JÉRÉMIE CRENNE

Laboratoire LIRMM
161 rue Ada
34095 Montpellier Cedex France
Téléphone : +33 (0)297874579 / Fax : +33 (0)297874527
jeremie.crenne@lirmm.fr
www.jeremiecrenne.com

SITUATION

- Chercheur postdoctoral à l'Université de Montpellier 2, Laboratoire LIRMM UMR CNRS 5506 — 2011
  Financement : ANR SecReSoC

  Sujet de recherche : ma recherche est liée aux architectures reconfigurables et parallèles. Je suis particulièrement intéressé par leur intégration dans le domaine des systèmes embarqués et aux aspects de sécurité logiciels et matériels.

FORMATION

- Doctorat Sciences et Techniques de l'Information et de la Communication, Université de Bretagne Sud (UBS) - 56100 Lorient — 2011
  Financement : Bourse ARED Région Bretagne
  Titre : Sécurité haut-débit pour les systèmes embarqués à base de FPGAs
  Mention : Très honorable
  Soutenue le 9 décembre 2011 à Lorient devant le jury composé de :

M. Olivier Sentieys	Professeur des universités, Université de Rennes 1	CNU 61	Président
M. Lilian Bossuet	Maître de conférences HDR, Université Jean Monnet	CNU 63	Rapporteur
M. Chistophe Jégo	Professeur des universités, IPB/ENSEIRB-MATMECA	CNU 61	Rapporteur
M. Russell Tessier	Professeur des universités, Université du Massachusetts	-	Examinateur
M. J.Ph Diguet	Directeur de recherche CNRS, Lab-STICC CNRS UMR 3192	-	Examinateur
M. Pierre Bomel	Docteur ingénieur de recherche, Université de Bretagne Sud	Qualifié 61 et 63	Examinateur
M. Guy Gogniat	Professeur des universités, Université de Bretagne Sud	CNU 61	Directeur

  Téléchargement des documents :

  manuscrit : www.jeremiecrenne.com/publications/2011_thesis.pdf
  présentation : http://www.jeremiecrenne.com/publications/2011_thesis_slides.pdf

- Master recherche en sciences et technologies, mention conception et gestion des systèmes électroniques d'information et de production, spécialité électronique, Rang 1er, mention bien — 2008

- Baccalauréat en sciences et technologie industrielles, spécialité génie électronique — 2003

EXPÉRIENCES PROFESSIONNELLES

- Doctorant au laboratoire en sciences et techniques de l'information, de la communication et de la connaissance (Lab-STICC) — 2008-2011
  Sujet de recherche : définition, proposition et optimisation d'unités cryptographiques adaptées pour les systèmes embarqués à base de FPGAs et compatibles haut-débit
  Direction : Professeur Guy Gogniat
  Financement : Région Bretagne (ARED)

- Participant au projet SecReSoC * — Depuis 2009
  Programme ARPEGE 2009 / Projet ANR-09-SEGI-013
  Partenaires : Laboratoire Hubert Curien, Laboratoire Lab-STICC, Laboratoire LIRMM, Département COMELEC de Telecom Paris Tech, Société NETHEOS de Montpellier
  Sujet de recherche: développement d'une architecture générique multiprocesseur permettant l'intégration dans une cible FPGA de niveaux de sécurisation des données et des traitements
  * http://labh-curien.univ-st-etienne.fr/secresoc/doku_wiki/doku.php

- Séjours de recherche de 2 fois 3 mois, au laboratoire Reconfigurable Computing Group (RCG) de l'Université du Massachusetts (UMASS) à Amherst, MA, USA — 2009 et 2010
  Sujets de recherche : Recherche et développement d'un cœur de sécurité matériel configurable, et proposition originale et optimisée du stockage du matériel cryptographique
  Direction : Pr. Russell Tessier
  Financement : École doctorale SICMA, Services des relations internationales UBS, Lab-STICC, UMASS, GDR ISIS

  Ces collaborations ont donné lieu à 3 publication communes : 1 en revue internationale ACM et 2 en conférences internationales IEEE (voir publications 1, 3, et 6). La partie authentification du cœur de sécurité est disponible en tant qu'IP complète et gratuite pour cible FPGA et sous licence BSD à l'adresse suivante : http://code.google.com/p/ghash/

- Moniteur à l'IUT, au département Génie Industriel et Maintenance à Lorient - CIES Grand Ouest — 2008-2011
  Niveau : 1ère année et apprentis
  Volume horaire total sur la période : 192 heures équivalentes TD
  Types d'enseignements : CM/TD/TP de microprocesseurs, TD/TP d'électronique numérique, TP d'électronique analogique

- Chaire de session pour la conférence FPT qui a eu lieu à New-Delhi du 12 au 14 décembre 2011.

