REPUBLIQUE TUNISIENNE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET LA RECHERCHE SCIENTIFIQUE
UNIVERSITE DE SOUSSE

المدرسة الوطنية للمهندسين بسوسة
Ecole Nationale d'Ingénieurs de Sousse

Invitation

Vous êtes cordialement invités à ma soutenance de thèse de doctorat en Génie Électrique, intitulée :

Secured Digital Architectures for Low Cost Full-fledged HF RFID Tags

Qui aura lieu le 06/12/2018 à (10h) à l'amphithéâtre de l'École Nationale d'Ingénieurs de Sousse.
La soutenance sera suivie d'un pot auquel vous êtes également conviés.

Résumé

L'identification par radiofréquence (RFID) est une technologie émergente qui permet l'authentification d'objets sans contact physique. Les tags RFID sont présents dans de nombreuses applications sécurisées de la vie quotidienne, tels que le paiement sans contact, les passeports électroniques et le contrôle d'accès. Du fait que la technologie RFID est sans fil, plusieurs attaques passives telles que l'espionnage des communications, la désynchronisation des clés, et les attaques par canaux cachés peuvent être réalisées. Dans ce contexte, la sécurité des tags RFID contre ces types d'attaques est un enjeu majeur.

Cette thèse propose des solutions de sécurité à faible coût pour des tags RFID HF afin d'assurer une communication sécurisée. Pour cette raison, nous avons proposé des architectures de tags numériques faible coût et sécurisées qui implémentent un contrôleur logique simple à base d'une machine à états finis (FSM) (plutôt qu'un contrôleur plus complexe basé sur un processeur) et qui respectent l'ISO / IEC 14443 type A. Ces architectures de tags implémentent des blocs de chiffrements classiques comme AES et 3DES et des blocs des chiffrements légers tels que PRESENT et XTEA. Nous avons validé toutes ces architectures de tags en utilisant une plateforme d'émulation à base de FPGA.

En outre, pour évaluer la sécurité des tags numériques contre les attaques par exploitation des radiations électromagnétiques (EMA), nous avons proposé une plateforme de test pour la mise en place d'attaques. Afin de sécuriser les architectures attaquées contre ces EMA, nous avons proposé des améliorations de sécurité au niveau des protocoles d'authentification mutuelles (respectant l'ISO / IEC 9798-2) en utilisant des opérations de mise à jour de clé supplémentaires ou en utilisant des fonctions de temporisation.

Cordialement

NAIJA Yassine