Youssef El Housni

8 Rue du Parc
35510 Cesson-Sévigné
France
+33 (0) 662968238
youssef.housni21@gmail.com
born in Morocco the 23^{rd}, February 1994

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

Education

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

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.

Experience

10/2016–present **R&D Engineer**, *Secure-IC*, Rennes.
- Elliptic curve cryptography: Theory and countermeasures.
- Post-quantum cryptography (Isogenies-based and code-based cryptography i.e. SIKE, DAGS) (*submitted a paper with DAGS team, a NIST PQC candidate*)
- Stochastic models of a hardware TRNG (True Random Number Generator) (*a patent pending and two sumbitted papers*) and a hardware PUF (Phylically Unclonable Function) (*Contribution to appear in ISO 20807 part 2*).
- Video steganography and steganalysis on embedded devices.

03/2016–09/2016 **R&D Intern**, *Orange Labs*, Rennes.
developed 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 an active noise control system for IRM machines under the supervision of professor Yoshinobu Kajikawa.

Computer skills

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

Operating system: Linux, MacOS, Windows.

Versioning: svn, git.

Patents

Patent pending Embedded dynamic statistical tests for TRNGs (joint with Florent Lozac'h). Secure-IC S.A.S.

Submitted and working papers

accepted in FDTC 2018 Random numbers generation: Tests and attacks. (joint with Sylvain Guilley)

submitted to SSR 2018 Making randomness tests flexible. (joint with Sylvain Guilley)

submitted to the journal "Cryptography" On the performance and security of $GF(2^N)$ computation for small N. (joint with Sylvain Guilley, Adrien Facon, Jean-Luc Danger, Edoardo Persichetti, Cheikh Thiecoumba Gueye, Ousmane Ndiyae, Sylvie Herbel, and Alexander Schaub)

Interests

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

Mathematics Participated twice in the National Mathematical Olympiads.