Ilia Iliashenko

Contacts

iliailiashenko@gmail.com

Research interests

Privacy enhancing technologies, secure computation methods, fully homomorphic encryption, secure multi-party computation, zero-knowledge proofs

Contributions

I contributed to several software libraries implementing privacy-enhancing technologies. In particular,
- Microsoft SEAL (CKKS/HEAAN homomorphic encryption scheme, C++),
- FINAL (FINAL fully homomorphic encryption scheme, C++),
- Ciphercore (ABY3 secure multi-party computation protocol, Rust/Python).

Employment

Aug. 2021 - present	Research engineer Ciphermode Labs DBA Pyte, Remote
May 2019 – Aug. 2021	Postdoctoral researcher ESAT/COSIC, KU Leuven, Leuven, Belgium
Jun. 2019 – Sep. 2019, Jun. 2018 – Sep. 2018	Research intern Cryptography and Privacy Research group, Microsoft Research, Redmond, WA, USA
Sep. 2013 – Aug. 2015	Postgraduate researcher IKBFU, Kaliningrad, Russia
Aug. 2012 – Jun. 2014	C++ programmer Mariaglorum, Kaliningrad, Russia

Education

Aug. 2015 – May 2019	Ph.D. in Engineering Science *"Optmisations of fully homomorphic encryption"* Supervisors: Prof. Bart Preneel, Prof. Frederik Vercauteren ESAT, KU Leuven, Belgium
Sep. 2007 – Jan. 2013	Diploma in Mathematics (summa cum laude) *"Quantum security of the McEliece public-key* cryptosystem" Supervisor: Dr. Sergey Aleshnikov IKBFU, Kaliningrad, Russia

Publications

R. Geelen, I. Iliashenko, Jiayi Kang and F. Vercauteren,
On Polynomial Functions Modulo p^e and Faster Bootstrapping for Homomorphic Encryption,
Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part III, volume 14006 of

Lecture Notes in Computer Science, C. Hazay and M. Stam (eds.), pp. 257-286, Springer-Verlag, 2023

C. Bonte, I. Iliashenko, J. Park, H. V. L. Pereira and N. P. Smart,
FINAL: Faster FHE Instantiated with NTRU and LWE,
Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part II, volume 13792 of Lecture Notes in Computer Science, S. Agrawal and D. Lin (eds.), pp. 188-215, Springer-Verlag, 2022.

I. Iliashenko, M. Izabachène, A. Mertens and H. V. L. Pereira,
Homomorphically counting elements with the same property,
Proceedings on Privacy Enhancing Technologies (PETS), Volume 2022 (2022): Issue 4, pp. 670-683, PoPETs, 2022

H. Chen, I. Iliashenko and K. Laine,
When HEAAN Meets FV: a New Somewhat Homomorphic Encryption with Reduced Memory Overhead,
Proceedings of the 18th IMA International Conference on Cryptography and Coding (IMA CC), pp. 265-285, Springer-Verlag, 2021

I. Iliashenko, C. Nègre and V. Zucca,
Integer Functions Suitable for Homomorphic Encryption over Finite Fields,
Proceedings of the 9th on Workshop on Encrypted Computing & Applied Homomorphic Cryptography (WAHC), pp. 1-10, ACM, 2021

K. Cong, R. Cruz Moreno, M. B. da Gama, W. Dai,
I. Iliashenko, K. Laine and M. Rosenberg,
Labeled PSI from Homomorphic Encryption with Reduced Computation and Communication,
Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS), pp. 1135-1150, ACM, 2021.

I. Iliashenko and V. Zucca,
Faster Homomorphic Comparison Operations for BGV and BFV,
Proceedings on Privacy Enhancing Technologies (PETS), Volume 2021 (2021): Issue 3 (July 2021), pp. 246-264, Sciendo, 2021.

C. Bonte and I. Iliashenko,
Homomorphic String Search with Constant Multiplicative Depth,
Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop (CCSW), pp. 105-117, ACM, 2020.

