+352 671 300487 marblesurf.github.io yurkov.semen@gmail.com

SEMYON YURKOV

PROFILE

I am a cybersecurity researcher, specializing in the design and analysis of cryptographic protocols. The focus of my work is traditional card payments (EMV) and methods that can be employed to reason about the privacy of systems in general. I also enjoy teaching students programming languages and modelling security protocols on both bachelor and master levels.

EDUCATON

PhD in Computer Science

2023: *"Analysis of smartcard-based payment protocols in the applied pi-calculus using quasi-open bisimilarity."* University of Luxembourg, Esch-sur-Alzette, Luxembourg.

MS in Economics

2012: *"Solution to the generalised bankruptcy problem."* Higher School of Economics, Moscow, Russia. Best student research paper award.

Ed.S. in Mathematics

2010: *"Extremal problems in plane geometry."* Kuzbass State Pedagogical Academy, Novokuznetsk, Russia.

KEY SKILLS

- Excellent writing & presentation
- Thoroughness
- Analytic thinking
- Curiosity
- IT: Java, Git, SQL, Jira, LaTeX, SageMath etc.

LANGUAGES

- English (fluent)
- Russian (mother)
- Italian (limited proficiency)
- Luxembourgish (beginner)

INTERESTS

- Skyrunning
- Cycling
- Cooking
- Local history
- Visiting museums

WORK EXPERIENCE

University of Luxembourg *Esch-sur-Alzette | Luxembourg*

2023-2024: Postdoctoral researcher. Developed a payment protocol, allowing to process payments while keeping all card details private to the merchant's terminal, while guaranteeing essential security to the bank, the merchant, and the cardholder, and that can coexist with the current payment infrastructure – published at a Big 4 security conference. Worked on algorithms for releasing social graph statistics in a differentially private way. Wrote paper reviews. The main lecturer in Security Protocols graduate class, improved student feedback in comparison to previous years.

2019-2023: Doctoral researcher. Worked on developing a method to model privacy of security protocols. Applied it to demonstrate that the key agreement, proposed by the developers of EMV to introduce privacy in payments, does not fulfil its goal – publications in A-level journals and conferences. Was running lab sessions in programming classes (*C* and *Swift*). Visited and presented at multiple venues. Wrote and sucessfully defended a doctoral thesis.

Rostelecom Information Technologies *Moscow | Russia*

2018-2019: Java software engineer. Implemented new features for the CRM system of Rostelecom (50+ million clients, infrastructure in 11 time zones) – integration with a fronted for businesses, KPIs for incident management. Proposed and developed a study program for new employees. SCRUM master of the team.

University of Trento *Trento | Italy*

2013-2016: Doctoral researcher. Worked on applications of Cox rings for studying Mori Dream Spaces, with a weighted projective space/blow-up as an ample divisor.

Self-employment *Moscow | Russia*

2008-2012: Private tutor. Prepared bachelor and high school students for qualifying exams in mathematics, physics, informatics and economics.

PUBLICATIONS

2023: Bursuc, S., Horne, R., Mauw, S., Yurkov S., *Provably unlinkable smart cards-based payments* in the proceedings of the ACM conference on Computer and Communications Security (CCS)

2023: Horne, R., Mauw, S., Yurkov S., *Whenever a privacy property fails, a formula describes an attack: a complete and compositional verification method for the applied pi-calculus* in Theoretical Computer Science (TCS) journal

2022: Horne, R., Mauw, S., Yurkov S., *Unlinkability of an improved key agreement protocol for EMV 2nd Gen payments* in the proceedings of the Computer Security Foundations Symposium (CSF) conference

2021: Horne, R., Mauw, S., Yurkov S., *Compositional analysis of protocol equivalence in the applied pi-calculus using quasi-open bisimilarity* in the proceedings of International Colloquium on Theoretical Aspects of Computing (ICTAC) conference

2012: Karpov, A., Yurkov S., *Generalized bankruptcy problem* in NRU HSE Series: Financial Economics journal