the Fuzzy Anonymous Complaint Tally System

(FACTS)
L. Liu, D.S. Roche, A. Theriault, and A. Yerukhimovich
The Network and Distributed System Security (NDSS) Symposium, 2022.

Compressed Oblivious Encoding for Homomorphically Encrypted Search
S.G. Choi, D. Dachman-Soled, S.D. Gordon, L. Liu, and A. Yerukhimovich
ACM Conference on Computer and Communications Security (CCS), 2021.

The More The Merrier: Reducing the Cost of Large Scale MPC
S.D. Gordon, D. Starin, and A. Yerukhimovich
International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt), 2021.

Differentially-Private Multi-Party Sketching for Large-Scale Statistics
S.G. Choi, D. Dachman-Soled, M. Kulkarni, and A. Yerukhimovich
Privacy Enhancing Technologies Symposium (PETS), 2020.

Stormy: Statistics in Tor by Measuring Securely
R. Wails, A. Johnson, D. Starin, A. Yerukhimovich, and S.D. Gordon
ACM Conference on Computer and Communications Security (CCS), 2019.

Location Leakage from Network Access Patterns
T. Tiwari, A. Klausner, M. Andreev, A. Trachtenberg, and A. Yerukhimovich
IEEE Conference on Communications and Network Security (CNS), 2019.

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.

Secure Multiparty Computation for Cooperative Cyber Risk Assessment
K. Hogan, N. Luther, N. Schear, E. Shen, D. Stott, S. Yakoubov, and A. Yerukhimovich
IEEE Cybersecurity Development (SecDev), 2016

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.

Journals:
Blockchain Technology: What is it good for?
S. Ruoti, B. Kaiser, A. Yerukhimovich, J. Clark, and R.K. Cunningham
Communications of the ACM Vol. 63 (1), 2020 (via ACM Queue).

(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.
Journal of Cryptology Vol. 32 (2), 2019.
One of three papers from TCC 2014 invited to this journal.

Secure and Resilient Cloud Computing for the Department of Defense.
N. Schear, P. Cable, R.K. Cunningham, V. Gadepally, T. Moyer, and A. Yerukhimovich
Lincoln Laboratory Journal Vol. 22 (1), 2016.

Authenticated Broadcast with a Partially Compromised Public-Key Infrastructure.
S.D. Gordon, J. Katz, R. Kumaresan, and A. Yerukhimovich
Information & Computation, Vol. 234, pp. 17-25, 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.

Technical Reports:

Secure Sampling with Sublinear Communication.
S.G. Choi, D. Dachman-Soled, S.D. Gordon, L. Liu, and A. Yerukhimovich
`https://eprint.iacr.org/2022/660.pdf`, 2022.

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

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.

Theses:

A Study of Separations in Cryptography: New Results and New Models
PhD Thesis, Computer Science, University of Maryland, August 2011.

A General Framework for One Database Private Information Retrieval.
A. Yerukhimovich
University of Maryland Master's Scholarly Paper, 2007.

Grant Activity

(Dollar amounts listed reflect George Washington University's portion of the award.)

"CAREER: Sketching for Secure Computation on Large Inputs", NSF, $596,765.
July 2022 – June 2027
PI: Arkady Yerukhimovich

"SaTC: CORE: Medium: Collaborative: New Approaches for Large Scale Secure Computation", NSF, $404,534.
May 2020 – April 2024
PI: Arkady Yerukhimovich

"Privacy-Preserving Multi-Party Sketching for Advertisement Measurement", Facebook, $59,913.
May 2020 – April 2021
PI: Arkady Yerukhimovich

"Secure Computation Education: Training Secure Computation Developers for the DoD Workforce", DoD Cyber Scholarship Program – Capacity Building, DoD, $148,336.
August 2019 – July 2020
PI: Arkady Yerukhimovich; co-PIs: Rachelle S. Heller, and Constantine Toregas.

Students

- Suvasree Biswas, PhD student (since 2022)
- Linsheng Liu, PhD student (since 2020)
- Thinh Dang, PhD student (since 2019)
- Gaurav Singh, M.Eng. student at MIT (2015-2016), co-advised with Prof. Shafi Goldwasser

Thesis committees

- David Balash, May 2023
- Qin Hu, CS PhD, March 2019
- Yinhao Xiao, CS PhD, March 2019

Courses taught

- CS 3313: Foundations of Computing, Spring 2023
- CS 4331/6331: Cryptography, Fall 2022
- CS 3907/6907: Advanced Cryptography, Spring 2021

- CS 4331/6331: Cryptography, Fall 2021
- CS 3907/6907: Advanced Cryptography, Spring 2021
- CS 4331/6331: Cryptography, Fall 2020
- CS 3907/6907: Advanced Cryptography, Spring 2020
- CS 4331/6331: Cryptography, Fall 2019
- CS 3907/6907: Advanced Cryptography, Spring 2019
- CS 4331/6331: Cryptography, Fall 2018

Awards and Honors

NSF: Faculty Early Career Development Program (CAREER) Award, 2022

NSF: East Asia And Pacific Summer Institutes for U.S. Graduate Students in Science and Engineering (EAPSI) Award, 2008

Invited Talks

Crypto techniques allow distrusting parties to perform joint computations! Ready to teach them?
Community College Cyber Summit (3CS) 2022

Stormy: Statistics in Tor by Measuring Securely
DC-Area Crypto Day, October 2019

Cryptographically Protected Database Search Beyond SQL
IEEE Symposium on Privacy-Aware Computing, September 2018

Cryptographically Protected Database Search
DC-Area Anonymity, Privacy, and Security Seminar, February 2018

Service Activities

Organizing Committees:
- IEEE Symposium on Security and Privacy 2022–2023 - Publicity Chair.
- IEEE Symposium on Security and Privacy 2019–2021 - Short Talks Chair.
- The Network and Distributed System Security Symposium (NDSS) 2020 - Student Travel Grants Committee.

Program Chair:
- International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS) 2017 – Computer Security and Information Privacy track (co-chair with Prof. Ari Trachtenberg).

Program Committees:
- Crypto 2023, 2024
- ACM Conference on Computer and Communications Security (CCS) 2019, 2021, 2023
- Information Security Conference (ISC) 2019, 2023
- Eurocrypt 2022
- Privacy Enhancing Technologies Symposium (PETS) 2020, 2021, 2022
- IEEE Conference on Communications and Network Security (CNS) 2019
- Workshop on Privacy in the Electronic Society (WPES) 2018
- Workshop on Blockchain and Sharing Economy Applications (BlockSEA) 2018
- International Conference on Applied Cryptography and Network Security (ACNS) 2015

Referee for the following publications:
- Privacy Enhancing Technologies Symposium (PETS) 2023
- ACM Symposium on the Theory of Computing (STOC) 2009, 2023
- IEEE Symposium on Security and Privacy 2012, 2013, 2019, 2020
- Eurocrypt 2009, 2014, 2019, 2020
- Network & Distributed System Security Symposium (NDSS) 2015, 2020
- Practice and Theory of Public-Key Cryptography (PKC) 2012, 2013, 2014, 2018
- USENIX Security Symposium 2017, 2018

- International Cryptology Conference (Crypto) 2016, 2018
- Theory of Cryptography Conference (TCC) 2011, 2012, 2015, 2016, 2017
- ACM Transactions on Database Systems (TODS) 2016
- European Symposium on Research in Computer Security (ESORICS) 2016
- IEEE Transactions on Knowledge and Data Engineering (TKDE) 2013
- 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 Conference on Computer and Communications Security (CCS) 2007, 2009