

FORMATION

- 2009 – 2012**
 - **Doctorant en informatique de l'Université Rennes 1 au sein de l'IRISA** (Institut de Recherche en Informatique et Systèmes Aléatoires)
 - **Titre** : Unités arithmétiques reconfigurables pour cryptoprocresseurs robustes aux attaques par canaux auxiliaires
 - **Encadrants** : Arnaud Tisserand (CR CNRS, HDR) et Emmanuel Casseau (Prof. Univ. Rennes 1 - ENSSAT, HDR)
- 2006 – 2008**
 - **Master CSI** (Cryptologie et Sécurité Informatique), Université Bordeaux 1
 - **Synthèses** : *Access Control Mechanisms* ; *Anti-spam techniques and proposals*
 - **Projets** : Etude de la transformée de Hough généralisée (implémentation en Python) ; Jeu d'échecs en Java et stéganographie en C et Java
- 2004 – 2006**
 - **Licence Mathématiques et Informatique**, Université Bordeaux 1
- 2002 – 2004**
 - **BTS Informatique de Gestion**, Mention A-Bien, Lycée Gustave Eiffel (Bordeaux 33)
- 2002**
 - **Baccalauréat série Scientifique**, Spécialité Mathématiques, Lycée François Mauriac (Bordeaux 33)

EXPERIENCES PROFESSIONNELLES

- 2009 – 2012**
 - **Mobilité** de trois mois au sein du groupe *Code and Cryptography* de l'*University College Cork* (UCC) en Irlande
 - Objectif : réalisation d'une attaque par canaux auxiliaires sur différents algorithmes de multiplication scalaire implantés sur circuit programmable FPGA
 - **Publication** : T. Chabrier, D. Pamula and A. Tisserand. **Hardware implementation of DBNS recoding for ECC processor**. In *Proc. 44rd Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, USA, pages 1129-1133, Nov. 7-10, 2010. IEEE
- Déc 2008 - Fév 2009**
 - **CDD au Centre de Microélectronique de Provence Georges Charpak (CMP-GC)**, Gardanne (13)
 - Création de documentations : guide de l'utilisateur et guide du développeur
 - Optimisation et ajout de fonctionnalités sur le programme réalisé lors du stage précédent
- Avril - Sept 2008**
 - **Stage de fin de Master au CMP-GC**, Gardanne (13)
 - Participation à un projet de recherche industriel ayant pour objet la sécurisation des systèmes à cartes à puce sans contact, et plus précisément le NFC (Near Field Communication)
 - Réalisation d'un programme en LabVIEW permettant d'utiliser un banc d'expérimentation (émulateur de cartes à puce sans contact) comme simulateur d'attaques et démonstrateur de contre-mesures
- Mai - Juin 2004**
 - **Stage de fin de BTS au Centre en Route de la Navigation Aérienne du Sud-Ouest**, Mérignac (33)
 - Création d'un site intranet en PHP avec une base de données MySQL

COMPETENCES

- Programmation**
 - C, Java, PHP, Python, SQL, LabVIEW, VHDL, Assembleur
- Systèmes de calcul**
 - Maple, Pari/GP, Magma, Matlab
- Mathématiques**
 - Arithmétique, corps finis, courbes elliptiques, ...
- Cryptologie**
 - Chiffrements symétriques et asymétriques, cryptanalyse
- Informatique**
 - Sécurité réseaux, sécurité des langages
- Anglais**
 - Conversation courante et technique
- Italien**
 - Lu, écrit, parlé

LOISIRS

Natation, water-polo, lecture, musique