# YOUSSEF EL HOUSNI

(+33)662968238 ⋄ youssef.housni21@gmail.com
1 Rue de l'aigle, 92250 La Garenne-colombes, France

yelhousni.github.com

## WORK EXPERIENCE

**EY Blockchain, Paris** August 2018 - present
*Cryptography Engineer*

· Applied cryptography research and implementation (Zero-knowledge proofs, elliptic curves, bilinear groups...).
· Blockchain development with focus on privacy.

**Secure-IC, Rennes** August 2018 - present
*Cryptography Engineer*

· Elliptic curve cryptography: Theory, implementations and countermeasures against side-channel and fault injection attacks.
· Pairing-based cryptography (id-based encryption).
· Post-quantum cryptography (Isogenies-based and code-based cryptography i.e. SIKE, DAGS) (*submitted a paper with DAGS team, a NIST PQC candidate*)
· Mathematical modeling of a hardware TRNG (True Random Number Generator) (*a patent pending and a published paper*) and a hardware PUF.
· Video steganography (up to UHD@60fps 10-bit) on embedded devices (Hisilicon Hi2798CV200 set-top box).

## EDUCATION

**Ecole Polytechnique, Paris** November 2019 - Present
PhD in cryptography
project-team GRACE under LIX and INRIA Saclay
supervisors: Daniel Augot and François Morain

**ENSEIRB-MATMECA, Bordeaux** September 2013 - September 2016
MEng in Electronics.
majors: Image and signal processing

## TECHNICAL AND SOFT SKILLS

**Software** C, C++, Python, SageMath, Bash, Latex
**Languages** English, French, Arabic

## PUBLICATIONS

"On the performance and security of $GF(2^N)$ computation for small $N$"
(joint with Sylvain Guilley, Edoardo Persichetti et al.)
Published in MDPI Cryptography 2018 Journal, Special Issue "Code-based Cryptography". (DOI)

"Random numbers generation: Tests and attacks"
(joint with Sylvain Guilley)
Published in 2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC). (DOI)

## PRE-PRINTS

"Making randomness tests flexible"
(joint with Sylvain Guilley)

## PATENTS

*Pending*: "Device and method for testing a sequence generated by a random number generator"
(joint with Florent Lozac'h)
Secure-IC S.A.S.

## EXTRA-CIRRUCULAR

Co-Organizer of "ZK-PAR" - A technical meetup held in Paris focussing on privacy-preserving technology in blockchains.

Played in the moroccan regional championship with Tetouan local team from 2000 to 2011.