Valeria Nikolaenko

Website: www.valeniko.com
Email: valeria.nikolaenko@gmail.com
Work authorization status: US Citizen

I am interested in all aspects of modern cryptography, computer and web security, privacy of data collection.

EDUCATION

Sep 2011 – Jun 2017 **Stanford University**, USA
Department of Computer Science
Doctor of Philosophy in Computer Science, GPA: 4.0/4.0

Sep 2009 – Jun 2011 **University of the Russian Academy of Sciences**, Russia
Department of Mathematical and Informational Technologies
Master of Science with Honors, GPA 4.0/4.0

Sep 2005 – May 2009 **St. Petersburg State Polytechnical University**, Russia
Department of Applied Mathematics and Informatics
Bachelor of Science with Honors, GPS 3.9/4.0

EXPERIENCE

Aug 2017 – July 2018 **Co-organized a family cycling expedition through South America**
Travel blog: holoholotales.com/en

Sep 2011 – Jun 2017 **Research Assistant, Stanford University, USA**
- Discovered a new cryptographic primitive "Fully Key-Homomorphic Encryption" based on random lattices, it allows to do smart key management
- Developed solutions for aggregating low frequency signals in a privacy preserving way
- Developed a protocol for accountable warrants execution, involving data carriers, investigator, court and independent auditor

Jun 2015 – Sep 2015 **Software Engineer Intern, Google, Mountain View, USA**
- Developed new exchange algorithm for TLS based on hard problems in random lattices
- Evaluated the algorithm proving its high performance
- The algorithm was submitted to NIST as a proposal for new generation of quantum secure ciphers: frodokem.org

Jun 2012 – May 2013 **Intern, Technicolor Research, Palo Alto, USA**
- Built a system for privacy preserving data-mining on massive data sets containing hundreds of millions of users' records (ridge regression and matrix factorization)
- Implemented in Java and evaluated on real datasets
- 7 US patents pending

Sep 2008 – Jun 2011 **Software Engineer, JetBrains/SwiftTeams, St. Petersburg, Russia.**
- Contributed features to smart development environments: IntelliJ IDEA/PhpStorm/WebStorm
- Started syntactic support for new languages: ColdFusion and Smarty
- Developed support for test frameworks of PHP and ColdFusion

Dec 2009 – Jun 2011 **Research Assistant, Laboratory of Mathematical Logic at PDMI RAS, Russia**
In the area of computational complexity studied optimal heuristic decision algorithms, constructed an optimal algorithm for an injective function.

Nov 2006 – Feb 2008 **Software Engineer, Transas, St. Petersburg, Russia**
Developed real-time computer graphics algorithms for marine and aviation training systems. Programmed pixel and vertex shaders. Designed and implemented algorithms for sea surface rendering via projective grid, underwater effects (caustics, intersection with sea surface), stereo rendering, volumetric clouds and light beams (particle systems). Worked with C++, OpenGL, Cg.

Sep 2008 – Dec 2009 **Research Assistant, Laboratory of Representation Theory at PDMI RAS, Russia**
Studied permutation binomials over finite fields in search for their application to cryptography.

SKILLS

- Secure solutions for communication/authentication/computation/storage
- Secure multi-party computations (secret sharing, garbled circuits)
- Privacy preserving data mining
- Post-quantum cryptography: secure key exchange, encryption, signatures
- Advanced cryptography: computations on encrypted data, attribute-based encryption
- Lattice based cryptography
- Languages: Java, C, C++, HTML, CSS

PAPERS & MANUSCRIPTS

- **Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE (Cited by 116)**
  J.Bos, C.Costello, L.Ducas, I.Mironov, M.Naehrig, V.Nikolaenko, A.Raghunathan, D.Stebila
  CCS 2016: 23rd ACM Conference on Computer and Communications Security.
- **Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits (Cited by 179)** D.Boneh, C.Gentry, S.Gorbunov, S.Halevi, V.Nikolaenko, G.Segev, V.Vaikuntanathan, D.Vinayagamurthy
  EUROCRYPT 2014: 33rd Annual International Conference on the Cryptographic Techniques.
- **Privacy Preserving Matrix Factorization (Cited by 121)**
  V.Nikolaenko, S.Ioannidis, U.Weindberg, M.Joye, N.Taft, D.Boneh
  CCS 2013: 20th ACM Conference on Computer and Communications Securit.
- **Privacy-Preserving Ridge Regression on Hundreds of Millions of Records (Cited by 149)**
  V.Nikolaenko, U.Weindberg, S.Ioannidis, M.Joye, D.Boneh, N.Taft
  IEEE SSP 2013: IEEE Symposium on Security & Privacy
- **Optimal heuristic algorithms for the image of an injective function**
  E.Hirsch, D.Itsykson, V.Nikolaenko, A.Smal
  Zapiski nauchnyh seminarov POMI 399:15-31 (2012)
- **PhD Thesis**: “Studies in secure computation: post-quantum, attribute-based and multi-party”
  Advisor Prof. Dan Boneh. Reading committee: Prof. Moses Charikar, Prof. Omer Reingold
- **MSc Thesis**: “Optimal Deterministic Heuristic Algorithm for the Image of an Injective Function”
  Advisor Prof. Dmitry Itsykson
- **BSc Thesis**: “Enumeration of Permutation Binomials over Finite Fields”
  Advisor Prof. Nikolai Vasiliev

RECENT TALKS

- STOC 2017, Invited Talk: “Practical post-quantum key agreement from generic lattices”
- RWC 2017, “Practical post-quantum key exchange from both ideal and generic lattices”
- Stanford Law School CIS 2016, “Secure Protocol for Accountable Warrant Execution”
- CCS 2016, “Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE”
- CryptoDay Stanford 2016, “Practical, Quantum-Secure Key Exchange for TLS from LWE”

AWARDS, FELLOWSHIPS

- Simons Award for Graduate Students in Theoretical Computer Science, 2014-2016.
- ACM University Student Research Competition (U-SRC) 2013, 3rd prize.

SELECTED PATENTS APPLICATIONS

- Nikolaenko V, et al. Privacy-preserving ridge regression. Application #14/771771, 01/21/2016
- Nikolaenko V, et al. Privacy-preserving ridge regression using masks. Application #14/767569, 12/31/2015
- Nikolaenko V, et al. Privacy-preserving ridge regression using partially homomorphic encryption and masks. Application #14/767568, 02/04/2016.

OTHER

Languages: English, Russian
Interests include mountaineering, bicycle touring, skiing, playing piano.