Job offer: postdoctoral Fellow

Project Title: Design and prototype of a coarse-grained reconfigurable and secured crypto-processor

Research Fields: CGRA, cybersecurity, asymmetric cryptography, physical attacks, side-channel, reconfigurable architectures

Work Place: Lorient-France + Singapore

Research Laboratory(ies): Lab-STICC/Université de Bretagne Sud + Nanyang Technological University

UBL Research Department: NUMERIC

Head(s) of the Scientific Project: Philippe COUSSY

Offer type: postdoctoral researcher (short term contract, 12 months, possibly once renewable)

Hiring Institutions: Université de Bretagne Sud + Nanyang Technological University

Application deadline: 2017, August 20

Job Starting Date: Sept. 2017

Environment

University of South Brittany (Université Bretagne Sud)

University of South Brittany (Université Bretagne Sud) was founded in 1995. It is a multidisciplinary institution with 3 main campuses located in Lorient, Vannes and Pontivy, Brittany, France. It offers academic programs from bachelor’s level to the doctorate in different areas: humanities, social sciences, engineering, computer science, biochemistry, mathematics, law, economics and business. It has developed recognized research skills in 4 majors fields: materials, costal and marine studies, social usages and practices, IT.

Lab-STICC (UMR CNRS 6285)

Created since 2008, the Lab-STICC is a multidisciplinary research laboratory in the field of Information and communication science and technology. Researchers work in a single structure within one central theme: “from sensor to knowledge”. The Lab-STICC is a research unit of the French national center for scientific research (CNRS) involving two universities (Université de Bretagne Occidentale, Brest; Université de Bretagne Sud, Lorient) and three graduate schools of engineering (Telecom Bretagne, ENSTA Bretagne and ENIB).

The Lab-STICC incorporates more than 560 people including 280 permanent staff, 220 PhD students and 60 non-permanent positions. The staffs are located over the different institutes on several geographical sites in Brittany: Brest, Lorient, Rennes, Quimper and Vannes.

In the Lab-STICC, The MOCS team carries out research on Hardware/Software Design Methodologies and Tools in the domain of embedded systems. The global project is to define a design continuum between applications embedded software, CAD tools and hardware architectures, it continues with embedded self-adaptation capacities.
Nanyang Technological University

Young and research-intensive, Nanyang Technological University (NTU Singapore) is ranked 11th globally (QS World University Ranking 2018). It is also the world’s top young university. The university has colleges of Engineering, Business, Science, Humanities, Arts, & Social Sciences, and an Interdisciplinary Graduate School. It also has a medical school, Lee Kong Chian School of Medicine, set up jointly with Imperial College London. NTU is also home to world-class autonomous entities such as the National Institute of Education, S Rajaratnam School of International Studies, Earth Observatory of Singapore, and Singapore Centre on Environmental Life Sciences Engineering. NTU provides a high-quality global education to about 33,000 undergraduate and postgraduate students. The student body includes top scholars and international olympiad medallists from the region and beyond. Hailing from 80 countries, the university’s 4,300-strong faculty and research staff bring dynamic international perspectives and years of solid industry experience.

Mission (scientific project)

Some professional and government applications requiring a high-level of security use asymmetric cryptosystems based on elliptic curves (e.g. ECDSA and ECDH on 256 to 600 bits), RSA or Diffie-Hellman (2048 to 8192 bits). The use of these cryptosystems with very large data / parameters gives a high degree of security against theoretical attacks (in 2009, a factorization record of a RSA number of 768 bits was established, current studies aim at 1024 Bits for the next few years). Optimized hardware accelerators are required to support the many arithmetic calculations on data of several hundred or even thousands of bits. When cryptosystems are embedded or buried in accessible electronic devices, they must also be protected against physical attacks. For example, attacks by observation (analysis of computation time, energy consumed or electromagnetic radiation) make it possible to retrieve secret information from external observation of the circuit.

