Kirill Nikitin

Curriculum Vitae
The New York Genome Center
101 Avenue of the Americas, New York, NY 10013

Updated: 10/02/2025

mob. +1 929 2565684
kirill.nikitin@columbia.edu
https://nikirill.com

Education

Ph.D. Computer and Communication Sciences   Sep 2015–Nov 2021
École polytechnique fédérale de Lausanne, Switzerland
    Thesis:"Integrity and Metadata Protection in Data Retrieval"

M.S. Communication Systems   Sep 2013–Oct 2015
KTH Royal Institute of Technology, Sweden
    Thesis: "DTLS Adaptation for Efficient Secure Group Communication" @ RISE SICS

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"

Refereed Publications [Google Scholar]

5. S. Colombo, K. Nikitin, B. Ford, D. Wu, H. Corrigan-Gibbs. "Authenticated private information retrieval". In *USENIX Security Symposium*, 2023.

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". *Proceedings on Privacy Enhancing Technologies, 2019(4)*, 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*, 2017.

Reports and manuscripts:

2. C. Basescu, M. Nowlan, K. Nikitin, J. Faleiro, and B. Ford, "Crux: Locality-Preserving Distributed Services". Technical report, in *CoRR*, 1405.0637, arXiv, 2018.

1. M. Tiloca, S. Raza, K. Nikitin, and S. Kumar. "Secure Two-Way DTLS-Based Group Communication in the IoT (work in progress)". *IETF*, 2015.

Professional Experience

Post-Doctoral Researcher   May 2023–now
G^2 *lab*, **Columbia University & New York Genome Center**, New York, NY

- Privacy-preserving analysis and sharing of biomedical data.

Post-Doctoral Researcher   Mar 2022–April 2023
Cornell Tech, **Cornell University**, New York, NY

- Protecting network metadata in online communication.

Doctoral Researcher   Sep 2015–Aug 2021
Decentralized and Distributed Systems laboratory, **EPFL**, Lausanne, Switzerland

- 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 editorial board for
  - USENIX Security 2025: USENIX Security Symposium
  - ACM CCS 2023, 2024: ACM Conference on Computer and Communications Security
  - RECOMB-PRIEQ 2024: Satellite Conference on Biomedical Data Privacy and Equity
  - 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 ISMB 2025, RECOMB 2024, 2025, Eurocrypt 2022, IEEE Transactions on Industrial Informatics 2019, IEEE Transactions on Parallel and Distributed Systems 2020, and ACM CCS 2017, 2021.

- I was a president of the graduate student association at IC EPFL where I organized invited talks, activities for students, and helped with the organization of Open Houses for newcomers.

Teaching and Supervision

- **CS-438 Decentralized Systems Engineering** (Fall 17, 18, 20)
- **ICC Information, Computation and Communication** (Spring 20)
- **CS-234 Technologies of societal self-organization** (Fall 19)
- **COM-402 Information Security and Privacy** (Spring 17, 18)
- **MATH-101 Analyse I** (Fall 16)
- **COM-102 Advanced information, computation, communication II** (Spring 16)

Awards

- 2020: The Doc.Mobility Fellowship from the Swiss National Science Foundation (declined)
- 2015: EPFL EDIC Fellowship for Doctoral Studies
- 2013-2015: The Swedish Institute Scholarship
- 2009, 2011, 2012: Triple scholar of The Vladimir Potanin Fellowship Program