ELIAS SUVANTO

Website: suvan.to & Email: elias.suvanto@uni.lu

EDUCATION

University of Luxembourg | **PhD supervised by Jean-Sébastien Coron** — Dec 2023 - Dec 2026

ENS de Lyon | **BSc and MSc in Computer Science** | **Lyon, France** — Sep 2019 - Sep 2023

Université Claude Bernard Lyon 1 | **BSc in Mathematics** | **Lyon, France** — Sep 2019 - Sep 2020

EXPERIENCE

University of Luxembourg | **Doctoral Researcher** | **Applied Crypto Group** — Sep 2025 - present

Extending discrete CKKS to support in-slot CRT arithmetic, finite-field arithmetic, and SHA3 under FHE [5-7]. Preparing an implementation of my thesis work in Poulpy.

FHElab & CryptoLab Inc. | **Joint PhD Student & Research Engineer** | **Lyon, France / Seoul, South Korea** | **advised by Damien Stehlé** — Sep 2023 - May 2025

- Recovered secret keys against exact FHE schemes [2] for parameter sets with high decryption-failure probability.
- Implemented functional bootstrapping for small integers [3] in the GPU-accelerated HEaaN library: 3.75 ms amortized time for 8-bit integer inputs on a single CPU thread.
- Designed a new high-precision CKKS bootstrapping [4], improving throughput by 2.4× over META-BTS. Delivered a baseline branch for engineering integration to production.

Seoul National University, IMDARC | **Research Intern** | **Seoul, South Korea** — May - Jul 2023

Investigated discrete-CKKS within Jung Hee Cheon's academic team.

CryptoLab Inc. | **Research Intern** | **Seoul, South Korea** — Aug - Dec 2022

Studied possible mitigations for IND-CPA^D security in CKKS.

Lund University | **Research Intern** | **Lund, Sweden** — Feb - Jul 2022

Cryptanalysis of CKKS [1].

University of Luxembourg | **Research Intern** | **Luxembourg** — May - Jul 2021

Side-channel attacks on the lattice-based signature scheme GLP, a precursor of Dilithium.

PUBLICATIONS

[1] Key Recovery Attacks on Approximate Homomorphic Encryption with Non-Worst-Case Noise Flooding Countermeasures, Q. Guo, D. Nabokov, E. Suvanto, T. Johansson, **USENIX Security 2024.**
[2] Attack Against the IND-CPA^D Security of Exact FHE Schemes, J. H. Cheon, H. Choe, A. Passelègue, D. Stehlé, E. Suvanto, **ACM CCS 2024.**
[3] Bootstrapping Small Integers with CKKS, Y. Bae, J. Kim, D. Stehlé, E. Suvanto, **ASIACRYPT 2024.**
[4] Leveraging Discrete CKKS to Bootstrap in High Precision, H. Choe, J. Kim, D. Stehlé, E. Suvanto, **ACM CCS 2025.**

PREPRINTS

[5] Character Block Encodings for Discrete CKKS: Single-Level LUTs and Low-Depth Arithmetic, J. Dumezy, E. Suvanto, (under submission).
[6] Finite-Field Arithmetic in CKKS, T. Seuré, E. Suvanto, (soon on ePrint).

POSTERS

[7] Faster Homomorphic Evaluation of SHA3, Tim Seuré, E. Suvanto, **FHE.org 2026**, Taipei

SKILLS

Programming: C++/C, Python, Go, Rust, SageMath
FHE frameworks: HEaaN, OpenFHE, TFHE-rs, Lattigo

LANGUAGES

English: **fluent** (Cambridge C1 Advanced)
French: **native** | Korean: **basic** (learning)

AWARDS

First prize, Korean National Cryptography Contest 2024 (NSRI, NIS) for the vulnerabilities discovered in [2].

TALKS

- Presented [3] at **ASIACRYPT 2024**, Kolkata and [2] at **CCS 2024**, Salt Lake City.

REVIEWS

- Artifact Evaluation Committee member for **USENIX Security 2025**
- Additional reviewer for **EUROCRYPT 2025, 2026** and **ASIACRYPT 2025.**