MSc/BSc projects in Cryptographic Engineering (1)

Random Number Generation

1. Unified hardware for all statistical tests including several new ones.
2. Studying and designing new kinds of TRNGs
3. Active attacks on RNGs.

Physically Unclonable Function (PUF)

1. Implementing PUFs in FPGAs
2. Studying machine learning attacks on them

Symmetric-key Cryptography

1. Efficient implementation of lightweight ciphers
2. Side-channel protection using masking

MSc/BSc projects in Cryptographic Engineering (2)

Public-key cryptography

Studying {Lattice, Code, Multivariate, Hash, Isogeny}-based schemes

1. Implementing public-key algorithms in hardware/microcontrollers/GPUs
2. Parameterizable hardware architecture
3. CAD tool development for design automation
4. Designing side-channel countermeasures

Fully Homomorphic encryption

1. Implementing computationally slow subroutines in FPGA or GPU
2. Developing applications for encrypted computing, e.g., machine learning.
3. Compilers for translating plaintext applications into homomorphic applications.

Topics of your own

1. You can propose your own project proposal.