Valeria Nikolaenko, PhD

www.valerini.com (650) 260-8363
valeria.nikolaenko@gmail.com
US Citizen

Areas of expertise: cryptography (traditional, blockchain, post-quantum), privacy, computer and web security.

EDUCATION

Sep 2011 – Jun 2017 — PhD, **Stanford University**, USA
Doctor of Philosophy in Computer Science, GPA: 4.0/4.0
Scientific advisor Prof. Dan Boneh

Sep 2009 – Jun 2011 — MSc, **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 — BSc, **St. Petersburg State Polytechnical University**, Russia
Department of Applied Mathematics and Informatics
Bachelor of Science with Honors, GPA 3.9/4.0

EXPERIENCE

May 2022 - present — **Research Partner, Andreessen-Horowitz, a16z Crypto Research, USA**
Independent research, consulting for portfolio companies, technical assessment of projects. For blog-posts, podcasts, research papers and more: a16zcrypto.com/team/valeria-nikolaenko

Feb 2018 – May 2022 — **Research Scientist, Meta / Facebook / Novi Research / Diem Research, USA**
Worked on core technologies underlying the Diem blockchain project as a member of Cryptography Research Team. Focusing on threshold signatures, Schnorr/EdDSA, distributed key generation, post-quantum security, light clients, randomness beacons, long-range attack, NFTs, smart contracts development.

Aug 2017 – July 2018 — **Cycling expedition through South America**
Ushuaia (Argentina) to Medellin (Colombia)
Travel blog: holoholotales.com/en

Sep 2011 – Jun 2017 — **Research Assistant, Stanford University, USA**
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 – Sep 2015 — **Software Engineer Intern, Google, Mountain View, USA**
Developed Frodo, a key exchange algorithm for TLS based on random lattices. Co-authoring NIST proposal for post-quantum standard: frodokem.org

Jun 2012 – May 2013 — **Intern, Technicolor Research, Palo Alto, USA**
Privacy preserving data-mining (ridge regression and matrix factorization) on massive datasets (>100,000,000 entries). Java implementation.

Sep 2008 – Jun 2011 — **Software Engineer, JetBrains/SwiftTeams, St. Petersburg, Russia**
IntelliJ IDEA, Php/Web-Storm, supporting ColdFusion, PHPUnit, CFUnit, MXUnit

Dec 2009 – Jun 2011 — **Research Assistant, Laboratory of Mathematical Logic at PDMI RAS, Russia**
Heuristic decision algorithms, constructing an optimal algorithm for injective functions.

Nov 2006 – Feb 2008 — **Software Engineer, Transas, St. Petersburg, Russia**
Real-time computer graphics for marine and aviation training. Sea surface rendering, projective grid, underwater effects, stereo, volumetric clouds. C++, OpenGL, Cg.

Sep 2008 – Dec 2009 — **Research Assistant, Laboratory of Representation Theory at PDMI RAS, Russia**
Permutation binomials over finite fields and their applications to cryptography.

PUBLICATIONS

Atomic and Fair Data Exchange via Blockchain
E.N.Tas, I.A.Seres, Y.Zhang, M.Melczer, M.Kelkar, J.Bonneau, V.Nikolaenko. **In submission**

Powers-of-tau to the people: Decentralizing setup ceremonies
V.Nikolaenko, S.Ragsdale, J.Bonneau, D.Boneh. **ACNS 2024**

STROBE: Streaming Threshold Random Beacons. D.Beaver, K.Chalkias, M.Kelkar, L.Kokoris-Kogias, K.Lewi, L.de Naurois, V.Nikolaenko, A.Roy, A.Sonnino. **AFT 2023**

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**

Homomorphic decryption in blockchains via compressed discrete-log lookup tables
P.Chatzigiannis, K. Chalkias, V.Nikolaenko. **DPM 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 453)
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 447)
D.Boneh, C.Gentry, S.Gorbunov, S.Halevi, V.Nikolaenko, G.Segev, V.Vaikuntanathan, D.Vinayagamurthy. **EUROCRYPT 2014**

Privacy Preserving Matrix Factorization (cited by 346)
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 553)
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 SERVICE

CCS24, AFT24, RWC24, FC24, ACNS24, AFT23, FC23, CCS23, SBC23, CCS22, SBC22, CCS21, SBC21.

OPEN-SOURCE 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 Fluent in English and Russian. I am a big fan of cross-country skiing, bicycle touring, sailing, hiking and argentine tango.