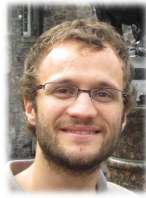


Simon Pontié

Curriculum Vitae



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 LETI](#),
[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 Leveugle and Paolo Maistri
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

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. [link](#) [DOI](#) [Slides](#).
- [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](#).

Refereed Conference Proceedings

- [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](#).

Other Communications

- [1] **S. Pontie** and D. Resende, “Accélération matérielle d’une signature ECDSA dans un ASIC en FD-SOI 22nm avec contremesures aux attaques physiques.” Journées Nationales 2024 du GDR Sécurité Informatique, 2024. [program](#).
- [2] **S. Pontie**, “Introduction aux attaques physiques.” Séminaire au M2 FSI (Fiabilité et Sécurité Informatique) d’Aix Marseille Université, 2023.
- [3] 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](#).
- [4] 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. [link Slides](#).
- [5] 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. [link Slides](#).
- [6] **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. [link Slides Video](#).
- [7] 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. [link Slides Video](#).
- [8] 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. [link Slides Video](#).
- [9] 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. [Slides Paper Video](#).
- [10] 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. [link](#).
- [11] 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. [link](#).
- [12] **S. Pontie** and D. Aboukassimi, “Attaque side-channel sur plateforme mobile android.” Séminaire à l’École des Mines de Saint-Etienne, Gardanne, 2018. [link](#).
- [13] **S. Pontie** and D. Aboukassimi, “Hardware characterization for mobile devices a security perspective.” 1st Mobitrust International Workshop, Portugal, Aveiro, 2017. [link](#).
- [14] **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](#).
- [15] **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](#).
- [16] **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](#).
- [17] **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](#).
- [18] **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](#).
- [19] **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](#).
- [20] **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.

RESEARCH ACTIVITIES

Supervisions

PhD students

- [Antonio Ras](#) (2022-2025): *Secured and optimized HW/SW Implementation of Agile Post-Quantum Cryptography based on lattices and codes.*
([LinkedIn](#))
Co-supervised with [Mikael Carmona](#), [Antoine Loiseau](#), [Emanuele Valea](#), [Guénaël Renault](#) and [Benjamin Smith](#).
- [Clément Fanjas](#) (2021-2024): *Hardware vulnerability exploitation for FORENSIC's use-cases on mobile devices.*
([LinkedIn](#))
Co-supervised with [Jessy Clédière](#) and Driss Aboukassimi.
- [Raphaël Joud](#) (2020-2023): *Side-Channel Analysis against the confidentiality of embedded neural networks: attack, protection, evaluation.*
([LinkedIn](#))
Co-supervised with [Pierre-Alain Moëllic](#) and Jean-Baptiste Rigaud.
The thesis was defended on 2024/01/18.
- [Elise Tasso](#) (2019-2022): *Hardware security for post-quantum cryptography based on elliptic curve isogenies.*
([dblp](#))
Co-supervised with [Nadia El Mrabet](#) and [Luca De Feo](#).
The thesis was defended on 2022/12/12.

Fixed-term contracts

- [Daniel Resende](#) (2022-2024): Software design for cryptography as part of the ACROQAY research project.
([LinkedIn](#))

Interships

- [Clement Fanjas](#) (2021): *Hardware vulnerability and new methods to resolve synchronization problem.*
([LinkedIn](#))
Co-supervised with Driss Aboukassimi and [Olivier Potin](#).
- [Soline Casavecchia](#) (2024): *Laser fault injection in System-on-Chip.*
([LinkedIn](#))
Co-supervised with Driss Aboukassimi, [Jessy Clédière](#) and [Jean-Max Dutertre](#).

Research Projects

- [POLHICE](#): Horizon Europe project (2022-2025).
- [REV](#): Cybersecurity PEPR project (2023-2028).
- [ACROQAY](#): Carnot Explorer project (2020-2024).
- [PICTURE](#): ANR project (PRCE, 2021-2024).
- [EXFILES](#): H2020 project (2020-2023).
- [CSAFE+](#): FUI project (2017-2021).
- [MobiTrust](#): CATRENE project (2014-2017)

Other Activities

- Program Committee of the [COSADE2024](#) workshop.
- Scientific and Program Committee of the [PHISIC2022](#) workshop.
- Technical committee of the [PHISIC2019](#) workshop.

Simon Pontié