Pascal Cotret | Embedded systems security

✉ pascal.cotret@ensta-bretagne.fr • pcotret.gitlab.io/index.html
Github/Gitlab: pcotret - **RootMe:** Pa0x73cal

Topics of interest

Last update: April 9, 2024

Embedded systems, security/cryptography, reconfigurables architectures, networks, low-level programming.

Work experience

ENSTA Bretagne - Associate professor **09/2019 ⇒ ...**

- Embedded systems security & reconfigurable architectures.
- Network basics, networks & security, embedded C, Python programming.
- Involved in the cybersecurity of maritime and port systems - post-master degree w/ IMT-A, École Navale and ENSM.

Thales - R&D engineer **09/2017 ⇒ 09/2019**

- Working with real-time operating systems, security and cryptographic applications.
- Also a researcher in my spare time.

CentraleSupélec Rennes - Associate professor **09/2014 ⇒ 08/2017**

- Embedded systems security, software/hardware codesign, reconfigurable architectures.
- HardBlare project: `https://project.inria.fr/hardblare/`
- Software-defined radio on FPGAs. Several stuff about hamradio and Cubesats.

CEA-LIST, Embedded Computing Lab - Research engineer **10/2013 ⇒ 08/2014**

- Research topic: Prototyping a smart camera for real-time face recognition and face detection.

ENSSAT, University of Rennes 1 - Assistant professor **09/2012 ⇒ 08/2013**

- Worked on countermeasures for an Elliptic Curve algorithm embedded in a reconfigurable device.

University of South Brittany - PhD student **11/2009 ⇒ 08/2012**

- Distributed security for communications and memories in multiprocessor architectures.

Education

University of South Brittany - PhD in Electronic Engineering **2009 ⇒ 2012**
Protection of heterogeneous multiprocessor architectures in embedded systems.

Télécom Saint-Étienne - Optoelectronic engineer diploma (MSc level) **2006 ⇒ 2009**
Analog and digital electronics, telecommunications, computer science, optoelectronics, optic systems.

University of South Wales - Bachelor of Engineering in Electronic Engineering **2007 ⇒ 2008**
Analog and digital electronics, telecommunications, computer science.

Computer skills

English: fluent, both written and oral – TOEIC score: 910.

Italian: intermediate level, both written and oral skills.

Programming: C/C++, assembly, VHDL/Verilog, Matlab, Unix. Scripting languages: Python, batch/bash.

Software: Matlab, Modelsim, FPGA tools, continuous integration (Jenkins), low level tools (GDB, etc.)

Interests

- Trail-running and hiking.
- Interested in CTFs and hacking challenges. Hamradio license owner since 2015.

Publications

Book chapters and journals

Pascal Cotret, Guy Gogniat, and Martha Johanna Sepúlveda Flórez. Protection of heterogeneous architectures on FPGAs: An approach based on hardware firewalls. *Microprocessors and Microsystems*, 42:127 – 141, 2016

Pascal Cotret and Guy Gogniat. Protection des architectures hétérogènes sur FPGA : une approche par pare-feux matériels. *Techniques de l'Ingenieur*, pages Référence IN175 – 10 pages, February 2014

E. Wanderley, R. Vaslin, J. Crenne, P. Cotret, G. Gogniat, J.-P. Diguet, J.-L. Danger, P. Maurine, V. Fischer, B. Badrignans, L. Barthe, P. Benoit, and L. Torres. Security FPGA analysis. In Benoit Badrignans, Jean Luc Danger, Viktor Fischer, Guy Gogniat, and Lionel Torres, editors, *Security Trends for FPGAS*, pages 7–46. Springer Netherlands, 2011

International publications

Moritz Peters, Nicolas Gaudin, Jan Philipp Thoma, Vianney Lapôtre, Pascal Cotret, Guy Gogniat, and Tim Güneysu. On The Effect of Replacement Policies on The Security of Randomized Cache Architectures. In *19th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2024)*, Jul 2024

