

JULES DUMEZY

jules.dumezy@gmail.com † jdumezy.com

Education

- Université Paris-Saclay** Ph.D Candidate in Mathematic and Computer Science **2024 – present**
Efficient computation for Fully Homomorphic Encryption
- Ecole Centrale de Lille** M.Sc in Engineering degree **2020 – 2024**
Speciality: Embedded and Cyberphysics Systems & International Project Management
- Lycée Saint-Louis Paris VI – MPSI/MP** **2018 – 2020**
Undergraduate studies in math and physics to prepare for competitive entry exams to engineering schools

Professional Experience

- CEA-List** *Ph.D Candidate* **Oct 2024 – present**
• Research on FHE *Université Paris-Saclay*
- iHub** *Research Intern* **Apr 2024 – Aug 2024**
↔ Prof. Bart Jacobs *Radboud University*
- Internship as part of the PubHubs social network project: research into the possibility of using a post-quantum cryptography compatible with PubHubs' identity management system
- CRISAL** *Research Intern* **Oct 2023 – Mar 2024**
• Homomorphic encryption on embedded systems and robotics using ROS
- CSTB** *Research Intern* **Jan 2021 – Feb 2021**
• Validation of a computational engine for predicting noise exposure from airborne sources in an urban environment

Publications

- [1] J. Dumezy, A. Alexandru, Y. Polyakov, P.-E. Clet, O. Chakraborty, and A. Boudguiga, "Evaluating larger lookup tables using CKKS." Cryptology ePrint Archive, Paper 2025/1301, 2025.
- [2] J. Adamek, A. Aikata, A. A. Badawi, A. Alexandru, A. Arakelov, P. Binfet, V. Correa, J. Dumezy, S. Gomenyuk, V. Kononova, D. Lekomtsev, V. Maloney, C.-H. Nguyen, Y. Polyakov, D. Pinykh, H. Shaul, M. S. Darup, D. Teichrib, D. Tronin, and G. Arakelov, "FHERMA cookbook: FHE components for privacy-preserving applications." Cryptology ePrint Archive, Paper 2025/1302, 2025.

Awards

- 1st place at FHERMA's LUT challenge** **2024**
Best solution for the LUT evaluation challenge using BFV on the FHERMA platform

Software libraries & Prototypes

- SEC-CKKS** <https://github.com/jdumezy/sec-ckks> **2025**
• Implementation of CKKS functional bootstrapping using OpenFHE
- SEAL x ROS** <https://github.com/jdumezy/seal-x-ros> **2024**
• ROS2 package to use the SEAL homomorphic encryption library with topics

Editorial & Review activity

- Reviewer for Conferences**
Asiacrypt 25

Dissemination

- Article** Article presenting post-quantum cryptography and FHE in "La Revue de l'Ingénieur"

Languages

- French** Native
English Fluent, 990/990 TOEIC
German C1, Allgemeine Hochschulreife 1.0
Japanese A2