

# Arkady B. Yerukhimovich

April 5, 2011

---

Contact Information	3204 A.V. Williams Bldg. University of Maryland College Park, MD 20742 USA	401-225-1339 arkady@cs.umd.edu <a href="http://www.cs.umd.edu/~arkady">http://www.cs.umd.edu/~arkady</a>
---------------------	--	--

---

Citizenship	USA
-------------	-----

---

Education	<b>University of Maryland</b> , College Park, MD USA Ph.D. Computer Science, expected graduation date: August 2011 <ul style="list-style-type: none"><li>• Advisor: Prof. Jonathan Katz</li><li>• Area of Study: Cryptography</li></ul> M.S. Computer Science, May 2008 <ul style="list-style-type: none"><li>• Advisor: Prof. William Gasarch</li><li>• GPA: 3.6</li></ul> <b>Brown University</b> , Providence, RI USA B.S., Computer Science, May 2003 B.A., Math-Physics, May 2003 <ul style="list-style-type: none"><li>• GPA: 3.9</li></ul>
-----------	---

---

Languages	Fluent and literate in Russian
-----------	--------------------------------

---

Research and Professional Experience	<b>University of Maryland</b> , College Park, MD USA <i>Research Assistant under Prof. Jonathan Katz</i> <b>2007-present</b>  My research is primarily focused on the limitations of “black-box” and “nonblack-box” constructions in cryptography. I have studied such limitations in areas such as zero-knowledge proofs, predicate encryption and blind signatures.  I am also very interested in the area of efficient secure multi-party computation (MPC). I am currently working on the design, implementation and evaluation of a general framework for measuring the performance of secure MPC protocols over real world networks. My other interests include differential privacy for statistical databases, secure encryption and byzantine agreement.  <b>The Johns Hopkins University Applied Physics Laboratory</b> Laurel, MD USA <i>Visiting Researcher under Dr. Jonathan Trostle</i> <b>Summer 2009</b>  Research topics included differential privacy for statistical databases and achieving optimal utility for privately answering multiple queries.  <b>Institute for Theoretical Computer Science, Tsinghua University</b> Beijing, China <i>Visiting Researcher under Dr. Andrej Bogdanov</i> <b>Summer 2008</b>  Research topics included pseudorandomness and unconditional cryptographic constructions secure against bounded adversaries.  <b>Uniteller, Inc.</b> , Rochelle Park, NJ USA <i>Research and Development</i> <b>2002-2004</b>  Designed, developed, and tested web-based financial application using J2EE technology as part of a small research and development team. My responsibilities included all aspects of the project life-cycle including design, coding, testing, documentation, and maintenance.  <b>Brown University</b> , Providence, RI USA <i>Research Assistant under Prof. John Savage</i> <b>2002-2003</b>  Researched techniques for efficient data storage in nanowire arrays. Formally defined and studied complexity of both exact and approximate solutions to related problems.
--------------------------------------	--

---

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

Publications

**Conferences:**

*Limits On The Power of Zero-Knowledge Proofs in Cryptographic Constructions*

Zvika Brakerski, Jonathan Katz, Gil Segev and **Arkady Yerukhimovich**

In 8th Theory of Cryptography Conference (TCC), 2011

*On the Impossibility of Blind Signatures From One-Way Permutations*

Jonathan Katz, Dominique Schröder and **Arkady Yerukhimovich**

In 8th Theory of Cryptography Conference (TCC), 2011

*Limits of Computational Differential Privacy in the Client/Server Setting*

Adam Groce, Jonathan Katz and **Arkady Yerukhimovich**

In 8th Theory of Cryptography Conference (TCC), 2011

*Authenticated Broadcast with a Partially Compromised Public-Key Infrastructure*

S. Dov Gordon, Jonathan Katz, Ranjit Kumaresan and **Arkady Yerukhimovich**

In Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS), 2010

*On the Round Complexity of Zero-Knowledge Proofs Based on One-Way Permutations*

S. Dov Gordon, Hoeteck Wee, David Xiao and **Arkady Yerukhimovich**

In Latincrypt 2010

*On Black-Box Constructions of Predicate Encryption from Trapdoor Permutations*

Jonathan Katz and **Arkady Yerukhimovich**

In Asiacrypt 2009

*Frequency Independent Flexible Spherical Beamforming via RBF Fitting*

**Arkady Yerukhimovich**, Ramani Duraiswami, Nail Gumerov and Dmitry N. Zotkin

In IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 2006

**Journals:**

*Efficient Data Storage in Large Nanoarrays*

Lee-Ad Gottlieb, John E. Savage and **Arkady Yerukhimovich**

In Theory of Computing Systems, Vol. 38, pp. 503-536, 2005

**Technical Reports:**

*A General Framework for One Database Private Information Retrieval*

Arkady Yerukhimovich

Master's Scholarly Paper, 2007

---

Teaching Experience **University of Maryland**, College Park, Maryland 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.

---

Software Experience Java, C, C++, Ruby on Rails, Linux, Unix, Windows