Quentin Ducasse, Pascal Cotret, and Loïc Lagadec. Gigue: A JIT Code Binary Generator for Hardware Testing. In *2023 Workshop on Virtual Machines and Language Implementations*, Oct 2023

Jean-Loup Hatchikian-Houdot, Nicolas Gaudin, Pascal Cotret, Frédéric Besson, Guy Gogniat, Guillaume Hiet, Vianney Lapôtre, and Pierre Wilke. Work in Progress: Thwarting Timing Attacks in Microcontrollers using Fine-grained Hardware Protections. In *SILM'23 - IEEE EuroSP workshop*, July 2023

Quentin Ducasse, Pascal Cotret, and Loïc Lagadec. JIT Compiler Security through Low-Cost RISC-V Extension. In *RAW - 30th Reconfigurable Architectures Workshop*, May 2023

Quentin Ducasse, Guille Polito, Pablo Tesone, Pascal Cotret, and Loïc Lagadec. Porting a JIT compiler to RISC-V: Challenges and Opportunities. In *MPLR - Managed Programming Languages and Runtimes 2022*, Sep 2022

Quentin Ducasse, Pascal Cotret, Loïc Lagadec, and Rob Stewart. Benchmarking quantized neural networks on FPGAs with FINN. In *SLOHA - DATE Friday Workshop on System-level Design Methods for Deep Learning on Heterogeneous Architectures*, Feb 2021

Muhammad Abdul Wahab, Pascal Cotret, Mounit Nasr Allah, Guillaume Hiet, Vianney Lapôtre, Guy Gogniat, and Arnab Kumar Biswas. A MIPS-based coprocessor for information flow tracking in ARM SoCs. In *2018 International Conference on Reconfigurable Computing and FPGAs (Reconfig)*, pages 1–8, Dec 2018

Muhammad Abdul Wahab, Pascal Cotret, Mounit Nasr Allah, Guillaume Hiet, Vianney Lapôtre, Guy Gogniat, and Arnab Kumar Biswas. A novel lightweight hardware-assisted static instrumentation approach for ARM SoC using debug components. In *Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, pages 1–6, Dec 2018

Pascal Cotret and Muhammad Abdul Wahab. TrustZone is not enough - Hijacking debug components for embedded security. In *Chaos Communication Congress*, Dec 2017

Muhammad Abdul Wahab, Pascal Cotret, Mounit Nasr Allah, Guillaume Hiet, Vianney Lapôtre, and Guy Gogniat. A framework for efficient DIFT in real-world SoCs. In *2017 27th International Conference on Field Programmable Logic and Applications (FPL) - Demo session*, pages 1–2, Sep 2017

Muhammad Abdul Wahab, Pascal Cotret, Mounit Nasr Allah, Guillaume Hiet, Vianney Lapôtre, and Guy Gogniat. ARMHEx: A hardware extension for DIFT on ARM-based SoCs. In *2017 27th International Conference on Field Programmable Logic and Applications (FPL)*, pages 1–7, Sep 2017

Muhammad Abdul Wahab and Pascal Cotret. Pwning ARM debug components for sec-related stuff. In *Hack In the Box Security Conference – CommSec track*, Apr 2017

Pascal Cotret, Vipin Kizheppatt, and Christophe Moy. Multi-standard OFDM transceiver for heterogeneous system-on-chips. In *WinnComm Europe*, Oct 2016

Muhammad Abdul Wahab, Pascal Cotret, Mounir Nasr Allah, Guillaume Hiet, Vianney Lapôtre, and Guy Gogniat. Towards a hardware-assisted information flow tracking ecosystem for ARM processors. In *2016 26th International Conference on Field Programmable Logic and Applications (FPL)*, pages 1–2, Aug 2016

Pascal Cotret, Guillaume Hiet, and Guy Gogniat. HardBlare: an efficient hardware-assisted DIFC for non-modified embedded processors. In *CHES (Workshop on Cryptographic Hardware and Embedded Systems)*, Sep 2015