- Rapporteur des conférences internationales (IEEE RAW 2011, IEEE FCCM 2010, ReConFig 2010, WESS 2010 et ARC 2010),

- Suppléant de Mme Ghizlane Lebreton au conseil des doctorants du laboratoire Lab-STICC — 2008-2011

COMPÉTENCES

- Architectures
  - OS : Windows, Linux
  - Systèmes reconfigurables : du gros grain au grain fin, FPGA
  - Systèmes programmables : RISC, microcontrôleur, DSP
- Langages
  - Programmation : C, C++, C#, Java, LUA, Assembleur
  - API : OpenGL, DirectX, SDL, QT
  - Description : Verilog, VHDL
- Outils CAO
  - FPGA : Altera Quartus, SOPC Builder, Xilinx ISE Fundation, XPS/EDK, PlanAhead
  - MentorGraphic : ModelSim
  - Autre : Matlab
- Anglais
  - Niveau professionnel
  - Lecture et écritures d'articles scientifiques, communication orales lors de congrès

PUBLICATIONS

- **Revue internationale (1 en publication)**

1. **J. Crenne**, R. Vaslin, G. Gogniat, J.-P. Diguet, R. Tessier et D. Unnikrishnan, Configurable Memory Security in Embedded Systems, dans la revue ACM Transactions on Embedded Computer Systems (TECS), acceptée le 9 septembre 2011, à paraître.

- **Chapitre de livre (1 publié)**

2. **J. Crenne**, P. Bomel, G. Gogniat, J.-P Diguet, End-to-End Bitstreams Repository Hierarchy for FPGA Partially Reconfigurable Systems, dans le livre Algorithm-Architecture Matching for Signal and Image Processing, Springer, ISBN: 978-90-481-9964-8, pp. 171-194.

- **Conférences internationales avec comités de lecture et actes (8 publiées)**

3. **J. Crenne**, P. Cotret, G. Gogniat, R. Tessier, and J.-P. Diguet, Efficient Key-Dependent Message Authentication in Reconfigurable Hardware, dans les actes de la conférence internatonale IEEE Proceedings of the International Conference on Field-Programmable Technology (FPT'11), 12-14 Décembre, 2011, New Delhi, Inde.

4. P. Cotret, **J. Crenne**, G. Gogniat, J.-P Diguet, L. Gaspar, G. Duc, Distributed Security for Communications and Memories in a Multiprocessor Architecture, dans les actes de la conférence internationale IEEE Reconfigurable Architecture Workshop (RAW'11), 16-17 Mai, 2011 , Anchorage, Alaska, USA.

5. G. Gogniat, J. Vidal, L. Ye, **J. Crenne**, S. Guillet, F. de Lamotte, J.-P Diguet, P. Bomel, Self-reconfigurable Embedded Systems: from Modeling to Implementation, dans les actes de la conférence internationale Engineering of Reconfigurable Systems and Algorithms (ERSA'10), 12-15 Juillet, 2010, Las Vegas, Nevada, USA.

6. D. Unnikrishnan, R. Vadlamani, Y. Liao, A. Dwaraki, **J. Crenne**, L. Gao, R. Tessier, Scalable Network Virtualization Using FPGAs, dans les actes de la conférence internationale IEEE International Symposium on Field-Programmable Gate Arrays (FPGA'10), 21-23 Février, 2010, Monterey, Californie, USA.

7. **J. Crenne**, P. Bomel, G. Gogniat, J.-P Diguet, UDP Partial Bitstreams Diffusion Through WLAN, dans les actes de la conférence internationale Design and Architectures for Signal and Image Processing (DASIP'09), 22-24 Septembre, 2009, Sophia Antipolis, France.

8. J.-P Diguet, L. Ye, Y. Eustache, **J. Crenne**, P. Bomel, G. Gogniat, J. Vidal, F. de Lamotte, Networked Self-adaptive Systems: An Opportunity for Configuring in the Large, dans les actes de la conférence internationale Engineering of Reconfigurable Systems and Algorithms (ERSA'09), July 13-16, 2009, Las Vegas, Nevada, USA.

