Volkhov Mikhail

Edinburgh,
United Kingdom

Citizenship: Russian
mikhail.volkhov@ed.ac.uk

EDUCATION

University of Edinburgh, Edinburgh, UK — Expected Aug 2023

PhD student in Computer Science.
Blockchain Technology Laboratory, School of Informatics.
Supervised by Markulf Kohlweiss.

ENS Paris-Saclay, Paris, France — Aug 2019

MSc in Computer Science "Master Parisien de Recherche en Informatique" (MPRI)
Joint programme by ENS, ENS Paris-Saclay, University Paris Diderot, INRIA, CNRS, and others.
7/11 of the selected courses were focused on cryptography.

ITMO University, Saint Petersburg, Russia — Jun 2017

BSc in Applied Mathematics and Computer Science.
Thesis title "Blockchain-Based Time-Tracking and Rating System".
Top 5/60, GPA 4.4/5.

PUBLICATIONS

1. K. Baghery, M. Kohlweiss, J. Siim, M. Volkhov: *Another Look at Extraction and Randomization in Groth's zk-SNARK.* Financial Cryptography 21.

   Investigates randomization in Groth's zk-SNARK, which allows to prove a stronger security property of the scheme. Suggests two different black-box NIZK constructions that take advantage of this new security property. These constructions can be used in Universally Composable proofs directly, and are more efficient than previous solutions, providing different trade-offs.

2. M. Kohlweiss, M. Maller, J. Siim, M. Volkhov: *Snarky Ceremonies.* 4th ZKProof workshop, 2021. Eprint 2021/219.

   Provides a rigorous treatment to the commonly used multi-party "ceremony" protocol that is used to generate the trusted parameters for pairing-based zk-SNARKs. The protocol is also simplified both structurally and functionally (we show that is not necessary to use the random beacon).

EXPERIENCE

Research intern — PROSECCO, INRIA
Paris, France — Apr – Aug 2019

Techniques, Software, and Applications for Packed Partially Homomorphic Encryption. Part of the master's thesis on Secure Machine Learning, supervised by Karthikeyan Bhargavan. Preprint.

Develops a parallelization mode for additively homomorphic cryptosystem that gives batched execution performance improvement. It it used to modify, parallelize, and in eventually speed up a common multiparty computation procedure used by different machine learning classifiers such as SVM. Also includes a verified implementation of three partially homomorphic schemes in the general purpose dependently-typed language F*, with respect to which the performance is evaluated.

Software developer — Serokell OÜ
Saint Petersburg, Russia — Nov 2015 – Sep 2018

Functional programming oriented software development.

- Cardano SL cryptocurrency core (in partnership with IOHK), second biggest contributor (as of 2018).
- Several more cryptocurrency-related projects including RSCoin (*Centrally Banked Cryptocurrencies* by G. Danezis and S. Meiklejohn) and Disciplina blockchain, numerous internal projects and libraries.

TEACHING

Teaching assistant University of Edinburgh
Jan – May 2020, 2021 Edinburgh

Introduction to Modern Cryptography course (2020 and 2021 years). Preparing the assignments. Verifying and marking courseworks and exams. Providing technical Q/A communication with students.

Teaching assistant ITMO University
2015 - 2017 Saint Petersburg

Was assisting with several university courses:

- Functional programming course, fall 2017. Marking courseworks, helping with the exam.
- Extended type theory (seminars) course, fall-spring 2014-2016. Giving lectures, preparing the course material.

PROJECTS

Member of the PRIViLEDGE project since Oct 2019 (European Union's Horizon 2020).
`https://priviledge-project.eu/`

OTHER

Talks: Financial Cryptography 2021, ZKProof 4 2021
Organizer: Security and Privacy Seminar (UoE 2019/2020)
Participant: Summer school on real-world cryptography and privacy, Šibenik, Croatia, Jun 2019; Composable and Code-based Cryptography reading group (UoE 2019/2020); Nordic SNARKs seminars (organized by Simula/Bergen 2020/2021).
Reviews: EC'20, AC'20, TCC'20, PETS'21, FC'21, AC'21, S&P'22.

PRACTICAL SKILLS

Programming Languages: Haskell (substantial), F*, Bash, Python, Java, Scala, C, C++, OCaml, Asm (y/n/g).
Sorted by experience in descending order. I have contributed to multiple open-source projects to different extent.

Technologies: OS/deployment: Unix/Linux, Nix(OS), Nixops; Mobile development (Android Java/Scala).

FURTHER INFORMATION

Languages: English (fluent), Russian, Ukrainian (both native).
Github: `https://github.com/volhovm`
Personal website: `https://metajoin.de` (includes more contact information)