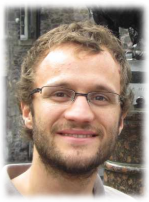
Simon Pontié
CurriculumVitae



Contacts

École des Mines de Saint-Étienne
Campus Georges Charpak Provence
880, route de Mimet
13541 GARDANNE Cedex France
+33442616728
simon.pontie@cea.fr
https://www.simon.pontie.fr

Work Experiences

Current **Researcher** at CEA Cadarache, CEA Tech across France, Provence-Alpes-Côte d'Azur region
SAS research group (*Secure Architectures and Systems*), Center of Microelectronics in Provence

2013-2016 **Ph.D.**, Grenoble-Alpes University (*France*), TIMA Laboratory, AMfoRS research group
Ph.D. thesis defence at Grenoble: November 21st, 2016. Jury: Arnaud Tisserand, Lionel Torres, Philippe Elbaz-Vincent, Pierre-Yvan Liardet, Viktor Fischer, Régis Leveugle, and Paolo Maistri
3 years of research, supervisors: Régis Leuveugle and Paolo Maïstri
Hardware security for cryptography based on elliptic curves (link)
3 years as a teacher at Phelma *(school of Physics and Electronics in Grenoble)* in addition to my PhD studies
digital and analog electronics, real-time systems, security of embedded systems, embedded systems

February-June 2012 Electronic sciences research during Master internship: TIMA Laboratory, Grenoble
Design and validation of a secure crypto-processor for cryptography based on elliptic curves

June-July 2010 Electronic sciences research during Bachelor internship: BIOMIS Laboratory, Rennes, France
Design of a potentiostat for micro sensor

Education

2013-2016 **Ph.D.**, Grenoble-Alpes University, TIMA Laboratory, Grenoble, France
Three years, researcher and teacher as Ph.D. student

2012-2013 **Research Master**: Joseph Fourier University, Grenoble
Nanoelectronic and Nanotechnology, Hardware design

June 2012 National Competitive Examination for Teacher Training in Electrical Engineering *(French agrégation)*

2011-2012 **Master**: École Normale Supérieure de Cachan, Rennes
Higher-education teacher training in electrical engineering
Preparation of the *French agrégation* in electrical engineering

2010-2011 First year of **Master**: École Normale Supérieure de Cachan and University of Rennes
Electronics and Telecommunications
First year of **Master**: École Normale Supérieure de Cachan and University of Rennes
Mechanical engineering

2009-2010 **Bachelor**: École Normale Supérieure de Cachan and University of Rennes
Electronics and Telecommunications
Bachelor: École Normale Supérieure de Cachan and University of Rennes
Mechanical engineering

Special Skills

- Hardware Design: Modelsim, ISE, EDK, Vivado, HLS softwares, HDLs: vhdl and verilog
- Programming Languages: C, Bash, Matlab, C++, Ruby
- Office automation tools: Latex, Beamer, Word, Power Point
- UNIX system administration

Languages

- Advanced English level
- Native French speaker
- Basic Spanish communication skills

Miscellaneous

- Ski touring
- Mountain hike
- Personal projects combining electronic and computer sciences

Publications and Conferences

Journal

[1] **S. Pontie**, P. Maistri, and R. Leveugle, "Dummy Operations in Scalar Multiplication over Elliptic Curves: a Tradeoff between Security and Performance," *Microprocessors and Microsystems*, vol. 47, Part A, pp. 23–36, 2016. link.

Refereed Conference Proceedings

[1] **S. Pontie**, A. Bourge, A. Prost-Boucle, P. Maistri, O. Muller, R. Leveugle, and F. Rousseau, "HLS-Based Methodology for Fast Iterative Development Applied to Elliptic Curve Arithmetic," in *19th Euromicro Conference on Digital System Design (DSD)*, 2016, pp. 511–518. link.

[2] T. Backenstrass, M. Blot, **S. Pontie**, and R. Leveugle, "Protection of ECC Computations against Side-Channel Attacks for Lightweight Implementations," in *1st International Verification and Security Workshop (IVSW)*, 2016, pp. 1–6. link.

[3] **S. Pontie**, P. Maistri, and R. Leveugle, "An Elliptic Curve Crypto-Processor Secured by Randomized Windows," in *17th Euromicro Conference on Digital System Design (DSD)*, 2014, pp. 535–542. link.

[4] **S. Pontie** and P. Maistri, "Randomized windows for secure scalar multiplication on elliptic curves," in *25th International Conference on Application-specific Systems, Architectures, and Processors (ASAP)*, 2014, pp. 78–79. link.

[5] **S. Pontie** and P. Maistri, "Design of a secure architecture for scalar multiplication on elliptic curves," in *10th Conference on Ph. D. Research in Microelectronics and Electronics (PRIME)*, 2014, pp. 1–4. link.

Other Communications

[1] **S. Pontie**, "Étude de la sécurité des courbes quartiques de Jacobi vis à vis des attaques par analyse de puissance consommée." Séminaire à l'École des Mines de Saint-Etienne, Gardanne, 2016. link.

[2] **S. Pontie**, "Prise en compte des fuites d'informations par canaux auxiliaires dans une implémentation ECC." Séminaire sécurité des systèmes électroniques embarqués, Rennes, 2016. link.

[3] **S. Pontie**, "Attaque par analyse de la puissance consommée contre un crypto-processeur basé sur les courbes Jacobi quartiques." Journées Codage et Cryptographie, Toulon, 2015. link.

[4] **S. Pontie**, P. Maistri, and R. Leveugle, "Tuning of randomized windows against simple power analysis for scalar multiplication on elliptic curves." TRUDEVICE 2015: Workshop on Trustworthy Manufacturing; Utilization of Secure Devices, Grenoble, 2015. link.

[5] **S. Pontie** and M.-A. Cornelie, "Fast and secure crypto-processor based on Elliptic Curve Cryptography." 2eme Journée SCCyPhy: Security; Cryptology for CyberPhysical systems, Grenoble, 2015. link.

[6] **S. Pontie**, "Architecture d'un crypto processeur ECC sécurisé contre les attaques physiques." Journées Nationales du Réseau Doctoral en Micro-nanoélectronique, Lille, pp. 1–4, 2014. link.

[7] **S. Pontie**, "Multiplication scalaire avec fenêtrage aléatoire pour la protection d'un coprocesseur de chiffrement basé sur les courbes elliptiques." 1er Journée SCCyPhy: Security; Cryptology for CyberPhysical systems, Grenoble, 2014.

Reviewer for

- Microprocessors and Microsystems
- IET Computers & Digital Techniques

Simon Pontié