Smart and low-cost RISC-V platform for cybersecurity

Duration : 3 years
Starting date : Autumn 2020
Institution : Laboratory Lab-STICC (UMR 6285) - ENSTA Bretagne, Brest
Application deadline : Open until filled
Restrictions : The candidate must be from the European Union

1 Abstract

This project aims to develop a computing architecture, based on RISC-V, for the IoT market with AI features aimed for cybersecurity applications. This architecture will be in line with RISC-V architectures, currently very promising from both academic and industrial point of views.

2 Thesis description

The main goal is to get well-tailored capacities in an *edge computing* context where computations (data fusion, analysis and processing) are performed on embedded nodes (which are constrained systems). These nodes are distributed around networks, they have a low communication rate as they transmit locally-processed data instead of raw data. This approach differs from *cloud computing* which relies on highly-connected centralized infrastructures.

Nodes must take target applications into account in order to get high performances while specifying their architecture. However, this architecture must also be easily adjustable for any other new application.

As mentioned before, the target architecture will be an embedded platform. In a nominal use, it allows to share the computing power over visible nodes (communications may be point-to-point), dynamic tasks allocation (sleep mode, performance/battery trade-off). The target has enough computing power to operate as a standalone unit (resilience in a damaged environment or with partial connectivity).

We will target use cases where a multi-source data analysis is needed for cyber-related situations :

— Occurrence of rare or unusual events in an infrastructure composed of several units (for instance, buildings in a port installation). For instance, we will look for identifying known scenarios or inconsistencies in captured data.

— In a military context, it may be a real-time monitoring solution of seagoing units in a restricted area where their behavior may indicate it can be considered as an enemy.

In order to benefit from a “non-specialized” architecture, a simple, low-power and adjustable processor is needed, with an “open source” software stack. In order to customize the architecture according to target applications, the approach consists in adding extensions to this processor :

— In particular, efficient *deep learning* features.

— Potentially, internal security mechanisms in order to avoid the processor from being compromised.

These architectures must be able to learn, process data and transmit diagnostics. It implies a high complexity during the development cycle as well as during runtime verification. Debug capabilities must be taken into account from the beginning. One of the main concern of such platforms is to keep a rational cost to deploy them "massively". The *edge computing* approach assumes indeed the presence of several architecture instances, such instances must be considered as consumable objects : for instance, in a military environment, it will consist in deploying several nodes aiming to perform a real-time tracking of enemy units.

3 Thesis plan

3.1 Hypothesis

The *edge computing* challenge consists in including the processing power as close as possible to the final user for performance, confidentiality and battery life purposes. For embedded industrial products, it means that power consumption is as important as the overall chip performance.

3.2 Methodology

In order to get enough computing power, especially for *deep learning* nodes, we want to add a dedicated unit to a RISC-V core. RISC-V architectures are excellent candidates for embedded applications as their instruction set is open and extensible. There are several RISC-V implementations (32 or 64-bits, accepting more or less complex operations...). From our point of view, a CGRA architecture (Coarse-Grain Reconfigurable Array) is a good candidate in our context : lower consumption compared to a multicore thanks to the reconfiguration mechanism, easier to program than an FPGA for CAD tools thanks to operators, flexible enough to implement intensive computations or to improve the chip reliability via behavior monitoring of the RISC-V core. Our research group at ENSTA Bretagne has RISC-V and CGRA knowledge (coding design tools and implementing such architectures).

3.3 Scientific environment

In our project, we will design an open and lasting architecture including a RISC-V core and a CGRA. Later on, it will be extended to a multicore version. A full architectural exploration environment will allow to study design approaches ; it will also evaluate the best parameters set according to performances and power consumption of the target application.

The same tools will generate code to produce a chip. Programming tools, based on standard specifications, will adapt to any architectural variant. Experimentations will use the Zebu equipment (chip emulator acquired for the team in 2018), it will give a significant advantage to study circuit complexity and to improve tests speed. Application tests will focus on local *deep learning* nodes aiming to characterize signals (radio, image) and detection of abnormal behavior. Use cases will be given by an industrial partner and related to maritime activities.

