YOUSSEF EL HOUSNI

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

yelhousni.github.io

EDUCATION

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

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

BEng at **ENSEIRB-MATMECA, Bordeaux** 2014
BEng in engineering sciences.

WORK EXPERIENCE

EY Blockchain, Paris August 2018 - present
Cryptography Engineer

- Applied cryptography research and implementation (Zero-knowledge proofs, elliptic curves and pairing-based cryptography).
- 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) (*published a journal paper [2] with DAGS team, a NIST PQC candidate*)
- Mathematical modeling of a hardware TRNG (True Random Number Generator) (*a pending patent [5] and a conference paper [3]*) and a hardware PUF.
- Video steganography (up to UHD@60fps 10-bit) on embedded devices (Hisilicon Hi2798CV200 set-top box).

TECHNICAL AND SOFT SKILLS

Software C, C++, Python, SageMath, Bash, Latex
Languages English (fluent), French (mother tongue), Arabic (mother tongue)

PUBLICATIONS

[1] **Youssef El Housni** and Guillevic Aurore, *"Optimized and secure pairing-friendly elliptic curves suitable for one layer proof composition"*, IACR Cryptology ePrint Archive 2020. url: ia.cr/2020/351

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

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

PATENTS

[5] **Youssef El Housni** and Florent Lozac'h *"Device and method for testing a sequence generated by a random number generator"* Patent pending. 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 football team from 2000 to 2011.