Pascal Cotret, Stéphane Chevobbe, and Mehdi Darouich. Embedded wavelet-based face recognition under variable position. In *SPIE Electronic Imaging*, volume 9400, pages 94000A–94000A–12. SPIE Electronic Imaging, 2015

Pascal Cotret, Guy Gogniat, Jean-Philippe Diguet, and Jérémie Crenne. Lightweight reconfiguration security services for AXI-based MPSoCs. In *22nd International Conference on Field Programmable Logic and Applications (FPL)*, pages 655–658, Aug 2012

Pascal Cotret, Florian Devic, Guy Gogniat, Benoit Badrignans, and Benoit Torres. Security enhancements for FPGA-based MPSoCs: A boot-to-runtime protection flow for an embedded Linux-based system. In *7th International Workshop on Reconfigurable and Communication-Centric Systems-on-Chip (ReCoSoC)*, pages 1–8, July 2012

Pascal Cotret, Jérémie Crenne, Guy Gogniat, and Jean-Philippe Diguet. Bus-based MPSoC security through communication protection: A latency-efficient alternative. In *2012 IEEE 20th International Symposium on Field-Programmable Custom Computing Machines*, pages 200–207, April 2012

Jérémie Crenne, Pascal Cotret, Guy Gogniat, Russell Tessier, and Jean-Philippe Diguet. Efficient key-dependent message authentication in reconfigurable hardware. In *Field-Programmable Technology (FPT), 2011 International Conference on*, pages 1–6, Dec 2011

Pascal Cotret, Jérémie Crenne, Guy Gogniat, Jean-Philippe Diguet, Lubos Gaspar, and Guillaume Duc. Distributed security for communications and memories in a multiprocessor architecture. In *Parallel and Distributed Processing Workshops and Phd Forum (IPDPSW), 2011 IEEE International Symposium on*, pages 326–329, May 2011

Lubos Gaspar, Viktor Fischer, Florent Bernard, Lilian Bossuet, and Pascal Cotret. HCrypt: A novel concept of crypto-processor with secured key management. In *Reconfigurable Computing and FPGAs (ReConFig), 2010 International Conference on*, pages 280–285, Dec 2010

Muhammad Abdul Wahab and Pascal Cotret. A hardware coprocessor for zynq-based dynamic information flow tracking. In *Cryptographic Architectures Embedded in Reconfigurable Devices, International Workshops on*, Jun 2016

Pascal Cotret, Guy Gogniat, Jean-Philippe Diguet, and Jérémie Crenne. Self-reconfigurable security-enhanced

communications in FPGA-based MPSoCs. In *Cryptographic Architectures Embedded in Reconfigurable Devices, International Workshops on*, Jun 2012

Pascal Cotret, Jérémie Crenne, Guy Gogniat, and Jean-Philippe Diguet. Protecting communications in bus-based MPSoCs using hardware firewalls. In *Cryptographic Architectures Embedded in Reconfigurable Devices, International Workshops on*, Jun 2011

National publications

Pierre Garreau, Pascal Cotret, Julien Francq, Jean-Christophe Cexus, and Loïc Lagadec. RISC-V Embedded AI for IDS Applications. In *RESSI 2024 : Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information*, May 2024

Nicolas Gaudin, Vianney Lapôtre, Pascal Cotret, and Guy Gogniat. Verrouillage des lignes de cache pour la lutte contre les attaques par canaux auxiliaires exploitant les mémoires caches. In *Cyber On Board*, Mar 2024

Nicolas Gaudin, Vianney Lapôtre, Pascal Cotret, and Guy Gogniat. Cache locking against cache-based side-channel attacks. In *Ecole d'hiver Francophone sur les Technologies de Conception des Systèmes Embarqués Hétérogènes (FETCH)*, Feb 2024

