Nicolas Bon

Cryptography Researcher & Engineer

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

ABOUT ME

I am a cryptography researcher and engineer at CryptoExperts. My main research topic is Fully Homomorphic Encryption but I have a broader interest for anything cryptography-related and more generally in cybersecurity and privacy-preserving technologies. I am also working on various within CryptoExperts, including development, security audit and consulting. Before that, I was a PhD student in Ecole Normale Supérieure de Paris (CASCADE team) , under the supervision of Sonia Belaïd, David Pointcheval and Matthieu Rivain.

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 NOV 2025
Cryptography Engineer

My missions include the development of cryptography-related software, security audits, and consulting different companies about cryptography.

CryptoExperts — OCT 2022 TO NOV 2025
PhD Student

I am the author of several contributions improving the performances of FHE schemes for different use-cases, that I implemented and tested in a library written in Rust. I presented these works in major international conferences of the field (see bibliography). Apart for this reseach activities, I did various activities for CryptoExperts, such as consulting and development

CryptoExperts — FEB. TO AUG. 2022
Engineering Intern

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

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

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 – 2025 **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.
- Belaïd, **Bon**, Boudguiga et al.(2025) Further Improvements in AES Execution over TFHE *IACR Communications in Cryptology*, *Vol.2, no 1.*,
- Baudrin, Belaïd, **Bon** et al.(2024). Transistor: a TFHE-friendly Stream Cipher. *Accepted at Crypto 2025.*
- **Bon**, Chevalier, Lebrun, Martinelli (2025) SUMAC: an Efficient Administrated-CGKA Using Multicast Key Agreement *Ongoing Submission.*
- Belaid, **Bon**, Rivain (2025) Decomposition of Large Look-Up Tables for Fast Homomorphic Evaluation *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, CRYPTO 2025 and in various seminars
VULGARIZATION 2 articles about Cryptography in MISC