Nicolas Bon

Cryptography PhD Student & Engineer

nicolas.bon38@gmail.com
https://www.nicolasbon.com
nicolasbon38
nicolas-bon-crypt

ABOUT ME

I am a PhD student at CryptoExperts and part of the CASCADE team of Ecole Normale Supérieure de Paris, under the supervision of Sonia Belaïd, David Pointcheval and Matthieu Rivain.

My main research topic is Fully Homomorphic Encryption, specifically the development and implementation of fast homomorphic operations. I also have a broader interest for anything cryptography-related and more generally in cybersecurity and privacy-preserving technologies.

Besides my research activities, I also take part in various engineering missions within CryptoExperts, including development, security audit and consulting. I also serve as a teaching assistant at the university.

I enjoy programming at all levels and have a strong passion for mathematics, particularly number theory and probabilities. Additionally, I am keen on writing and engaging in scientific communication.

WORK EXPERIENCE

CryptoExperts — CURRENT, FROM OCT 2022
PhD Student

I am the author of several contributions improving the performances of FHE schemes for several applications. I implemented all these constructions in a library written in Rust and gave several presentations in international conferences and seminars

CryptoExperts — CURRENT, FROM OCT 2022
Cryptography Engineer

While completing my PhD, CryptoExperts gave me the opportunity of widening my skill ranges by working on various missions, including development of post-quantum cryptographic libraries, audit of various systems relying on cryptography (random number generators, Android apps), and consulting different companies about cryptography.

CryptoExperts — FEB. TO AUG. 2022
Engineering Intern

This internship was my first step into the cryptography world: I've conceived and implemented an encrypted neural network for privacy-preserving document processing.

L.I.G. Grenoble — SUMMER 2021
Research Intern

In this summer job in an academic lab, I worked on simulations of voting systems and algorithms of graph theory applied to gerrymandering.

Gigs — BEFORE 2022

During my studies, I've done multiple gig jobs such as grape harvesting, private tutoring, I.T. support and various farming tasks.

TEACHING EXPERIENCE

2024	**Java Programming** (1 semester, 2nd y. Bachelor)
2023-24	**Cryptography** (3 semesters, 3rd y. Bachelor, 1st y. Master)

EDUCATION

2022 –	**PhD in Cryptography** Ecole Normale Supérieure & CryptoExperts
2019 – 22	**Master's Degree in CS and Applied Maths** HIGHEST HONORS *Grenoble INP - ENSIMAG*
2021	**Erasmus Exchange** *NTNU Trondheim (Norway)*
2017 – 19	**Preparatory Classes for "Grandes Ecoles"** *Lycée la Martinière Montplaisir*

PUBLICATIONS

- **Bon**, Pointcheval, Rivain (2024). Optimized Homomorphic Evaluation of Boolean Functions. *Transactions on Cryptographic Hardware and Embedded Systems*, *Vol 3*, 302-341.
- Baudrin, Belaïd, **Bon** et al.(2024). `Transistor`: a TFHE-friendly Stream Cipher. *On-going Submission*.
- Belaïd, **Bon**, Boudguiga et al.(2025) Further Improvements in AES Execution over TFHE: Towards Breaking the 1 sec Barrier *Ongoing Submission*.
- Belaïd, **Bon**, Pointcheval, Rivain (2025) ORPHEUS: Efficient Machine-Tailored Parameter Optimization for FHE *Ongoing Submission*.

AWARDS

2019	**Fondation Georges Besse Scholarship** *Grant for top students from modest background*

TECHNICAL SKILLS

PROGRAMMING	**Rust, C, Python**, Java
TOOLS	Git, Linux, LaTeX

COMMUNICATION SKILLS

CONFERENCES	Presentation at CHES 2024 and in various seminars
POSTERS	Poster at FHE.org conference 2024
VULGARIZATION	2 articles about Cryptography in MISC

HOBBIES

I like to tinker with computers, cars and bicycles. I'm the co-founder of an association of restoration of old cars. I'm also into swimming, cycling (road and cross-country) and reading.