

Louiso Hugo

Nationality: French

Born: 01/07/2001 (Bergerac, France)

+33 6 51 88 54 40

hugolouiso@gmail.com



Master's graduate

Cryptography & Computer Security, University of Bordeaux, France

I'm looking for PhD/work opportunities in the area of Cryptology/Cybersecurity

Academic Background

- **Master Cryptology & Computer Security** (University of Bordeaux)
- Bachelor's degree in **Fundamental Mathematics** (University of Bordeaux)
- First year of the preparatory class for French engineering schools, with a focus on Mathematics, Physics, Computer Science and Engineering (MPSI) (Lycée Michel de Montaigne, Bordeaux)

Skills & Subjects Studied

Master subjects (Mathematics/Cryptography)

- **Cryptology** (15,3/20)
- **Arithmetic** (19,8/20)
 - Finite Fields, Polynomial Factorization, Linear codes, Cyclic code, Error-correcting codes
- **Information Theory** (17,5/20)
 - Entropy, Linear codes, Huffman codes, Discrete Channels, Channel Capacity
- **Symbolic Computation** (SageMath, Python) (17,2/20)
 - Divide and Conquer Algorithms, Factorization
- **Complexity Theory**
 - Automata, Grammars, Decidability, Complexity of Algorithmic Problems, Problem Reduction
- **Advanced Cryptology** (14/20)
 - Security Proofs, CPA security, Problem Reductions, Zero Knowledge Proofs, MPC, MPC-in-the-Head
- **Cryptanalysis** (16/20)
- **Post-Quantum Cryptography**
 - Lattices, Linear codes (RS Codes)
- **Arithmetic Algorithms**
 - Quantum Computing (qubits), Quantum circuits, Complexity, SageMath

Programming Knowledge

- | | |
|----------------|----------------------------------|
| • C/C++ | • SageMath |
| • Assembly x86 | • Bash + manipulating Unix shell |
| • Java | • LaTeX |
| • Python | • Learning Rust |

Master subjects (Computer Science)

- **Programming** (C, Java)
 - C: Generalized Sudoku Generator/Solver project
- **Operating Systems** (C++, 18/20)
- **Software Security**
- **Linux Network Administration** (16,5/20)
- **Smart Cards**
 - Communicating with Smart Cards, Side-Channel attacks, JavaCards

Master Supervised Research Works

- 1st Year:
 - Studying a "Schnorr threshold signature" (with DKG Protocol)
- 2nd Year:
 - Studying "Threshold Raccoon" (Threshold Lattice based signature)

Master Internship (5 months)

- Research internship in Cryptology at Universitat Politècnica de Catalunya (Barcelona), supervised by Javier Herranz Sotoca
- **Subject:** On the feasibility of Blind Signatures based on the MPC-in-the-head paradigm.
- Paper: eprint.iacr.org/2025/2097
- Solution implemented in C:
github.com/hlouiso/blind_MSS

Previous Work Experiences

- Diesel operator: Diesel injector repair technician
- Bartender

Hobbies

- Dancing: Salsa, Bachata, Rock
- Travels
 - Latin America, Spain, Vietnam, Japan

Languages

- French: Native Language
- English:
 - IELTS 7.5 (C1)
 - Master Internship in english, courses in english
- Spanish:
 - DELE B1
 - Master Internship in Barcelona