UCL Université catholique de Louvain

# LELEC2760

*2014-2015*

# Secure electronic circuits and systems

| 5.0 credits | 30.0 h + 30.0 h | 2q |
|---|---|---|

| | |
|---|---|
| Teacher(s) : | Standaert François-Xavier ; |
| Language : | Anglais |
| Place of the course | Louvain-la-Neuve |
| Inline resources: | > http://perso.uclouvain.be/fstandae/ELEC2760/ |
| Main themes : | The course material includes the following topics:<br><br>--<br>black box assumptions for cryptographic algorithms and block ciphers,<br>--<br>mathematical cryptanalysis issues (statistical, algebraic, ...),<br>--<br>efficient implementation of cryptosystems,<br>--<br>physical attacks exploiting side-channels (e.g. power consumption, electromagnetic radiation, ...) or fault insertion,<br>--<br>random number generation, biometrics, physically unclonable functions, ...<br>--<br>integration of cryptographic hardware devices in secure systems and applications. |
| Aims : | In view of the LO frame of reference of the "Master Electrical Engineering", this course contributes to the development, acquisition and evaluation of the following learning outcomes :<br>Axis 1 (1.1, 1.2, 1.3), Axis 2 (2.2), Axis 3 (3.2), Axis 4 (4.3)<br>Axis 5 (5.3, 5.6)<br>At the end of the course, the student will be able to :<br>- Define the notion of secure cipher and argue about the difficulty of building efficient block ciphers that are provably secury in come formal model,<br>- Identify the properties that enable guaranteeing the "practical" security of a cipher, as well as the structural weaknesses to be avoided when designing such ciphers,<br>- Criticize the heuristic assumptions that are used in the (mathematical and physical) security analysis of a block cipher algorithm ofr its implementation,<br>- Apply cryptanalytic techniques (for example statistical, algebraic, combinatorial) and evaluate their impact for the security of an encryption algorithm,<br>- Describe and analyze the hardware architecture of a cryptographic implementation fulfilling a number of constraints provided in terms of cost or performance,<br>- Implement a cryptographic algorithm in a low-cost microcontroller,<br>- Evaluate the physical security of a cryptographic implementation against-side-channel attacks, taking advantage of physical information leakage (e.g. the power consumption of a microelectronic device performing some sensitive crypographic computations),<br>- Propose countermeasures and protection mechanisms against different physical attacks and justify their relevance in function of the adversarial context considered,<br>- Formalize physical properties that can be constructively exploited in cryptography (e.g. for random number generation, physically unclonable functions, IP protection),<br>- Enumerate the pros and cons of a cryptographic algorithm in function of its compromise between (mathematical, physical) security vs. implementation efficiency,<br>- Understand, summarize and present the results of a scientific paper related to the design and implementation of cryptograhic algorithms (e.g. such as published in conferenes like Eurocrypt, Crypto, Asiacrypt, CHES, FSA, ACM CCS, ...)<br><br>*The contribution of this Teaching Unit to the development and command of the skills and learning outcomes of the programme(s) can be accessed at the end of this sheet, in the section entitled "Programmes/courses offering this Teaching Unit".* |
| Evaluation methods : | Students will be evaluated individually, based on the following elements :<br>- Solving of implementation and cryptanalysis problems proposed during the exercise sessions that will be structured as several short-term projects.<br>- Written summary and/or oral presentation of a scientific paper.<br>- Answers to the questions at the beginning of each course, about preliminary readings.<br>- Written and/or oral examination about the previously listed course goals.<br>The respective importance of each element of the evaluation can vary in function of the years and will be specified at the first course of each year. Under individual demand of a student, the evaluation can be limited to the written work and session examination. |

| | |
|---|---|
| Teaching methods : | The course is organized in 14 lectures and 14 exercice sessions (2hours each). Every lecture starts with a preliminary reading to prepare. Students will be questioned about these lectures at the beginning of the course. Exercice sessions are dedicated to solving implementation and cryptanalysis problems, and are structured as different projetcts to carry out by small (2 or 3 student) groups. The last hour will be devoted to the oral presentation of scientific papers proposed by the students |
| Content : | Block ciphers (2 lectures), hardware implementations (1 lecture), software implementations (1 lecture), side-channel attacks (2 lectures), tamper resilience and fault attacks (1 lecture), physically unclonable functions (1 lecture), + open topics |
| Bibliography : | Lecture notes to complete and readings available on the course webpage |
| Other infos : | The course is open to any master student in electrical engineering, electromechanical engineering, computer science engineering and mathematical engineering. Prerequisites only include courses from the UCL bachelor in engineering (mathematics, statistics, ...). |
| Cycle and year of study : | > Master [120] in Electro-mechanical Engineering<br>> Master [120] in Electrical Engineering<br>> Master [120] in Mathematical Engineering<br>> Master [120] in Computer Science and Engineering |
| Faculty or entity in charge: | ELEC |