

Valeria Nikolaenko

Areas of expertise: modern cryptography,
computer and web security, privacy of data collection.

www.valeniko.com
valeria.nikolaenko@gmail.com
US Citizen

EDUCATION

- Sep 2011 – **Stanford University, USA**
Jun 2017 Doctor of Philosophy in Computer Science, GPA: 4.0/4.0
Scientific advisor Prof. Dan Boneh
- Sep 2009 – **University of the Russian Academy of Sciences, Russia**
Jun 2011 Master of Applied Mathematics and Physics
Honors Degree, GPA 4.0/4.0
- Sep 2005 – **St. Petersburg State Polytechnical University, Russia**
May 2009 Bachelor of Applied Mathematics and Computer Science
Honors Degree, GPA 3.9/4.0

EXPERIENCE

- Aug 2017 – **Co-organized a 7000 km cycling expedition across South America**
July 2018 Travel blog: holoholotales.com/en
- Sep 2011 – **Research Assistant, Stanford University, USA**
Jun 2017
 - Discovered “Fully Key-Homomorphic Encryption”, based on random lattices
 - Developed a secure protocol for accountable warrants execution
 - Collaborated with Google on building a new generation of quantum-secure ciphersuites
 - Collaborated with Technicolor on building systems for privacy preserving data-mining
- Jun 2015 – **Software Engineer Intern, Google, Mountain View, USA**
Sep 2015
 - Developed a new key exchange algorithm for TLS based on random lattices
 - Implemented in C and evaluated on emulated internet traffic
 - Co-authored NIST proposal for post-quantum cryptography standard: frodokem.org
- Jun 2012 – **Intern, Technicolor Research, Palo Alto, USA**
May 2013
 - Built a system for privacy preserving data-mining (ridge regression and matrix factorization) on massive datasets, containing >100,000,000 entries
 - Implemented in Java and evaluated on real datasets
 - 7 US patents pending
- Sep 2008 – **Software Engineer, JetBrains/SwiftTeams, St. Petersburg, Russia**
Jun 2011
 - Built new functionality for development environments IntelliJ IDEA, PhpStorm
 - Developed support for ColdFusion, Smarty, PHPUnit, CUnit, MXUnit
- Dec 2009 – **Research Assistant, Laboratory of Mathematical Logic at PDMI RAS, Russia**
Jun 2011 Studied heuristic decision algorithms, built an optimal algorithm for injective functions.
- Nov 2006 – **Software Engineer, Transas, St. Petersburg, Russia**
Feb 2008 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, stereo rendering, volumetric clouds. Worked with C++, OpenGL, Cg.
- Sep 2008 – **Research Assistant, Laboratory of Representation Theory at PDMI RAS, Russia**
Dec 2009 Studied permutation binomials over finite fields and their applications 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
- Lattice based cryptography
- Advanced cryptography: computations on encrypted data, attribute-based encryption
- Languages: Java, C, C++, HTML, CSS

PUBLICATIONS

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 Security

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 AND FELLOWSHIPS

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

SELECTED PATENTS

Nikolaenko V, et al. Privacy-preserving ridge regression. US Patent #14/771771, 01/21/2016

Nikolaenko V, et al. Privacy-preserving ridge regression using masks. US Patent #14/767569, 12/31/2015

Nikolaenko V, et al. Privacy-preserving ridge regression using partially homomorphic encryption and masks. US Patent #14/767568, 02/04/2016

OTHER

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