Youssef El Housni

Cryptographer

1 Rue de l'aigle
92250 La Garenne-Colombes, France
+33 (0) 662968238
youssef.housni21@gmail.com
medium.com/@youssef.housni21
`crypto.stackexchange.com/users/63311`

"Imagination is more important than knowledge."
- Albert Einstein

Experience

08/2018– present **R&D Engineer**, *EY Wavespace Lab*, Paris.
Lead cryptographer in the Blockchain team.
- Zero-knowledge proofs (ZKP) for the Blockchain (ZK-SNARks, ZK-STARKS, Bulletproofs).
- Secure multiparty computation (SMPC) for the Blockchain (Enigma, HAWK).
- Implementing proxy re-encryption and attribute-based encryption.
- Designing a pairing-friendly elliptic curve in Edwards form resistant to exTNFS (128-bit security).

10/2016– 08/2018 **R&D Engineer**, *Secure-IC*, Rennes.
- Elliptic curve cryptography: Theory, implementations and countermeasures against side-channel and fault injection attacks.
- Pairing-based cryptography (id-based encryption, BLS signatures).
- 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 (Phylically Unclonable Function) (*Contribution to appear in ISO 20807 part 2*).
- Video steganography (up to UHD@60fps 10-bit) on embedded devices (Hisilicon Hi2798CV200 set-top box).

03/2016– 09/2016 **R&D Intern**, *Orange Labs*, Rennes.
Developed in C language a state-of-the-art speaker recognition system based on machine learning techniques (*ranked second best internship*)

06/2015– 09/2015 **R&D Intern**, *Kansai University*, Osaka, Japan.
Developed in Matlab an active noise control system for IRM machines under the supervision of professor Yoshinobu Kajikawa.

Education

2013–2016 **ENSEIRB-MATMECA School of engineering**, *Bordeaux, France*.
Master of science in Signal Processing and Applied Mathematics.

2011–2013 **Moulay Al-Hassan**, *Tangier, Morocco*.
Preparatory classes for the French national entrance exam for admission to the 'Grandes Ecoles' Science and Engineering schools.

Computer skills

Programming and software: C, Python, Bash, SageMath, Matlab, LaTeX.

Operating system: Linux, MacOS, Windows.

Languages

English (fluent), French/Arabic (bilingual), Spanish (intermediate).

Patents

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

Research Papers

Published: "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:10.3390/cryptography2030025

Published: "Random numbers generation: Tests and attacks"
(joint with Sylvain Guilley)
Published in 2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)
DOI:10.1109/FDTC.2018.00016

Pre-print: "Making randomness tests flexible"
(joint with Sylvain Guilley)

HAL Research documents

2018: "Introduction to the Mathematical Foundations of Elliptic Curve Cryptography"
HAL Id: hal-01914807
https://hal.archives-ouvertes.fr/hal-01914807

2018: "Edwards Curves"
HAL Id: hal-01942759
https://hal.archives-ouvertes.fr/hal-01942759

Interests

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

Mathematics: Finalist twice in the National Mathematical Olympiads.

Blogging: Write Medium blogs about cryptography https://medium.com/@youssef.housni21 and active on Cryptography StackExchange https://crypto.stackexchange.com/users/63311/youssef-el-housni