

## Kirill Nikitin

Updated: 28/07/2021

Curriculum Vitae  
EPFL IC IINFCOM DEDIS, BC 209,  
Station 14, CH-1015 Lausanne, Switzerland

mob. +47 77 9866320  
[kirill.nikitin@epfl.ch](mailto:kirill.nikitin@epfl.ch)  
<https://nikirill.com>

## Education

---

### Ph.D. Computer and Communication Sciences

Sep 2015–Aug 2021

*École polytechnique fédérale de Lausanne, Switzerland*

Thesis: “Integrity and Metadata Protection in Data Retrieval”. Oral exam: 20/07/2021

Advisor: Bryan Ford

### M.S. Communication Systems

Sep 2013–Jun 2015

*KTH Royal Institute of Technology, Sweden*

Thesis: “DTLS Adaptation for Efficient Secure Group Communication” @ RISE SICS

Advisors: Marco Tiloca, Shahid Raza (both RISE SICS), Markus Hidell (KTH)

### Diploma Information Security (with honors)

Sep 2008–Jun 2013

*Kazan (Volga Region) Federal University, Russia*

Thesis: “Cryptographic Key Distribution via Randomness from Multipath Propagation of Radio Waves”

Advisor: Arkady Karpov

### Exchange Student Computer Science

Jan–May 2012

*University of Helsinki, Finland*

## Refereed Publications [\[Google Scholar\]](#)

---

4. J. Lee, [K. Nikitin](#), S. Setty. “[Replicated state machines without replicated execution](#)”. In *IEEE Symposium on Security and Privacy*, 2020.
3. [K. Nikitin](#), L. Barman, W. Lueks, M. Underwood, J.-P. Hubaux, B. Ford. “[Reducing Metadata Leakage from Encrypted Files and Communication with PURBs](#)”. In *Privacy Enhancing Technologies Symposium*, 2019.
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 *USENIX Security Symposium*, 2017.
1. M. Tiloca, [K. Nikitin](#), S. Raza. “[Axiom: DTLS-Based Secure IoT Group Communication](#)”. In *ACM Transactions on Embedded Computing Systems (TECS), Special Issue on Embedded Computing for IoT*, 16(3), 66, April 2017.

### Reports and manuscripts under submission:

2. S. Colombo, [K. Nikitin](#), B. Ford, H. Corrigan-Gibbs. “Verifiable private information retrieval”. In *Under submission*, 2021.
1. C. Basescu, M. Nowlan, [K. Nikitin](#), J. Faleiro, and B. Ford, “[Crux: Locality-Preserving Distributed Services](#)”. Technical report, in *CoRR*, 1405.0637, arXiv, 2018.

## Professional Experience

---

**Doctoral Researcher** Sep 2015–Aug 2021

*Decentralized and Distributed Systems laboratory, EPFL, Lausanne, Switzerland*

The lead of the research projects on:

- Exploiting and protecting metadata in encrypted files and communications;
- Security and transparency of software-distribution systems.

**Research Intern** Aug–Oct 2019

*Confidential Computing Group, Microsoft Research, Cambridge, UK*

- Information-flow control for confidentiality in smart contracts.

**Research Intern** Aug–Nov 2018

*Systems Security and Privacy Group, Microsoft Research, Redmond, US*

- Improving scalability 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, Stockholm, Sweden*

- Designing a protocol for secure group communication for the Internet-of-Things.

**Research Intern** Jun–Aug 2014

*Laboratory for Cryptologic Algorithms, EPFL, Lausanne, Switzerland*

- Integer factorization and analysis of public-key ecosystem weaknesses.

## Academic Service and Extracurricular Activities

---

- A member of the program committee or the student editorial board for
  - [JSys 2021](#): Journal of Systems Research
  - [ACM CCS 2021 Posters & Demos](#)
  - [CryBlock 2019, 2020](#): Workshop on Cryptocurrencies and Blockchains for Distributed Systems
  - [BlockSys 2019](#): Workshop on Blockchain-enabled Networked Sensor Systems
  - [ICBC 2019](#): IEEE International Conference on Blockchain and Cryptocurrency
- An external reviewer for IEEE Transactions on Industrial Informatics 2019 and IEEE Transactions on Parallel and Distributed Systems 2020, and ACM CCS 2017, 2021.
- 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.

## Teaching and Supervision

---

- [CS-438 Decentralized Systems Engineering](#) (Fall 17, 18, 20)  
As a part of a team, designed, implemented and graded homework assignments, gave guest lectures, supervised semester group projects, and evaluated student progress throughout semester. *Student reviews*:  
“The course is very demanding as time is concerned but the topics and the assignments are very fascinating.” “The TAs are awesome. I can’t imagine the problem they went through preparing these testcases.”

- **ICC Information, Computation and Communication** (Spring 20)  
Guided students during exercise solving.
- **CS-234 Technologies of societal self-organization** (Fall 19)  
Participated in the design of the brand-new course: guiding projects and creating assignments, quizzes, and the exam.
- **COM-402 Information Security and Privacy** (Spring 17, 18)  
As a part of a team, designed and implemented CTF-style exercise labs from scratch, contributed to creating lectures and guided 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)  
Guided students during exercise solving.
- **COM-102 Advanced information, computation, communication II** (Spring 16)  
Designed exercises on basic cryptography (part of the course) and guided students.

#### Supervision:

- Fernando Monje Real. “Traffic analysis of real-time collaborative editors”. *Master’s thesis* (Spring 20).
- Carlos Villa Sánchez. “Secure management of browser extensions and their dependencies”. *Master’s thesis* (Spring 20).
- Charles Parzy-Turlat. “Tree-based Group Key Agreement”. *Master’s project* (Spring 19).
- Simone Colombo. “DecenArch: a decentralized system for privacy-conscious Web archiving against censorship”. *Master’s thesis* (Spring 18).
- Nicolas Plancherel. “Decentralized Internet Archive”. *Master’s thesis* (Fall 17).
- Nicolas Ritter. “Access Control In Real-Time Peer-to-Peer Collaboration”. *Master’s project* (Fall 17).
- Damien Aymon. “Implementation of an Algorithm for Peer-to-Peer Collaborative Editing”. *Bachelor’s project* (Spring 17).
- Rehan Mulakhel. “Web Interface for Secure Decentralized Collaboration Platform”. *Bachelor’s project* (Spring 17).
- Gaspard Zoss. “Enhancing Debian Update Service”. *Master’s project* (Fall 17).

## Awards

---

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