C. Bootland, W. Castryck, I. Iliashenko and F. Vercauteren,
Efficiently Processing Complex-Valued Data in Homomorphic Encryption,
Journal of Mathematical Cryptology 14 (1, Special Issue Mathcrypt 2018): 55-65, 2020.

W. Castryck, I. Iliashenko and F. Vercauteren,
Homomorphic SIM2D Operations: Single Instruction Much More Data,
Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I, volume 10820 of Lecture Notes in Computer Science, J. Nielsen and V. Rijmen (eds.), pp. 338-359, Springer-Verlag, 2018.

C. Bonte, C. Bootland, J. W. Bos, W. Castryck, I. Iliashenko, and F. Vercauteren,

Faster Homomorphic Function Evaluation Using Non-Integral Base Encoding,
In Cryptographic Hardware and Embedded Systems – CHES 2017 – 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings, volume 10529 of Lecture Notes in Computer Science, W. Fischer, and Naofumi Homma (eds.), pp. 579-600, Springer-Verlag, 2017.

J. W. Bos, W. Castryck, I. Iliashenko, and F. Vercauteren,
Privacy-friendly Forecasting for the Smart Grid Using Homomorphic Encryption and the Group Method of Data Handling,
In Progress in Cryptology - AFRICACRYPT 2017 - 9th International Conference on Cryptology in Africa, Dakar, Senegal, May 24-26, 2017, Proceedings, volume 10239 of Lecture Notes in Computer Science, M. Joye, and A. Nitaj (eds.), pp. 184-201, Springer-Verlag, 2017.

W. Castryck, I. Iliashenko, and F. Vercauteren,
On Error Distributions in Ring-based LWE,
LMS Journal of Computation and Mathematics 19 (Special Issue ANTS-XII), pp. 130-145, 2016.

W. Castryck, I. Iliashenko, and F. Vercauteren,
Provably Weak Instances of Ring-LWE Revisited,
In Advances in Cryptology – EUROCRYPT 2016 – 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I, volume 9665 of Lecture Notes in Computer Science, J. Coron, and M. Fischlin (eds.), pp. 147-167, Springer-Verlag, 2016.

Talks/Demos

Dec. 2021	When HEAAN Meets FV: a New Somewhat Homomorphic Encryption with Reduced Memory Overhead IMA CC 2021
Oct. 2021	Private set intersection via somewhat homomorphic encryption FHE.org meetup
Aug. 2021	Private set intersection via somewhat homomorphic encryption IKBFU, Kaliningrad, Russia
Jul. 2021	Faster homomorphic comparison operations for BGV and BFV PETS 2021
Jun. 2020	Lattices in cryptography ANTS-XIV summer school
Dec. 2019	On error distributions in ring-based LWE IKBFU, Kaliningrad, Russia
Nov. 2019	Sparse-secret Ring-LWE in FHE: Is It Really Needed? London Lattice meeting Royal Holloway University, Egham, UK
Aug. 2019	Noise-free FHE Crypto Lunch meeting Microsoft Research, Redmond, WA, USA
Aug. 2018	Efficiently processing complex-valued data

	in homomorphic encryption Mathcrypt 2018 Santa Barbara, CA, USA
May 2018	Secure smart meter demo Imec Technology Forum Antwerp, Belgium
May 2018	Secure smart meter demo HEAT project final review meeting Leuven, Belgium
Jul. 2018	w-NIBNAF for faster evaluation in SHE schemes IKBFU, Kaliningrad, Russia
May 2017	Privacy-friendly forecasting for the smart grid using homomorphic encryption AFRICACRYPT 2018 Dakar, Senegal
Aug. 2016	On error distributions in ring-based LWE ANTS-XII Kaiserslautern, Germany
Nov. 2016	Privacy-friendly forecasting for the smart grid using homomorphic encryption Colloquium Coding Theory and Cryptography Brussels, Belgium

