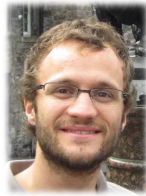


Simon Pontié

Curriculum Vitae



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 LETI](#), Laboratoire Sécurité des COmposants (LSCO)
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 Leveugle et Paolo Maistri
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

Journal

- [1] L. De Feo, N. El Mrabet, A. Genêt, N. Kaluderović, N. Linard de Guertechin, **S. Pontie**, and É. Tasso, “SIKE channels : Zero-value side-channel attacks on SIKE,” *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 264–289, 2022. [lien DOI](#) [Présentation](#).
- [2] **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. [DOI](#).

Actes de Conférences à Comité de Lecture

- [1] R. Joud, P.-A. Moëllic, **S. Pontie**, and J.-B. Rigaud, “Like an open book ? Read neural network architecture with simple power analysis on 32-bit microcontrollers,” in *Smart card research and advanced applications : 22nd international conference, CARDIS 2023*, 2023, pp. 256–276. [DOI](#) [arXiv](#).
- [2] C. Fanjas, D. Aboukassimi, **S. Pontie**, and J. Clédière, “Exploration of system-on-chip secure-boot vulnerability to fault-injection by side-channel analysis,” in *2023 IEEE international symposium on defect and fault tolerance in VLSI and nanotechnology systems (DFT)*, 2023, pp. 1–6. [DOI](#) [hal](#).
- [3] M. Dumont, K. Hector, P.-A. Moëllic, J.-M. Dutertre, and **S. Pontie**, “Evaluation of parameter-based attacks against embedded neural networks with laser injection,” in *Computer safety, reliability, and security : 41st international conference, SAFECOMP 2023*, 2023, pp. 259–272. [DOI](#) [arXiv](#).
- [4] C. Fanjas, C. Gaine, D. Aboukassimi, **S. Pontie**, and O. Potin, “Combined fault injection and real-time side-channel analysis for android secure-boot bypassing,” in *Smart card research and advanced applications : 21st international conference, CARDIS 2022, birmingham, UK, november 7–9, 2022, revised selected papers*, 2022, pp. 25–44. [hal](#) [ePrint](#) [DOI](#).
- [5] R. Joud, P.-A. Moëllic, **S. Pontie**, and J.-B. Rigaud, “A practical introduction to side-channel extraction of deep neural network parameters,” in *Smart card research and advanced applications : 21st international conference, CARDIS 2022, birmingham, UK, november 7–9, 2022, revised selected papers*, 2022, pp. 45–65. [hal](#) [arXiv](#) [DOI](#).
- [6] D. Bellizia, N. El Mrabet, A. Fournaris, **S. Pontie**, R. Francesco, F.-X. Standaert, É. Tasso, and E. Valea, “Post-quantum cryptography : Challenges and opportunities for robust and secure HW design,” in *2021 IEEE international symposium on defect and fault tolerance in VLSI and nanotechnology systems (DFT)*, 2021, pp. 1–6. [hal](#) [DOI](#).
- [7] É. Tasso, L. De Feo, N. El Mrabet, and **S. Pontie**, “Resistance of isogeny-based cryptographic implementations to a fault attack,” in *International workshop on constructive side-channel analysis and secure design*, 2021, pp. 255–276. [hal](#) [ePrint](#) [DOI](#).
- [8] C. Gaine, D. Aboukassimi, **S. Pontie**, J.-P. Nikolovski, and J.-M. Dutertre, “Electromagnetic fault injection as a new forensic approach for SoCs,” in *2020 IEEE international workshop on information forensics and security (WIFS)*, 2020, pp. 1–6. [hal](#) [DOI](#).
- [9] 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, pp. 19–22. [hal](#) [DOI](#).
- [10] **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. [hal](#) [DOI](#).
- [11] 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. [DOI](#).
- [12] **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. [DOI](#).
- [13] **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. [DOI](#).
- [14] **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. [DOI](#).

