

Valeria Nikolaenko

www.valerini.com (650) 260-8363

Areas of expertise: blockchain cryptography,
byzantine and fault-tolerant systems.

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 Department of Mathematical and Informational Technologies
Master of Science with Honors, GPA 4.0/4.0
- Sep 2005 – **St. Petersburg State Polytechnical University, Russia**
May 2009 Department of Applied Mathematics and Informatics
Bachelor of Science with Honors, GPA 3.9/4.0

EXPERIENCE

- Feb 2018 – **Research Scientist, Facebook / Novi Research / Diem Research, USA**
present Light clients. Randomness beacons. VDFs. Distributed key generation. Threshold signatures, Schnorr/EdDSA signatures: security, malleability, half-aggregation. Long-range attack. Elliptic-curve cryptography. NFTs. Smart contracts development.
- Aug 2017 – **Family cycling expedition through South America**
July 2018 Travel blog: holoholotales.com/en
- Sep 2011 – **Research Assistant, Stanford University, USA**
Jun 2017 First “Fully Key-Homomorphic Encryption” construction (based on random lattices). Secure protocol for accountable warrants execution. Quantum-secure cryptography. Privacy preserving data-mining and Multi-Party Computations.
- Jun 2015 – **Software Engineer Intern, Google, Mountain View, USA**
Sep 2015 Developed Frodo, a key exchange algorithm for TLS based on random lattices. Implementation. Co-authoring NIST proposal for post-quantum standard: frodokem.org
- Jun 2012 – **Intern, Technicolor Research, Palo Alto, USA**
May 2013 Privacy preserving data-mining (ridge regression and matrix factorization) on massive datasets (>100,000,000 entries). Java implementation. 7 US patents applications.
- Sep 2008 – **Software Engineer, JetBrains/SwiftTeams, St. Petersburg, Russia**
Jun 2011 Team: IntelliJ IDEA, Php/Web-Storm, supporting ColdFusion, PHPUnit, CFUnit, MXUnit
- Dec 2009 – **Research Assistant, Laboratory of Mathematical Logic at PDMI RAS, Russia**
Jun 2011 Heuristic decision algorithms, constructing optimal algorithm for injective functions.
- Nov 2006 – **Software Engineer, Transas, St. Petersburg, Russia**
Feb 2008 Real-time computer graphics for marine and aviation training. Sea surface rendering, projective grid, underwater effects, stereo, volumetric clouds. C++, OpenGL, Cg.
- Sep 2008 – **Research Assistant, Laboratory of Representation Theory at PDMI RAS, Russia**
Dec 2009 Permutation binomials over finite fields and their applications to cryptography.

SKILLS

- Blockchain cryptography: light clients, randomness beacons, VDFs, distributed key generation, threshold signatures, long-range attacks, post-quantum protection, smart contract development.
- 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
- Java, C, C++, Rust, Solidity, Move

PUBLICATIONS

Threshold Schnorr with Stateless Deterministic Signing from Standard Assumptions

F.Garillot, Y.Kondi, P.Mohassel, [V.Nikolaenko](#). [CRYPTO 2021](#)

Non-interactive half-aggregation of EdDSA and variants of Schnorr signatures

K.Chalkias, F.Garillot, Y.Kondi, [V.Nikolaenko](#). [CT-RSA 2021](#)

Taming the many EdDSAs

K. Chalkias, F.Garillot, [V.Nikolaenko](#). [SSR 2020](#)

Winkle: Foiling Long-Range Attacks in Proof-of-Stake Systems

S.Azouvi, G.Danezis, [V.Nikolaenko](#). [ACM AFT 2020](#)

Lattice-based DAPS and generalizations: Self-enforcement in signature schemes

D.Boneh, S.Kim, [V.Nikolaenko](#). [ACNS 2017](#)

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](#)

Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE, Compact Garbled Circuits (cited by 179)

D.Boneh, C.Gentry, S.Gorbunov, S.Halevi, [V.Nikolaenko](#), G.Segev, V.Vaikuntanathan, D.Vinayagamurthy. [EUROCRYPT 2014](#)

Privacy Preserving Matrix Factorization (cited by 121)

[V.Nikolaenko](#), S.Ioannidis, U.Weindberg, M.Joye, N.Taft, D.Boneh. [CCS 2013](#)

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](#)

Optimal heuristic algorithms for the image of an injective function

E.Hirsch, D.Itsykson, [V.Nikolaenko](#), A.Smal. Zapiski nauchnyh seminarov POMI (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

PROGRAM COMMITTEE

SBC 2021, ACM CCS 2021, SBC 2022, ACM CCS 2022

OPENSOURCE PROJECTS

Ristretto255-js: github.com/novifinancial/ristretto255-js

Java-script implementation of arithmetic for co-factor free elliptic-curve group ristretto255.

FrodoKEM: frodokem.org

"Round 3 alternate candidate" in the [NIST Post-Quantum Cryptography Standardization project](#).

Ed25519-speccheck: github.com/novifinancial/ed25519-speccheck

Methodology to check conformance of EdDSA implementations across blockchain clients.

OTHER

Languages: English, Russian

I am a big fan of cross-country skiing, bicycle touring, sailing, mountaineering, illustrating and sketching.