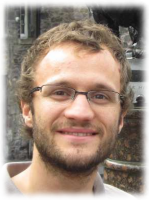
Simon Pontié
CurriculumVitae



Contacts

École des Mines de Saint-Étienne
Campus Georges Charpak Provence
880, route de Mimet
13541 GARDANNE Cedex France
0442616728
simon.pontie@cea.fr
https://www.simon.pontie.fr

Expériences

En poste **Ingénieur Chercheur** au CEA Cadarache, CEA Tech en région, département PACA
Dans une équipe commune entre le CEA et l'école des Mines de Saint-Étienne
Équipe de recherche SAS (*Systèmes et Architectures Sécurisés*)

2013-2016 **Thèse de doctorat** de l'Université Grenoble-Alpes, Laboratoire TIMA, équipe AMfoRS
soutenue à Grenoble le 21 novembre 2016 devant le jury composé de : Arnaud Tisserand, Lionel Torres, Philippe Elbaz-Vincent, Pierre-Yvan Liardet, Viktor Fischer, Régis Leveugle et Paolo Maistri
3 ans de recherche sous la direction de Régis Leuveugle et Paolo Maïstri
Sécurisation matérielle pour la cryptographie à base de courbes elliptiques (lien)
3 ans d'enseignement dans l'école d'ingénieur PHELMA *(PHysique, ÉLectronique, MAtériaux)*, Grenoble
Électronique numérique et analogique, Système temps-réels, Sécurité des systèmes embarqués, Systèmes embarqués

Février-Juillet 2012 Chercheur en qualité de stagiaire de Master 2 : Laboratoire TIMA, Grenoble
Conception et validation d'un coprocesseur de chiffrement basé sur les courbes elliptiques

Juin-Juillet 2010 Initiation à la Recherche : Stage de License au Laboratoire BIOMIS, Rennes
Conception d'un potentiostat pour micro capteur

Formation

2013-2016 **Thèse de doctorat en électronique** de l'Université Grenoble-Alpes, Laboratoire TIMA, Grenoble
Trois années de recherche et d'enseignement en qualité de doctorant

2012-2013 **Master 2 Recherche** : Université Joseph Fourier, Grenoble
Nanoélectronique et Nanotechnologie, parcours conception, mention très bien

Juin 2012 **Agrégation externe** de génie électrique

2011-2012 **Master 2** : École Normale Supérieure de Cachan, Rennes
Formation à l'enseignement supérieur
Préparation à l'agrégation de Génie Électrique

2010-2011 **Master 1** : École Normale Supérieure de Cachan et Université de Rennes 1
Électronique et Télécommunication
Master 1 : École Normale Supérieure de Cachan et Université de Rennes 1
Mécanique et Science de l'Ingénieur

2009-2010 **License** : École Normale Supérieure de Cachan et Université de Rennes 1
Électronique et Télécommunication
License : École Normale Supérieure de Cachan et Université de Rennes 1
Mécanique et Science de l'Ingénieur

Compétences Spécifiques

- Conception numérique : Modelsim, ISE, EDK, Vivado, logiciels de HLS, Description matériel : vhdl et verilog
- Conception logiciel : C, Bash, Matlab, C++, Ruby
- Bureautique : Latex, Beamer, Word, Power Point
- Administration de système UNIX

Langues

- Maîtrise de l'anglais
- Notions d'espagnol

Centres d'interets

- Ski de randonnée
- Marche en montagne
- Projets personnels alliant électronique et informatique

Publications, Conférences et Projets de Recherche

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. lien.

Actes de Conférences à Comité de Lecture

[1] P. Leignac, O. Potin, J.-M. Dutertre, J.-B. Rigaud, and **S. Pontie**, "Comparaison of side-channel leakage on Rich and Trusted Execution Environments," in *6th Workshop on Cryptography and Security in Computing Systems*, 2019. lien.

[2] **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. lien.

[3] 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. lien.

[4] **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. lien.

[5] **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. lien.

[6] **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. lien.

Autres interventions

[1] **S. Pontie** and D. Aboulkassimi, "Attaque side-channel sur plateforme mobile Android." Séminaire à l'École des Mines de Saint-Etienne, Gardanne, 2018. lien.

[2] **S. Pontie** and D. Aboulkassimi, "Hardware characterization for mobile devices a security perspective." 1st Mobitrust International Workshop, Portugal, Aveiro, 2017. lien.

[3] **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. lien.

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

[5] **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. lien.

[6] **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. lien.

[7] **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. lien.

[8] **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. lien.

[9] **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.

Participation à des projets de recherche

- CSAFE+ : projet FUI
- MobiTrust : projet CATRENE

Simon Pontié