Université de Monastir
Faculté des Sciences
Département de Physique

Proposition d'un sujet de stage de Master de Recherche en Physique*

Titre du Stage : Conception et implémentation d'un système de chiffrement par bloc chaotique pour la sécurité d'information.

Encadrant(s) : WAJIH El hadj youssef **Email :** elhadjyoussef_wajih@yahoo.fr **Etablissement :** ENIM

Structure de Recherche : Laboratoire d'Electronique et de Micro-électronique, FSM

Le Stage sera suivi par une thèse : oui

Résumé du travail :

Le sujet proposé a pour objectif l'étude et l'application de mécanisme cryptographique chaotique pour une transmission sécurisée. En effet, la protection de la vie privée des utilisateurs, l'intégrité et l'authenticité des circuits intégrés déployés sont quelques problématiques de sécurité identifiées. De tels besoins en sécurité imposent la recherche d'algorithmes cryptographiques efficaces et ayant une petite empreinte matérielle.

Dans ce contexte, ce travail s'intéressera à l'étude et la conception d'un système chaotiques unidimensionnels pour la génération des nombres pseudo-aléatoires, destiné au chiffrement par bloc. Une implémentation sera effectuée sur une plateforme matérielle pour tester les performances de la solution proposée. Dans ce notre travail, on prendra en considération les besoins des circuits intégrés utilisés dans l'IoT. Cette étude portera non seulement sur l'étude et l'implémentation d'algorithmes rapides, peu coûteux et sûrs mais intègrera aussi la notion de résistance aux attaques physiques.

*__NB :__

- L'étudiant doit contacter l'encadrant pour plus d'information.
- L'étudiant ne peut commencer son sage qu'après accord de la commission du Master (signature de la fiche du stage par les différentes parties).