Securing External Shared Memory in Multi-FPGA Context

(Abstract)

Jérémie Crenne [†], Russel Tessier [‡], Pascal Cotret [†], Guy Gogniat [†] and Jean-Philippe Diguet [†]

[†] LabSTICC Laboratory CNRS UMR 3192 Université de Bretagne Sud UEB Lorient, France
[‡] Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, MA USA

{jeremie.crenne, pascal.cotret, guy.gogniat, jean-philippe.diguet}@univ-ubs.fr, tessier@ecs.umass.edu

As CPUs are not getting faster easily, it's now a common practice to multiply the number of processor cores. Plenty of architectures propose to handle properly an increasing number of possible applications into one device. FPGA is a well known technology that can help in acceleration by taking advantage of the reconfiguration of the chip and by exploiting pipeline at fine-grain parallelism. Acceleration can be up to 2 or 3 orders of magnitude. Supercomputers and clusters try to enhance this factor by exploiting coarse grain parallelism. Large-Scale computing solutions are divided in 3 classes: class 1 embeds supercomputers or clusters of workstations, with up to 10-10^5 CPUs. Class 2 corresponds to hybrids networks of CPUs and FPGAs. Class 3 deals with network of FPGAs only. From this last class, trends show that in the future, numbers of FPGAs could be embedded in a single handled device. In addition, embedded multi-core in handled systems is starting to become a common practice to unleashed intensive computation and provide "true" parallelism even for public consumers. Advancement in ambient and cloud computing for civil users leads also to an over-communicating world. More and more private data will be embedded (banking, heath or secret data) and subject to be broadcast anywhere. By the intrinsic nature of this information, it gives also a difficult but needed challenge: security.

We propose to deal with multi-core designs security in multi-FPGA context where the goal is to protect external shared memories against spoofing, relocation and replay attack. Our threat model considers the FPGA to be the only secure and trusted entity. All other peripherals (buses, memories) are thus unsecure and un-trusted. As we target embedded devices, all used resources have to be minimized. Area cost, latency, throughput and especially power consumption are centric. These parameters are generally admitted to be the most important and thus must be taken into consideration to build a secure robust design.

In this talk, we will first presents a simple secure multi-core architecture in multi-FPGA context fitted for low cost devices such as Spartan family. Fundamentally, the use of two well known authentication modes AES-CMAC and AES-GCM as security primitives will be weighted and an exhaustive comparison will be given. We will secondly review state of the art techniques to avoid cache coherency issue due to shared memories in multi core context and discus its feasibility for embedded systems.