YOUSSEF EL HOUSNI

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

`https://yelhousni.github.io`

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 October 2016 - August 2018
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

[1] Danger, Jean-Luc and **El Housni, Youssef** and Facon, Adrien and Gueye, Cheikh T. and Guilley, Sylvain and Herbel, Sylvie and Ndiaye, Ousmane and Persichetti, Edoardo and Schaub, Alexander, *"On the Performance and Security of Multiplication in* $GF(2^N)$*"*, Cryptography Journal, Volume 2, 2018. DOI: `10.3390/cryptography2030025`

[2] Guilley, Sylvain and **El Housni, Youssef** *"Random Numbers Generation: Tests and Attacks"*, 2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC) pages: 49-54 DOI: `10.1109/FDTC.2018.00016`

PRE-PRINTS

[1] Guilley, Sylvain and **El Housni, Youssef** *"Making randomness tests flexible"*

PATENTS

(Pending) "Device and method for testing a sequence generated by a random number generator"
El Housni, Youssef and Lozac'h, Florent
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.