9. P. Bomel, **J. Crenne**, L. Ye, G. Gogniat, J.-P Diguet, Ultra-Fast Downloading of Partial Bitstreams Through Ethernet, dans les actes de la conférence internationale Architecture of Computing Systems (ARCS'09), 10-13 Mars, 2009, Delft, Hollande.

10. P. Bomel, G. Gogniat, J.-P Diguet, **J. Crenne**, Bitstreams Repository Hierarchy for FPGA Partially Reconfigurable Systems, dans les actes de la conférence internationale IEEE International Symposium on Parallel and Distributed Computing (ISPDC'08), 1-5 Juillet, 2008, Cracovie, Pologne.

- **Conférences nationale avec comités de lecture et actes (1 publiée)**

11. P. Cotret, **J. Crenne**, G. Gogniat, Sécurisation des communications dans une

architecture multi-processeurs, dans les actes de la conférence MAnifestation des JEunes Chercheurs en Sciences et Technologies de l'Information et de la Communication (MajecSTIC'10), Octobre 14, 2010, Bordeaux, France.

COMMUNICATIONS

1. Efficient Key-Dependent Cryptographic Message Authentication in FPGA, Poster pour le congrès GDR System-On-Chip System-In-Package (SOC-SIP), 15-17 Juin, 2011, Lyon, France

2. Securing External Shared Memory in Embedded Systems, Poster pour le congrès GDR System-On-Chip System-In-Package (SOC-SIP), 9-11 Juin, 2010, Paris, France

3. J'ai besoin de sécurité ! Ou comment protéger nos gentilles données des affreux méchants ?, Poster de vulgarisation pour le congrès rencontre des jeunes chercheurs du Grand Ouest (CIES), Élu meilleur poster par les lycéens (1er sur 200), 27-28 Mai, 2010, Rennes, France

4. Securing External Shared Memory in Multi-FPGA Context, J. Crenne, R. Tessier, P. Cotret, G. Gogniat, J.-P. Diguet, Communication pour le workshop Cryptographic architectures embedded in reconfigurable devices (CryptArchi), 27-30 Juin, 2009, Paris, France

5. IEEE 802.11 WIFI Partial Bitstreams Diffusion, Poster pour le congrès GDR System-On-Chip System-In-Package (SOC-SIP), 10-12 Juin, 2009, Paris, France

6. Déploiement de systèmes matériels à la demande : de l'idée à la mise en œuvre, Démonstrateur pour la Journée Image et Systèmes Embarqués (JISE), 12 Mai, 2009, Rennes, France

7. De la puce à ses applications : les technologies de l'information et de la communication nous entourent, Présentation pour la fête de la science, 16-22 Novembre et 17-23 Novembre, 2009, Lorient, France

ENSEIGNEMENTS

- **Microprocesseurs** CM/TD/TP (60h eq. TD) / IUT 1ère année et apprentis

  - Architectures et programmation à base de microcontrôleur 80537
  - Étude des interruptions, compteurs, convertisseurs CAN, CNA et du port série

- **Electronique numérique** TD/TP (84h eq. TD) / IUT 1ère année et apprentis

  - Numération et codage
  - Algèbre de Boole
  - Analyse et conception de systèmes combinatoires
  - Analyse de systèmes séquentiels
  - Analyse et conception de compteurs synchrones et asynchrones

- **Électronique analogique** TP (48h eq. TD) / IUT 1ère année

  - Utilisation de l'oscilloscope
  - Filtres passifs du 1er et 2ème ordre
  - Filtre actifs
  - Amplificateurs opérationnels en régime linéaire en non linéaire

- **Projet de VHDL** TP (20h) / M1 GEII

  - Analyse et conception d'une IP de compression/décompression Lempel-Ziv-Welch (LZW)

- **Encadrement de stagiaires**

  - Cédric Séguin, Master 2 recherche électronique, UBS, Architecture reconfigurable et sécurité. Le but de ce projet était de proposer une architecture reconfigurable sécurisée pour le chargement de bitstreams complets ou partiels.

  - Noufel Belfathi, Master 1ère année électronique, UBS, Multithreading avec le noyau Xilkernel sur une architecture MPSOC. Le but de ce projet était d'évaluer la suite de benchmarks PARSEC sur une architecture à base de multiples processeurs synthétisables Microblaze.

  - Amine Chaoui, Master 2 recherche électronique UBS, Reconfiguration dynamique partielle sur processeur synthétisable Microblaze. Le but de ce projet était de porter une plateforme de reconfiguration dynamique partielle ayant pour architecture un processeur PowerPC en dur, vers une architecture avec processeur synthétisable Microblaze.