Ilia Iliashenko

Cryptography Research Engineer — SMPC · FHE · ZKP · Lattice / Post-Quantum

Antwerp, Belgium (EU citizen) · iliailiashenko@gmail.com · GitHub · LinkedIn · Google Scholar

SUMMARY

Cryptography research engineer with 11 years of experience taking privacy-enhancing technologies from theory to production including

- Design and implementation of the three-party SMPC protocol behind World ID iris authentication (Rust),
- SMPC solutions for enterprise machine-learning and data-collaboration use cases (Rust / Python),
- Implementation of the CKKS scheme in Microsoft SEAL (used by the Microsoft Edge Password Monitor),
- Design of the labeled PSI protocol that Microsoft's APSI library is based on,
- PhD in fully homomorphic encryption (KU Leuven),
- 14 peer-reviewed papers including 3× Eurocrypt, Asiacrypt, ACM CCS and CHES.

CORE SKILLS

Cryptography: secure multi-party computation, fully homomorphic encryption, lattice-based / post-quantum cryptography, zero-knowledge proofs, private set intersection, security & leakage analysis

Engineering: Rust, C++, Python, Lean, Circom, Protobuf, SageMath, Magma, R; performance tuning of distributed protocols (round complexity vs. bandwidth vs. throughput); agentic development with Claude Code; LP solvers (Gurobi, RoundingSAT, Exact)

Languages: English (full professional), Russian (native), Dutch (intermediate), German (elementary)

EXPERIENCE

Research Engineer · Inversed Tech — Oct 2024 – Jun 2026

Remote · cryptography R&D consultancy (ZK, SMPC), Madrid, Spain

- Co-designed and implemented the **3-party SMPC protocol for World ID biometric authentication** (github, Rust): privacy-preserving fuzzy iris matching via fractional Hamming distance using the ABY3 protocol; irises stay protected both at rest and in use.
- Owned the **security analysis of the HNSW-based private search** that replaced a non-scaling linear database scan: reduced the leakage of distance orderings to a pseudo-boolean constraint system, estimated computational and statistical security with LP solvers, and designed countermeasures (oblivious shuffling and partial-sorting sub-protocols).
- Optimised the end-to-end SMPC pipeline for **latency vs. throughput** under production infrastructure limits, e.g. selecting different binary-adder circuits per sub-protocol to trade communication rounds against bandwidth.
- Prototyped a regulated privacy-focused crypto mixer including a proof of encryption for ML-KEM in Circom.

Research Engineer · Ciphermode Labs (DBA Pyte) — Aug 2021 – Sep 2024

Remote · privacy-enhancing technologies start-up, Los Angeles, US

- Contributed to **CipherCore**, the company's open-source library implementing the ABY3 three-party SMPC protocol (Rust / Python).
- Designed and evaluated SMPC-based solutions for **ML inference and training, private data collaboration, private database retrieval and membership testing** for clients ranging from multinationals with complex cloud infrastructure to consortia of peer organisations running distributed servers.
- Assessed the practical limits of FHE versus 3-party SMPC for each use case and steered technology choices towards SMPC and ZKP where they better met clients' performance and deployment constraints.
- Contributed to deploying SMPC-based solutions on clients' Azure and GCP infrastructure.

Postdoctoral Researcher (FWO Junior Postdoctoral Fellow) · COSIC, KU Leuven — May 2019 – Aug 2021

Leuven, Belgium

- Co-designed **FINAL**, a new FHE scheme based on NTRU and LWE with faster bootstrapping, and its C++ implementation (Asiacrypt 2022).
- Co-designed, with Microsoft Research, a **labeled unbalanced private set intersection protocol** with reduced computation and communication (ACM CCS 2021), which is the basis of Microsoft's open-source **APSI library**.
- Developed faster homomorphic comparison, string search and counting algorithms (PETS 2021/2022, CCSW 2020).
- Led an independently funded research project on privacy-friendly pattern matching; supervised 4 MSc theses.

Research Intern (2 summers) · Microsoft Research, Cryptography & Privacy group Jun–Sep 2018, Jun–Sep 2019
Redmond, WA, USA

- Implemented the **CKKS approximate-arithmetic FHE scheme in Microsoft SEAL** (C++), one of the most widely used open-source homomorphic encryption libraries; SEAL powers the Password Monitor in the Microsoft Edge browser.
- Co-designed a new somewhat-homomorphic encryption scheme with reduced memory overhead (IMA CC 2021).

Earlier: Postgraduate Researcher, IKBFU, Kaliningrad, Russia (2013–2015), C++ Programmer, Mariaglorum (2012–2014)

EDUCATION

Ph.D. in Engineering Science · KU Leuven, Belgium 2015 – 2019
Thesis: "Optimisations of fully homomorphic encryption" — advisors Prof. Bart Preneel and Prof. Frederik Vercauteren

Diploma in Mathematics, summa cum laude · IKBFU, Kaliningrad 2007 – 2013
Thesis: "Quantum security of the McEliece public-key cryptosystem" · DAAD Leonhard Euler Scholarship

SELECTED PUBLICATIONS (14 PEER-REVIEWED IN TOTAL)

- On Polynomial Functions Modulo p^e and Faster Bootstrapping for Homomorphic Encryption — **Eurocrypt 2023**
- FINAL: Faster FHE Instantiated with NTRU and LWE — **Asiacrypt 2022**
- Labeled PSI from Homomorphic Encryption with Reduced Computation and Communication — **ACM CCS 2021**
- Faster Homomorphic Comparison Operations for BGV and BFV — **PETS 2021**
- Homomorphic SIM^{2}D Operations: Single Instruction Much More Data — **Eurocrypt 2018**
- Faster Homomorphic Function Evaluation Using Non-Integral Base Encoding — **CHES 2017**
- Provably Weak Instances of Ring-LWE Revisited — **Eurocrypt 2016**

COMMUNITY

- Program committee: WAHC 2022, 2024, 2026.
- Reviewer: Eurocrypt, Crypto, Asiacrypt, CHES, PKC, USENIX Security, CT-RSA, ACNS; Journal of Cryptology, IEEE TIFS, Designs, Codes and Cryptography.
- Invited and conference talks at FHE.org, PETS, IMA CC, Mathcrypt, ANTS and the London Lattice Meeting; lecture on lattices in cryptography at the ANTS-XIV summer school.

References available on request.