Valeria Nikolaenko

Updated: 7 Sep 2018

valeria.nikolaenko@gmail.com

EDUCATION

Sep 2011 – Jun 2017 **Stanford University**, USA
Department of Computer Science
Doctor of Philosophy in Computer Science, GPA: 4.0/4.0
Phd Thesis "Studies in secure computation: post-quantum, attribute-based and multi-party"
Scientific advisor - Dan Boneh. Area of research: cryptography

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
MSc Thesis: "Optimal Deterministic Heuristic Algorithm for the Image of an Injective Function". Scientific advisor D.Itsykson (PDMI RAS)

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
BSc Thesis: "Enumeration of Permutation Binomials over Finite Fields". Advisor N.Vasiliev (PDMI RAS)

EXPERIENCE

Aug 2017 – July 2018 **Cycling South America South-to-North**, 7000 km with high altitudes.
Travel blog: holoholotales.com

Sep 2011 – Jun 2017 **Research Assistant, Stanford University, USA**
- Built a system for privacy preserving data-mining on massive data sets: the server learns ridge regression or matrix factorization over users' inputs learning nothing else about users' inputs.
- Developed a new key exchange algorithm for TLS based on hard problems in random lattices. Submitted to NIST as a proposal for new generation of quantum secure ciphers: frodokem.org
- Discovered a new cryptographic primitive "Fully Key-Homomorphic Encryption", it's security is based on hard problems in random lattices. The primitive allows to do smart key management.

Jun 2015 – Sep 2015 **Software Engineer Intern, Google, Mountain View, USA**
Developed, prototyped in C and evaluated new lattice-based quantum resistant ciphersuites within OpenSSL. Emulated internet traffic running this ciphersuite for establishing secure connections.

Jun 2012 – May 2013 **Intern, Technicolor Research, Palo Alto, USA**
Developed, implemented in Java and evaluated a system for privacy preserving data mining: linear regression and matrix factorization. 7 US patents are pending.

Sep 2008 – Jun 2011 **Software Engineer, JetBrains/SwiftTeams, St. Petersburg, Russia.**
Designing of Integrated Development Environments in Java: IntelliJ IDEA, PhpStorm and WebStorm. ColdFusion and Smarty languages support. Test frameworks for Php and ColdFusion.

Dec 2009 – Jun 2011 **Research Assistant, Laboratory of Mathematical Logic at PDMI RAS, St. Petersburg, Russia**
Explored 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**
Development of 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, St. Petersburg, Russia**
Studied permutation binomials over finite fields in search for their application to cryptography.

PAPERS

- J.Bos, C.Costello, L.Ducas, I.Mironov, M.Naehrig, V.Nikolaenko, A.Raghunathan, D.Stebila
  "Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE"
  CCS 2016: 23rd ACM Conference on Computer and Communications Security.
- D.Boneh, C.Gentry, S.Gorbunov, S.Halevi, V.Nikolaenko, G.Segev, V.Vaikuntanathan, D.Vinayagamurthy
  "Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits"**,**
  EUROCRYPT 2014: 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques.
- V.Nikolaenko, S.Ioannidis, U.Weindberg, M.Joye, N.Taft, D.Boneh
  "Privacy Preserving Matrix Factorization"
  CCS 2013: 20th ACM Conference on Computer and Communications Securit.
- V.Nikolaenko, U.Weindberg, S.Ioannidis, M.Joye, D.Boneh, N.Taft
  "Privacy-Preserving Ridge Regression on Hundreds of Millions of Records"
  IEEE SSP 2013: IEEE Symposium on Security & Privacy
- E.Hirsch, D.Itsykson, V.Nikolaenko, A.Smal.
  "Optimal heuristic algorithms for the image of an injective function"
  Zapiski nauchnyh seminarov POMI 399:15-31 (2012)

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 Center for Internet and Society 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.

SKILLS

- Designing 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
- Languages: Java professionally; experienced: C, C++, HTML, CSS; beginner: PHP, Ruby, Python

PATENTS APPLICATIONS

- "Privacy-preserving ridge regression." U.S. Patent Application No. 14/771,771
- "Privacy-preserving ridge regression using masks." U.S. Patent Application No. 14/767,569.
- "Privacy-preserving ridge regression using partially homomorphic encryption and masks." U.S. Patent Application No. 14/767,568.
- "A method and system for privacy preserving matrix factorization." U.S. Patent Application No. 14/771,534.
- "Method and system for privacy preserving counting." U.S. Patent Application No. 14/771,608.
- "A method and system for privacy-preserving recommendation to rating contributing users based on matrix factorization." U.S. Patent Application No. 14/771,659.
- "Method and system for privacy-preserving recommendation based on matrix factorization and ridge regression." U.S. Patent Application No. 14/771,527.

OTHER

Work authorization status: US citizen
Languages: English, Russian
Interests include mountaineering, climbing, cycling, bicycle touring, cross-country and downhill skiing, playing piano, drawing, making toys, dancing Argentinean tango.