

EDUCATION

- 2009 – 2012**
 - **Ph.D. Thesis in computer science from University Rennes 1 - IRISA** (Institut de Recherche en Informatique et Systèmes Aléatoires)
 - **Title:** Reconfigurable Arithmetic Units for Cryptoprocessors with Protection against Side Channel Attacks
 - **Supervisors:** Arnaud Tisserand (CR CNRS, HDR) and Emmanuel Casseau (Prof. Univ. Rennes 1 - ENSSAT, HDR)
- 2006 – 2008**
 - Postgraduate degree CSI (Cryptography and IT Security), University Bordeaux 1
 - **Synthesis:** Access Control Mechanisms; Anti-spam techniques and proposals
 - **Projects:** Study of generalized Hough transform (implementation in Python); Chess game in Java; Steganography in C and Java
- 2004 – 2006**
 - Bachelor's Degree in science : Mathematics and IT, University Bordeaux 1
- 2002 – 2004**
 - 2 years technical degree (BTS) in computer science (Bordeaux)
- 2002**
 - High School Diploma in science with a speciality in mathematics, in Bordeaux

WORK EXPERIENCE

- 2009 – 2012**
 - **Doctoral student** exchange with the **Coding and Cryptography** Research Group in UCC (University of College Cork, Ireland) from July 2011 to September 2011
 - Goal: applying template attacks to hardware implementations of Elliptic Curve cryptographic algorithms and investigating the strength of some proposed countermeasures
 - **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
- Dec 2008 - Feb 2009**
 - **Three months contract in Centre de Microélectronique de Provence Georges Charpak, Gardanne (13)**
 - Documentation creation : user's guide and developer's guide
 - Development of an attack scenario
- April - Sept 2008**
 - **Compulsory 3 months work placement for the postgraduate** degree in Centre de Microélectronique de Provence Georges Charpak, Gardanne (13)
 - Participation to an industrial research project for the security of the contactless smartcard, more precisely the NFC (Near Field Communication)
 - Programming of a demonstrator of attacks and counter-measures in LabVIEW
- May - June 2004**
 - **Compulsory 2 months work placement for the BTS diploma** in CRNA/SO (Centre en Route de la Navigation Aérienne de Sud-ouest), Mérignac (33)
 - Creation of a technical phone book intranet site using PHP/MySQL

SPECIAL SKILLS

- Programming**
 - C, Java, PHP, Python, SQL, LabVIEW, VHDL, Assembler
- Computation**
 - Maple, Pari/GP, Magma, Matlab
- Mathematics**
 - Arithmetics in Z field, finite fields, elliptic curves, ...
- Cryptography**
 - Symmetric and asymmetric encryption, cryptanalysis
- Computer Science**
 - Network security, language security
- English**
 - Conversational and working knowledge
- Italian**
 - Fluent (10 months spent in Bologna, Italia)