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 & Internationl 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

CRIStAL *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. Adamek, A. Aikata, A. Al Badawi, A. Alexandru, A. Arakelov, G. Arakelov, P. Binfet, V. Correa, J. Dumezy, S. Gomenyuk, V. Kononova, D. Lekomtsev, V. Maloney, C.-H. Nguyen, Y. Polyakov, D. Pianykh, H. Shaul, M. S. Darup, D. Teichrib, and D. Tronin, "Fherma cookbook: Fhe components for privacy-preserving applications," in *Proceedings of the 13th Workshop on Encrypted Computing & Applied Homomorphic Computing*, WAHC '25, (New York, NY, USA), p. 68–76, Association for Computing Machinery, 2025.

[2] J. Dumezy, A. Alexandru, Y. Polyakov, P.-E. Clet, O. Chakraborty, and A. Boudguiga, "Evaluating larger lookup tables using CKKS." To appear in CHES '26, 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 and Subreviewer 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