UCL Université catholique de Louvain

LELEC2760

2010-2011

Secure electronic circuits and systems

5.0 credits	30.0 h + 30.0 h	2q

Teacher(s) :	Quisquater Jean-Jacques ; Standaert François-Xavier ;
Language :	Anglais
Place of the course	Louvain-la-Neuve
Prerequisites :	Prerequisites and evaluation. This course is open to any student following a master in electrical engineering, electromechanical engineering, computer engineering and mathematical engineering. The only prerequisites are basic courses from the bachelor in engineering (mathematics, statistics, programming, ...). The evaluation combines a project work and a written examination More details : http://www.dice.ucl.ac.be/~fstandae/teaching.html
Main themes :	Identical to the contents of the course
Aims :	This course aims to analyze the different implementation issues that are raised by the design of cryptographic circuits and systems (hardware and software). It is part of the option in "Cryptography and Information Security", as a complementary to courses in cryptography (MAT2450) and computer system security (INGI2347). *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".*
Content :	Cryptography generally assumes the existence of certain basic primitives acting as perfect black boxes in order to prove the security of advanced functionalities (identification, signature, voting, ...).& bsp; On the other hand, the more general field of information security exploits cryptographic protocols and their implementations in order to secure any computer-based application such as e-mails, Internet, payment systems, ...& bsp; And these applications also imply different constraints on the & uot;efficiency& uot; of the cryptographic implementations.& bsp; This course on secure electronic circuits and systems studies the resulting tradeoff between security and performance.& bsp; It discusses how to select algorithms and implementations that satisfy application constraints from these two points of view.& bsp; Additionally, a significant attention will be paid in showing that implementation issues are not only related to performances, but also to the so-called physical security of cryptographic devices.& bsp; That is, adversaries against cryptographic systems can sometimes take advantage of alternative information channels (e.g. the time or energy need to perform a computation) in order to recover secret data.& bsp; Such problems are essential for the deployment of small embedded devices such as smart cards, RFIDs, ... Contents : - black box assumptions for cryptographic algorithms, - efficient implementation of cryptosystems, - mathematical cryptanalysis issues (statistical, algebraic, ...) - physical attacks exploiting side-channels (e.g. power assumption, electromagnetic radiation, ...) or fault insertion, - random number generation, biometrics and physically unclonable functions, - integration of cryptographic hardware devices in secure systems and applications, - ...
Other infos :	Prerequisites and evaluation.& bsp; This course is open to any student following a master in electrical engineering, electromechanical engineering, computer engineering and mathematical engineering.& bsp; The only prerequisites are basic courses from the bachelor in engineering (mathematics, statistics, programming, ...).& bsp; The evaluation combines a project work and a written examination More details : http://www.dice.ucl.ac.be/~fstandaert/teaching
Cycle and year of study :	> Master [120] in Electrical Engineering > Master [120] in Electro-mechanical Engineering > Master [120] in Computer Science and Engineering > Master [120] in Mathematical Engineering

Faculty or entity in charge:	ELEC