Research stays

Nov. 2019	Information Security Group, Royal Holloway University, UK Topic: noise analysis of FHE schemes
Jun. 2019 – Sep. 2019, Jun. 2018 – Sep. 2018	Cryptography and Privacy Research group, Microsoft Research, Redmond, WA, USA Topic: optimization and implementation of the HEAAN HE scheme in the SEAL library
Feb. 2012	Institute of Computer Science, University of Leipzig, Germany Topic: cryptography based on AG-codes
Oct. 2011 – Jan. 2012	Institute of Mathematics and Computer Science, University of Greifswald, Germany Topic: applied mathematics

Teaching

Spring 2019, Spring 2018	Advanced Crypto Teaching assistant Practice session on quantum algorithms KU Leuven, Belgium
Fall 2014	Geometric codes Lecturer IKBFU, Kaliningrad, Russia

Students

2017 – 2018	Robbe Motmans Master of Science in Mathematics

"Analysis and simulations of Shor's algorithm"
Department of Mathematics, KU Leuven, Belgium

2020-2021 — Pieterjan Thijs
Master of Science in Mathematics
"Conversion algorithms between homomorphic encryption schemes"
Department of Mathematics, KU Leuven, Belgium

Jiayi Kang
Master of Science in Mathematics
"Efficient Homomorphic Encryption for Fixed Point Arithmetic"
Department of Mathematics, KU Leuven, Belgium

Helena Heerwegh
Master of Science in Mathematics
"Groups of Unknown Order"
Department of Mathematics, KU Leuven, Belgium

Wannes Manhaeve
Master of Science in Artificial Intelligence
"Training least squares support vector machines with homomorphic encryption"
Department of Electrical Engineering, KU Leuven, Belgium

Grants

Oct. 2019 – Aug. 2021 — FWO junior postdoctoral fellowship
Project: Analysis of privacy-friendly pattern matching using homomorphic encryption

Feb. 2012 — DAAD - Leonhard Euler Scholarship

Seminars

Aug. 2015 – present — COSIC seminar
Public-key group meeting
Computation on Encrypted Data (CoED) meeting
ESAT, KU Leuven, Belgium

Jun. 2019 – Aug. 2019
Jun. 2018 – Aug. 2018 — Crypto Lunch meetings
Cryptography and Privacy Research group, Microsoft Research, Redmond, USA

Reviews

Conferences — CHES 2016
Asiacrypt 2016, 2017, 2019, 2021, 2022
SAC 2016
ArcticCrypt 2016
Eurocrypt 2017-2021
Crypto 2017, 2018, 2020, 2021
PKC 2018-2020, 2022
ACNS 2018, 2020
CT-RSA 2020, 2021
USENIX 2021

Workshops — Waifi 2016
WIFS 2017
WAHC 2022 (PC member)
WAHC 2024 (PC member)

Journals — International Journal of Information Security

Journal of Cryptology
IEEE Transactions on Information Forensics and Security
Designs, Codes and Cryptography

Skills

Human languages	Russian (native) English (full proficiency) Dutch (intermediate) German (elementary)
Programming languages	C++, Python, Rust, Protobuf SageMath, Magma, R LaTeX, HTML/CSS
IDEs	Microsoft Visual Studio, Sublime Text

References

Prof. Frederik Vercauteren
ESAT/COSIC, KU Leuven
Kasteelpark Arenberg 10
3001, Leuven, Belgium
+32 16 37 60 80
frederik.vercauteren@kuleuven.be

Dr. Kim Laine
Microsoft Research
14820 NE 36th Street, Building 99
98052, Redmond, Washington, USA
kim.laine@microsoft.com

Dr. Ilya Razensteyn
Ciphermode Labs Inc.
4470 W Sunset Blvd Suite 107 PMB 92370
Los Angeles, CA 90027
ilya.razenshteyn@ciphermode.tech

Last update: 3 Sep. 2024