



Kirill Nikitin

Curriculum Vitae
EPFL IC IINFCOM DEDIS, BC 209,
Station 14, CH-1015 Lausanne, Switzerland
+47 21 6935613, mob. +47 77 9866320
kirill.nikitin@epfl.ch
<https://nikirill.com>

OVERVIEW

I am a forth-year Ph.D. student in the [Decentralized/Distributed Systems lab](#) at EPFL working in the areas of Systems Security, Distributed Systems and Privacy. In particular, my experience is in building secure peer-to-peer systems, designing distributed ledgers and smart contract solutions, securing software-update systems and developing techniques for anonymous communication.

I am looking for a research internship for summer 2019 in the areas of blockchain / smart contracts or privacy-enhancing technologies!

QUALIFICATION SUMMARY

- Smart contracts, blockchain, Solidity, consensus mechanisms;
- Decentralized systems: communication, storage, sybil-resistance;
- Design of data and communication privacy techniques, metadata protection;
- Network protocols (TLS, TCP/IP, DNS, BGP), security in wireless networks and constrained environments (DTLS, CoAP);
- Computer security and software containerization (Docker);
- Distributed systems programming;
- Coding proficiency: Go, C, Python.

EDUCATION

- Ph.D. Computer and Communication Sciences** 2015-now
Decentralized/Distributed Systems Lab, École polytechnique fédérale de Lausanne, Switzerland
“Decentralized Cooperation and Its Applications in Security”
Thesis advisor: B. Ford
- M.S. Communication Systems** 2013-2015
KTH Royal Institute of Technology, Stockholm, Sweden
Thesis: “[DTLS Adaptation for Efficient Secure Group Communication](#)” @ RISE SICS
Research/Academic advisors: M. Tiloca, S. Raza (both RISE SICS), M. Hidell (KTH)
- Specialist Degree Information Security (with honors)** 2008-2013
Kazan (Volga Region) Federal University, Russia

Thesis: “Cryptographic Key Distribution via Randomness from Multipath Propagation of Radio Waves”
Research/Academic advisor: A. Karpov

Exchange Student Computer Science
University of Helsinki, Finland

2012

PUBLICATIONS AND REPORTS [stat]

4. [K. Nikitin](#), L. Barman, M. Underwood, B. Ford, “[Reducing Metadata Leakage from Encrypted Files and Communication with PURBs](#)”, In *CoRR*, 1806.03160, arXiv, 2018, *Under submission*.
3. C. Basescu, M. Nowlan, [K. Nikitin](#), J. Faleiro, and B. Ford, “[Crux: Locality-Preserving Distributed Services](#)”, In *CoRR*, 1405.0637, arXiv, 2018, *Under submission*.
2. [K. Nikitin](#), E. Kokoris-Kogias, P. Jovanovic, N. Gailly, L. Gasser, I. Khoffi, J. Cappos, and B. Ford. “[CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds](#)”. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 1271–1287, Vancouver, BC, 2017.
1. M. Tiloca, [K. Nikitin](#), S. Raza. “[Axiom: DTLS-Based Secure IoT Group Communication](#)”. In *ACM Trans. Embed. Comput. Syst. (TECS), Special Issue on Embedded Computing for IoT*, 16(3), 66, April 2017.

PROFESSIONAL EXPERIENCE

Research Intern

Aug–Nov 2018

Systems Security and Privacy Group, Microsoft Research

- Research project on improving scalability and privacy of smart contracts via off-chain execution and verifiable computation.

External Master’s Thesis

Jan–Jun 2015

Security Lab, RISE Swedish Institute of Computer Science

- Work on securing group communication in the IoT.

Research Intern

Jun–Aug 2014

Laboratory for Cryptologic Algorithms, EPFL

- Factorization of openly accessible public keys ($\approx 50M$), suffering from the lack of randomness. My tasks were improving the existing implementation, modifying the algorithm to handle an order-of-magnitude larger amount of data, and analyzing the collected data set.

AWARDS

- 2015: EPFL Fellowship for Doctoral Studies
- 2013-2015: [The Swedish Institute Scholarship](#)
- 2009, 2011, 2012: Triple scholar of [Vladimir Potanin Fellowship Program](#)

TEACHING AND SUPERVISION

- **CS-438 Decentralized Systems Engineering** (Fall 17, 18)
 - Designing and implementing homework assignments, supervising semester group projects, student progress evaluation throughout semester.
- **COM-402 Information Security and Privacy** (Spring 17, 18)
 - Designing and implementing CTF-style exercise labs and guiding students. *Student reviews:* “Best homeworks I’ve ever had at EPFL so far. They are neither too guided or too free just perfect...” “Exercises are really interesting...” “Homeworks are awesome.” “Oscillating between ”These exercises are insufferable!” (before you get your token...) and ”These exercises are so fun!” (after you get your token!) ...” “The Exercises are not always easy, but they are fun to do and give a good practical insight into security.”
- **MATH-101 Analyse I** (Fall 16)
 - Guiding students during exercise solving.
- **COM-102 Advanced information, computation, communication II** (Spring 16)
 - Designed exercise for basic cryptography (part of the course) and guided students

Supervision:

- Simone Colombo. “DecenArch: a decentralized system for privacy-conscious Web archiving against censorship”. *Master’s thesis* (Spring 2018).
- Nicolas Plancherel. “Decentralized Internet Archive”. *Master’s thesis* (Fall 2017).
- Nicolas Ritter. “Access Control In Real-Time Peer-to-Peer Collaboration”. *Master semester project* (Fall 2017).
- Damien Aymon. “Implementation of an Algorithm for Peer-to-Peer Collaborative Editing”. *Bachelor semester project* (Spring 2017).
- Rehan Mulakhel. “Web Interface for Secure Decentralized Collaboration Platform”. *Bachelor semester project* (Spring 2017).
- Gaspard Zoss. “Enhancing Debian Update Service”. *Master semester project* (Fall 2017).

PROFESSIONAL AND EXTRACURRICULAR ACTIVITIES

- Member of the Technical Program Committee at
 - **ICBC 2019**: IEEE International Conference on Blockchain and Cryptocurrency 2019
 - **CryBlock 2019**: 2nd Workshop on Cryptocurrencies and Blockchains for Distributed Systems.
- Sub-reviewer for ACM Conf. on Computer and Communications Security 2017.
- I was a president of a graduate student association at IC EPFL. Organized invited talks, activities for current students, and helped with the organization of Open Houses for newcomers.
- Back in the past, I played in a student theater, performing team comedy stand-ups.