Autres interventions

- [1] **S. Pontie**, “Introduction aux attaques physiques.” Séminaire au M2 FSI (Fiabilité et Sécurité Informatique) d’Aix Marseille Université, 2023.
- [2] A. Ras, M. Carmona, A. Loiseau, **S. Pontie**, G. Renault, B. Smith, and E. Valea, “Secure, optimized and agile HW/SW implementation for post-quantum cryptography.” Poster at CHES 2023, 2023. [hal](#).
- [3] D. Aboukassimi, **S. Pontie**, and C. Fanjas, “How to exploit EMFI to bypass the secure-boot of SoC.” Cyber in Sophia Antipolis (8th edition of the Cyber in ... French Cybersecurity Doctoral School), 2023. [lien](#) [Présentation](#).
- [4] C. Fanjas, C. Gaine, D. Aboukassimi, **S. Pontie**, and O. Potin, “Méthode combinée d’injection de faute et d’analyse side-channel temps réel pour contourner le secure-boot d’android.” Journée thématique sur les attaques par injection de fautes (JAIF), 2022. [lien](#) [Présentation](#).
- [5] **S. Pontie**, É. Tasso, N. El Mrabet, L. De Feo, and G. Clément, “SIKE : Injection de fautes et contre-mesure sur la génération de clés.” Journée thématique des GDR SoC² et Sécurité Informatique : Algorithmes de chiffrement post-quantiques et sécurité matérielle, 2021. [lien](#) [Présentation video](#).
- [6] É. Tasso, L. De Feo, N. El Mrabet, and **S. Pontie**, “Resistance of isogeny-based cryptographic implementations to a fault attack.” Journée thématique sur les attaques par injection de fautes (JAIF), 2021. [lien](#) [Présentation video](#).
- [7] C. Gaine, D. Aboukassimi, **S. Pontie**, J.-P. Nikolovski, and J.-M. Dutertre, “Electromagnetic fault injection on SoCs.” Journée thématique sur les attaques par injection de fautes (JAIF), 2021. [lien](#) [Présentation video](#).
- [8] É. Tasso, L. De Feo, N. El Mrabet, and **S. Pontie**, “Resistance of isogeny-based cryptographic implementations to a fault attack.” 3th NIST PQC Standardization Conference, 2021. [Présentation Article video](#).
- [9] É. Tasso, L. De Feo, N. El Mrabet, and **S. Pontie**, “Résistance des implémentations cryptographiques basées sur les isogénies à une attaque en faute.” Séminaire de l’équipe Informatique et algèbre appliquée, Institut de mathématiques de Toulon, 2021. [lien](#).
- [10] N. El Mrabet, M. Carmona, **S. Pontie**, J.-P. Enguent, and P. Galy, “La cryptographie post-quantique et les enjeux associés aux implémentations des algorithmes proposés.” Webinaire du pôle SCS : WebTech#SCS, 2021. [lien](#).
- [11] **S. Pontie** and D. Aboukassimi, “Attaque side-channel sur plateforme mobile android.” Séminaire à l’École des Mines de Saint-Etienne, Gardanne, 2018. [lien](#).
- [12] **S. Pontie** and D. Aboukassimi, “Hardware characterization for mobile devices a security perspective.” 1st Mobitrust International Workshop, Portugal, Aveiro, 2017. [lien](#).
- [13] **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](#).
- [14] **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](#).
- [15] **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](#).
- [16] **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](#).
- [17] **S. Pontie** and M.-A. Cornélie, “Fast and secure crypto-processor based on elliptic curve cryptography.” 2eme Journée SCCyPhy : Security ; Cryptology for CyberPhysical systems, Grenoble, 2015. [lien](#).
- [18] **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. [hal](#).
- [19] **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.

ACTIVITÉS DE RECHERCHE

Encadrements

Doctorants/Doctorantes

- [Antonio Ras](#) (2022-2025) : *Accélération et sécurisation de la cryptographie post-quantique agile basée sur les réseaux euclidiens et les codes-correcteurs.*
([LinkedIn](#))
Encadré avec [Mikael Carmona](#), [Antoine Loiseau](#), [Emanuele Valea](#), [Guénaël Renault](#) et [Benjamin Smith](#).
- [Clément Fanjas](#) (2021-2024) : *Exploitation des vulnérabilités matérielles des dispositifs mobiles comme nouvelle approche pour l'analyse Forensic.*
([LinkedIn](#))
Encadré avec [Jessy Clédière](#) et [Driss Aboukassimi](#).
- [Raphaël Joud](#) (2020-2023) : *Attaques Side-Channel contre la confidentialité des modèles de Machine Learning embarqués : attaques, protections, évaluation.*
([LinkedIn](#))
Encadré avec [Pierre-Alain Moëllic](#) et [Jean-Baptiste Rigaud](#).
- [Elise Tasso](#) (2019-2022) : *Sécurisation matérielle de cryptographie post-quantique basée sur les isogénies entre courbes elliptiques.*
([dblp](#))
Encadrée avec [Nadia El Mrabet](#) et [Luca De Feo](#).
La soutenance a eu lieu le 12-12-2022

Contrats à durée déterminée

- [Daniel Resende](#) (2022-2024) : Développement logiciel pour la cryptographie dans le cadre du projet de recherche ACROQAY.
([LinkedIn](#))

Stagiaires

- [Clement Fanjas](#) (2021) : *Vulnérabilités matérielles des smartphones face aux verrous de la synchronisation.*
([LinkedIn](#))
Encadré avec [Driss Aboukassimi](#) et [Olivier Potin](#).

Participation à des projets de recherche

- [POLIICE](#) : projet Horizon Europe (2022-2025).
- [REV](#) : projet lauréat de l'appel à projets du PEPR Cybersécurité (2023-2028).
- [ACROQAY](#) : projet Carnot Exploratoire (2020-2024).
- [PICTURE](#) : projet ANR (PRCE, 2021-2024).
- [EXFILES](#) : projet H2020 (2020-2023)
- [CSAFE+](#) : projet FUI (2017-2021)
- [MobiTrust](#) : projet CATRENE (2014-2017)

Autres Activités

- Comité de programme du workshop [COSADE2024](#)
- Comité scientifique et comité de programme du workshop [PHISIC2022](#)
- Comité technique du workshop [PHISIC2019](#)

Simon Pontié