UCL Université catholique de Louvain

LELEC2760

2012-2013

Secure electronic circuits and systems

5.0 crédits	30.0 h + 30.0 h	2q

Enseignants:	Standaert François-Xavier ;
Langue d'enseignement:	Anglais
Lieu du cours	Louvain-la-Neuve
Préalables :	Prérequis et évaluation. Le cours est ouvert à tout étudiant suivant un master en ingéniérie électrique, électromécanique, informatique ou mathématiques appliquées. Les seuls prérequis sont les cours de base du BAC en sciences de l'ingénieur (mathématiques, statistique, programmation, ...). L'évaluation combine un projet et un examen écrit Plus de détails : http://perso.uclouvain.be/fstandae/teaching.html
Thèmes abordés :	Voir descriptif
Acquis d'apprentissage	Ce cours a pour but d'analyser les différents problèmes de mise-en-oeuvre qui se posent lors de la conception de circuits et systèmes sécurisés (hardware et software). Il fait partie de l'option "Cryptographie et Sécurité de l'Information" et est un complément aux cours de cryptographie (MAT2450) et de sécurité des systèmes informatiques (INGI2347) *La contribution de cette UE au développement et à la maîtrise des compétences et acquis du (des) programme(s) est accessible à la fin de cette fiche, dans la partie « Programmes/formations proposant cette unité d'enseignement (UE) ».*
Contenu :	La cryptographie fait g& acute;n& acute;ralement l'hypoth& grave;se que certaines primitives math& acute;matiques id& acute;ales existent, afin de prouver la s& acute;curit& acute; de fonctionnalit& acute;s avanc& acute;es (identification, signature, vote, ...).& bsp; Et le domaine plus g& acute;n& acute;ral de la s& acute;curit& acute; informatique utilise ensuite des protocoles cryptographiques afin de s& acute;curiser des applications concr& grave;tes telles l'e-mail, les syst& grave;mes de paiement en ligne, ...& bsp; Ces applications impliquent des contraintes en termes d'efficacit& acute; des mises en oeuvre cryptographiques.& bsp; Le cours de circuits et syst& grave;mes s& acute;curis& acute;s & acute;& acute;tudie le compromis entre s& acute;curit& acute; et performance qui r& acute;sulte de ces objectifs.& bsp; Il discute comment s& acute;lectionner des algorithmes et des mises-en-oeuvre qui satisfont des contraintes applicatives donn& acute;es.& bsp; Il a & acute;galement pour but de d& acute;montrer que les questions de mise-en-oeuvre ne se limitent pas & grave; des optimisations de performance, mais sont & acute;galement au centre des questions de s& acute;curit& acute; physique des circuits cryptographiques.& bsp; Il s'agit de s& acute;curiser ces derniers contre des adversaires qui tirent parti de canaux d'informations alternatifs (comme le temps ou la quantit& acute; d'& acute;nergie n& acute;cessaire pour r& acute;aliser un calcul) afin d'extraire des informations secr& grave;tes.& bsp; De telles questions sont essentielles pour le d& acute;ploiement de petits circuits int& acute;gr& acute;s, comme des cartes & grave; puces, RFIDs, ... Contenu : - Hypoth& grave;ses math& acute;matiques des algorithmes cryptographiques, - Mises-en-oeuvre efficaces de cryptosyst& grave;mes, - Probl& grave;mes de cryptanalyse math& acute;matique (statistique, alg& acute;brique, ...), - Attaques physiques & grave; partir de canaux cach& acute;s ou d'insertions de faute, - G& acute;n& acute;ration de nombres al& acute;atoires, biom& acute;trie, fonctions physiques inclonables, - Int& acute;gration de circuits cryptographiques dans des syst& grave;mes s& acute;curis& acute;s, - ...
Autres infos :	Pr& acute;requis et & acute;valuation.& bsp; Le cours est ouvert & grave; tout & acute;tudiant suivant un master en ing& acute;ni& acute;rie & acute;lectrique, & acute;lectrom& acute;canique, informatique ou math& acute;matiques appliqu& acute;es.& bsp; Les seuls pr& acute;requis sont les cours de base du BAC en sciences de l'ing& acute;nieur (math& acute;matiques, statistique, programmation, ...)& bsp; L'& acute;valuation combine un projet et un examen & acute;crit. Plus de d& acute;tails : http://www.dice.ucl.ac.be/~fstandaert/teaching

Cycle et année d'étude: :	> Master [120] : ingénieur civil électricien > Master [120] : ingénieur civil électromécanicien > Master [120] : ingénieur civil en informatique > Master [120] : ingénieur civil en mathématiques appliquées
Faculté ou entité en charge:	ELEC