UCL Université catholique de Louvain

LELEC2760

2015-2016

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
Ressources en ligne:	> http://perso.uclouvain.be/fstandae/teaching.html
Thèmes abordés :	Le cours développe plus précisément les sujets suivants: -- les hypothèses idéales pour des algorithmes cryptographiques (en particulier les chiffrements par bloc), -- la cryptanalyse mathématique (statistique, algébrique, ...), -- la mise en oeuvre efficace des systèmes de chiffrement, -- les attaques physiques exploitant des canaux d'information auxiliaires (par exemple la consommation d'énergie, le rayonnement électromagnétique, ...) ou l'insertion de fautes, -- génération de nombres aléatoires, la biométrie, les fonctions physiquement inclonables, ... -- l'intégration de fonctionalités cryptographiques dans des systèmes et des applications sécurisés.
Acquis d'apprentissage	Eu égard au référentiel AA du programme « Master ingénieur civil électricien », ce cours contribue au développement, à l'acquisition et à l'évaluation des acquis d'apprentissage suivants : -- AA1.1, AA1.2, AA1.3 -- AA2.2 -- AA3.2 -- AA4.3 -- AA5.3, AA5.6 Plus précisément, à l'issue de ce cours, l'étudiant sera en mesure de: - Définir la notion de chiffrement sécurisé et argumenter la difficulté de construire des chiffrements par bloc efficaces dont la sécurité est prouvée dans un modèle formel. - Identifier les propriétés qui permettent de garantir la sécurité «pratique» d'un chiffrement, ainsi que les faiblesses structurelles à éviter lors de leur conception. - Critiquer les hypothèses heuristiques utilisées dans les analyses de sécurité mathématiques et physiques d'une fonction de chiffrement ou de son implémentation. - Appliquer des techniques de cryptanalyse (par exemples statistiques, algébriques, combinatoires) et évaluer leur impact sur des algorithmes de chiffrements. - Décrire et analyser l'architecture d'une implémentation cryptographique respectant des contraintes formulées selon différents critères de coût et de performances. - Implémenter un algorithme cryptographique dans un microcontrôleur. - Evaluer la sécurité physique d'une implémentation cryptographique contre des attaques par canaux cachés, exploitant des fuites physiques d'information (par exemple, la consommation énergétique d'un circuit effectuant des calculs cryptographiques). - Proposer des contremesures et mécanismes de protection contre différentes attaques physiques et justifier leur pertinence en fonction des contextes d'attaques. - Formaliser des propriétés physiques pouvant être exploités de façon constructive en cryptographie (par exemple pour la génération de nombres aléatoires, la conception de fonctions physiques inclônables ou la protection de la propriété intellectuelle). - Enumérer les avantages et inconvénients d'un algorithme cryptographique en fonction de son compromis sécurité (mathématique et physique) vs. efficacité d'implémentation. - Comprendre, résumer et présenter les résultats d'un article scientifique touchant aux domaines de la conception ou de la mise en oeuvre d'algorithmes cryptographiques (par exemple publié aux conférences Eurocrypt, Crypto, CHES, FSE, ACM CCS, ...). *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) ».*

Modes d'évaluation des acquis des étudiants :	Les étudiants seront évalués individuellement, sur base des éléments suivants: - Résolution des problèmes d'implémentation et de cryptanalyse proposés lors des séances d'exercices du cours et structurés sous forme de projets. - Synthèse écrite et/ou présentation orale d'un article scientifique. - Réponse aux questions de début de cours sur les lectures préliminaires. - Examen écrit et/ou oral portant sur les objectifs d'apprentissage listés ci-dessus. La pondération entre ces différents éléments peut varier d'année en année et sera annoncée lors du premier cours de chaque année académique. Sur demande individuelle, l'évaluation sera limitée à un travail écrit et un examen en session.
Méthodes d'enseignement :	Le cours est organisé en 14 exposés et 14 séances d'exercices (de 2 heures). Chaque exposé est préparé par une lecture préliminaire, au sujet de laquelle les étudiants sont interrogés en début de séance. Les périodes d'exercices sont consacrées à la résolution de problèmes d'implémentation et de cryptanalyse, structurés sous forme de projets à réaliser par groupes de 2 ou 3 étudiants. Les dernières heures de cours sont consacrées à la présentation d'articles scientifiques proposés par les étudiants.
Contenu :	Chiffrements par bloc (2 cours), implémentations matérielles (1 cours), implémentations logicielles (1 cours), attaques par canaux cachés (2 cours), tamper résilience et attaques par fautes (1 cours), fonctions physiques inclônables (1 cours), + sujets ouverts
Bibliographie :	Notes de cours et articles disponibles sur la page du cours
Autres infos :	Le cours est ouvert à tout étudiant suivant un master en ingénierie électrique, électromécanique, informatique ou mathématiques appliquées. Les prérequis sont les cours du BAC en sciences de l'ingénieur (mathématiques, statistique, programmation).
Faculté ou entité en charge:	ELEC

Programmes / formations proposant cette unité d'enseignement (UE)				
Intitulé du programme	Sigle	Crédits	Prérequis	Acquis d'apprentissage
Master [120] : ingénieur civil électromécanicien	ELME2M	5	-	
Master [120] : ingénieur civil électricien	ELEC2M	5	-	
Master [120] : ingénieur civil en informatique	INFO2M	5	-	
Master [120] : ingénieur civil en mathématiques appliquées	MAP2M	5	-	