Purely software-based implementations using processors are very flexible, but much slower and energy-intensive than purely hardware-based ASICs. FPGA implementations offer a flexibility / performance compromise. However, this flexibility comes at the cost of very large configuration files that should be protected and stored in the cryptosystem. The goal of this project is to design a secure crypto-processor against side channel attacks. The proposed crypto-processor is a programmable hardware accelerator that provides asymmetric cryptographic primitives. The processor architecture will be based on a technological brick reconfigurable at coarse grain (called CGRA for Coarse Grain Reconfigurable Array) and its compiler, both developed for other needs and non-security domains [1] - [6]. This architecture will allow achieving performances close to those of the ASICs and a flexibility / programmability similar to those of the processors without having the disadvantages of the FPGA implementations.

Bases of this architecture and its associated compilation tool [1] [2] have been proposed in the PhD. thesis of T. Peyret [3] which also lays down bases for the reliability of the calculation elements of the architecture. The architectural solution of S. Das, called IPA for Integrated Programmable Accelerator [5], extends the work of T. Peyret on the architecture and on the compilation flow [4]. It is capable of running an average of 507 MOPS with an energy efficiency of 142 MOPS / mW at 0.6V, surpassing six times the performance and ten times the energy efficiency of an ultra-low power OR1K processor. The IPA also surpasses the state-of-the-art CGRA architectures in the field of video surveillance: for the same processing, the IPA requires 1.6 times less cycles per pixel [6].

The excellent performances we have obtained for applications in the field of signal and image processing lead us to believe that this architectural brick once adapted will improve the security of certain cryptographic devices while controlling their cost and consumption energy. The adaptations will concern the architecture of the calculation grid and the elements of calculation (choice of type, number and positioning of the elements) of the IPA and its dynamic reconfiguration module ("just-in-time compilation"). They will make it possible to execute more complex cryptographic algorithms and to limit the behavioral signature (temporal, current, etc.) of the crypto-processor.
Scientific program

The post-doc program consists of three major stages. The first step is familiarization with asymmetric cryptography, the operations involved in implementing some cryptographic primitives, and the architecture and compilation flow of the existing CGRA. The second part of the work consists in physically designing the new operators to be integrated into the CGRA. Finally, the last step is the modification of the compilation tool to exploit the new material available. We will evaluate the performance (speed, surface, energy) and the security to the main hidden channel attacks.

Required Profile

Doctor (PhD) in hardware design, cybersecurity, reconfigurable computing, maximum 3 years of experience after thesis defense\(^1\). An international experience in research is required (during or after Doctorate). Candidates must not have supported their thesis in the hiring institution and not previously worked in the host research unit.

Useful References


[5] Satyajit Das, Kevin J. M. Martin, Philippe Coussy, Davide Rossi, Luca Benini: Efficient mapping of CDFG onto coarse-grained reconfigurable array architectures. 22nd Asia and South Pacific IEEE Design Automation Conference (ASP-DAC), 2017


How to apply?

Please send the following documents by email to : Philippe COUSSY philippe.coussy@univ-ubs.fr + cc to UBL recherche@u-bretagneloinre.fr :

- Short Curriculum Vitae and a covering letter showing your interest and especially addressing your professional project

---

\(^1\) The thesis defense must have taken place after 31/08/2014, except in rare exceptions. Periods of sickness, maternity or parental leave shall not be counted in this 3 years period.
- A list of your major works (2 pages max.): scientific publications, patents and others scientific productions
- Letters of recommendation (not required)
- A copy of your PhD diploma

The general selection process is described here: [https://u-bretagne-loire.fr/dossiers/postdoc/candidatures](https://u-bretagne-loire.fr/dossiers/postdoc/candidatures)

Two interviews will be organized for this job offer.

**Further information**

This Fellowship is cofunded by Université Bretagne Loire and Nanyang Technological University, Singapore

The Université Bretagne Loire federates 7 universities, 15 “grandes écoles” and 5 research organizations in the West of France (Bretagne and Pays de la Loire). This community of universities and institutions aims to develop the scientific and academic potential of this territory at national and international level.

Nanyang Technological University (NTU Singapore) is ranked 13th globally and the world’s top young university.

---

2 For doctors graduated from a French establishment, a link to the thesis notice in the SUDOC Catalogue or the French official portal Theses.fr is sufficient.