Quentin Ducasse, Pascal Cotret, and Loïc Lagadec. Securing a high-level language virtual machine through its ISA: Pharo as a case study. In *GDR SoC2*, Jun 2021

Valérie Viet Viem Tong, Benoît Fournier, Guillaume Fournier, Leopold Ouairy, Pascal Cotret, and Gilles Guette. Dis, c'est quoi là haut dans le ciel ? - c'est un linux, mon petit. In *Magazine MISC*, july 2019

Muhammad Abdul Wahab, Pascal Cotret, Mounir Nasr Allah Allah, Guillaume Hiet, Vianney Lapôtre, and Guy Gogniat. Monitoring information flows in heterogeneous SoCs with a dedicated coprocessor. In *GDR SoC-SiP*, june 2018

Guillaume Fournier, Paul Audren de Kerdrel, Pascal Cotret, and Valérie Viet Triem Tong. DroneJack: kiss your drones goodbye ! In *SSTIC (Symposium sur la sécurité des technologies de l'information et des communications)*, Jun 2017

Muhammad A. Wahab, Pascal Cotret, Mounir N. Allah, Guillaume Hiet, Vianney Lapôtre, and Guy Gogniat. ARMHEx: a hardware extension for information flow tracking on ARM-based platforms. In *GDR SoC-SiP*, june 2017

Muhammad Abdul Wahab, Pascal Cotret, Mounir Nasr Allah Allah, Guillaume Hiet, Vianney Lapôtre, and Guy Gogniat. ARMHEx: a hardware extension for information flow tracking on ARM-based platforms. In *RESSI 2017 (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des systèmes d'information)*, May 2017

Guillaume Fournier, Pierre Matoussowsky, and Pascal Cotret. Hit the KeyJack: stealing data from your daily wireless devices incognito. In *Journées C&ESAR 2016*, Nov 2016

Muhammad Abdul Wahab, Pascal Cotret, Mounir Nasr Allah Allah, Guillaume Hiet, Vianney Lapôtre, and Guy Gogniat. A portable approach for soc-based dynamic information flow tracking implementations. In *GDR SoC-SiP*, june 2016

Pascal Cotret, Stéphane Chevobbe, and Mehdi Darouich. Reconnaissance faciale basée sur les ondelettes robuste et optimisée pour les systèmes embarqués. In *Colloque GRETSI*, Sep 2015

Pascal Cotret, Guy Gogniat, and Jean-Philippe Diguet. Self-configuration of latency-efficient security enhancements for mpsoc communications monitoring. In *GDR SoC-SiP*, Jun 2012

Pascal Cotret, Jérémie Crenne, Guy Gogniat, and Jean-Philippe Diguet. A case study for distributed and efficient protection of communications in reconfigurable embedded systems. In *GDR SoC-SiP*, Jun 2011

Pascal Cotret, Jérémie Crenne, and Guy Gogniat. Sécurisation des communications dans une architecture multi-processeur. In *MajecSTIC (MAnifestation des JEunes Chercheurs en Sciences et Technologies de l'Information et de la Communication)*, page 163–170, Oct 2010

Pascal Cotret, Jérémie Crenne, and Guy Gogniat. Secured communications within a multiprocessor architecture. In *GDR SoC-SiP*, Jun 2010

Invited talks

Pascal Cotret. Monitoring program execution (and more) on ARM processors. In *Toulouse Hacking Convention*, pages 1–2, Mar 2018

Pascal Cotret. Towards a hardware-assisted information flow tracking approach for ARM processors. In *France/Japan Cybersecurity workshop*, pages 1–2, Mar 2016

Research reports

Guillermo Polito, Stéphane Ducasse, Pablo Tesone, Luc Fabresse, Gaël Thomas, Mathieu Bacou, Loïc Lagadec, and Pascal Cotret. Remarkable Challenges of High-Performance Language Virtual Machines. In *Research Report Inria Lille - Nord Europe*, 2022