Semen Yurkov

Luxembourg yurkov.semen@gmail.com +352 671 30 04 87 marblesurf.github.io

Education

University of Luxembourg Esch-sur-Alzette, Luxembourg *2023*
PhD in Computer Science

Higher School of Economics Moscow, Russia *2012*
MS in Economics

Kuzbass State Pedagogical Academy Novokuznetsk, Russia *2010*
Ed.S. in Mathematics

Experience

Postdoctoral researcher
University of Luxembourg, Esch-sur-Alzette, Luxembourg *2023-24*

- Developed a payment protocol that allows processing payments while keeping all card details private to the merchant's terminal, guarantees essential security for the bank, the merchant, and the cardholder, and can coexist with the current payment infrastructure
- Worked on algorithms for releasing social graph statistics in a differentially private way

Doctoral researcher
University of Luxembourg, Esch-sur-Alzette, Luxembourg *2019-23*

- Worked on methodology to verify the privacy of cryptographic protocols; applied it to demonstrate that the key agreement, proposed by the developers of the EMV standard to introduce privacy in payments, does not fulfil its goal
- Defended the doctoral thesis Analysis of smartcard-based payment protocols in the applied π-calculus using quasi-open bisimilarity

Java software engineer
RTK IT, Moscow, Russia *2018-19*

- Implemented new features for the CRM system of the largest digital services provider in Russia (50+ million customers, infrastructure in 11 time zones), i.e., integration with a frontend for businesses, KPI system for incident management
- Proposed and developed a study program for new employees
- Was a SCRUM master of the team

Doctoral researcher in Algebraic Geometry
University of Trento, Trento, Italy *2013-16*

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

Private tutor
Self-employment, Moscow, Russia *2008-12*

- Prepared bachelor and high school students for qualifying exams in mathematics, physics, informatics and economics

Publications

- S. Bursuc, R. Horne, S. Mauw, and S. Yurkov. **Provably unlinkable smart cards-based payments**. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS'23), Copenhagen, Denmark, November 2023, pages 1392–1406. ACM.
- R. Horne, S. Mauw, and S. Yurkov. **When privacy fails, a formula describes an attack: A complete and compositional verification method for the applied π-calculus**. Theoretical Computer Science, 959(113842), May 2023. Elsevier.
- R. Horne, S. Mauw, and S. Yurkov. **Unlinkability of an improved key agreement protocol for EMV 2nd Gen payments**. In Proceedings of the 35th IEEE Computer Security Foundations Symposium (CSF'22), Haifa, Israel, August 2022, pages 348-363. IEEE Computer Society.
- R. Horne, S. Mauw, and S. Yurkov. **Compositional analysis of protocol equivalence in the applied π-calculus using quasi-open bisimilarity**. In Proceedings of the 18th International Colloquium on Theoretical Aspects of Computing (ICTAC'21), Nur-Sultan, Kazakhstan, September 2021, volume 12819 of LNCS, pages 235-255. Springer-Verlag.
- A. Karpov, S. Yurkov. **Generalized bankruptcy problem**. Higher School of Economics, Series "Financial Economic". Volume 8, November 2012. **Best student research paper award**.

Paper reviews

ICTAC 2020, SECRYPT 2021, WPES 2022, IEEE DSC 2022, ESORICS 2022, ACM CODASPY 2024, ARES 2024

Selected Talks

SRM 2018, FOSAD 2021, VTSA 2021, FCS 2022, STEP 2023 TU Delft 2023

Teaching (University of Luxembourg)

Graduate classes

Fall 2023: Security Protocols – Main Lecturer

Fall 2019-22: Security Protocols – Teaching Assistant

Undergraduate classes

Spring 2021-22: Programming II (C and Swift) – Lab Sessions

Spring 2021: Security II – Lecturer

Spring 2020: Programming Fundamentals II (Swift) – Lab Sessions

Languages

- English (fluent)
- Russian (mother tongue)
- Italian (advanced)
- Luxembourgish (intermediate)

Citizenships

- Luxembourg
- Russia