3.4 Thesis organization

The first year will be focused on two actions :

1. Study of the state-of-the-art of RISC-V variants ([Ext1]), simulation ([Ext2, Ext3]) and generation environments ([Ext4], [Int1], etc.) as well as possible extensions [Int2, Int3]. The candidate will study both academic and industrial solutions.
2. Acquiring experience with tools (for instance, HLS [Int4, Int5], but also ARGEN [Int6] and the CGRA generation environment) and infrastructures available in the lab (Xilinx FPGA boards, Zebu hardware emulator).

The second year will be devoted to the conception of the architecture and related tools : it will be relevant for architectural exploration and generation. At the end of the first year, an article will be submitted with preliminary results on a use case given by an industrial partner : it will assess benefits compared to a conventional architecture.

In the third year, the approach will be generalized and hardened. Several publication targets will be taken into account : AI-related journals where we will claim an architecture with computation speed improvements, Transactions journals related to reconfigurable architectures, IoT-related journals and contributions in the RISC-V community. Of course, the last part of the thesis will be devoted to the manuscript writing.

3.5 Thesis supervision

The thesis will be supervised by Loïc Lagadec, professor at ENSTA-Bretagne, and co-supervised with Dr. Pascal Cotret and Dr. Jean-Christophe Cexus. Permanent staff involved in this thesis complement one another. At ENSTA-Bretagne, Loïc Lagadec has a strong expertise in programming/synthesis tools development for reconfigurable architectures (FPGA and/or CGRA). Pascal Cotret is an expert for developing applications on such architectures and is involved for several years in the RISC-V community. Jean-Christophe Cexus is an expert in signal processing and AI.

3.6 Partnership

This thesis takes place in the context in the cyberdefense of naval systems chair, but also addresses a community in development (embedded systems based on RISC-V) : this community gathers well-known industrial partners such as Thales, and academics.

3.7 Publications

Publications will mainly be between architectures (Transactions on CAD, Transactions on Embedded Computing Systems, Journal of Systems Architecture and conferences such as DATE, FPL, etc.) and “Edge computing” networks (Transactions on emerging telecommunications technologies).

3.8 Expectations about the candidate

The candidate must have a Master degree or equivalent. He/she will present his/her knowledge in fields related to the project (IoT, AI, reconfigurable architectures, software) with a priority on AI to ensure a full complementarity with current expertise within ENSTA Bretagne.

4 Contacts

Documents to be transmitted : curriculum, diplomas, grades, motivation and recommendation letters.

— **PhD director :** Prof. Loïc Lagadec, `loic.lagadec@ensta-bretagne.fr`
— **Advisor #1 :** Dr. Pascal Cotret, `pascal.cotret@ensta-bretagne.fr`
— **Advisor #2 :** Dr. Jean-Christophe Cexus, `jean-christophe.cexus@ensta-bretagne.fr`

Références internes

[Int1] Junya Miura, Hiromu Miyazaki, and Kenji Kise. A portable and Linux capable RISC-V computer system in VerilogHDL. 2020. `https://arxiv.org/pdf/2002.03576.pdf`.

[Int2] M. A. Wahab, P. Cotret, M. N. Allah, G. Hiet, V. Lapôtre, and G. 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, 2017.

[Int3] Youenn Corre, Jean-Philippe Diguet, Dominique Heller, Dominique Blouin, and Loïc Lagadec. Tbes : Template-based exploration and synthesis of heterogeneous multiprocessor architectures on fpga. *ACM Trans. Embed. Comput. Syst.*, 15(1), January 2016.

[Int4] E. Fabiani, L. Lagadec, M. B. Hammouda, and C. Teodorov. Asserting causal properties in high level synthesis. In *2017 IEEE 2nd International Verification and Security Workshop (IVSW)*, pages 111–116, 2017.

[Int5] M. B. Hammouda, P. Coussy, and L. Lagadec. A unified design flow to automatically generate on-chip monitors during high-level synthesis of hardware accelerators. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 36(3) :384–397, 2017.

[Int6] Mohamad Najem, Théotime Bollengier, Jean-Christophe Le Lann, and Loïc Lagadec. Extended overlay architectures for heterogeneous fpga cluster management. *Journal of Systems Architecture*, 78 :1 – 14, 2017.

Références externes

[Ext1] RISC-V. Risc-v international. 2020. `https://riscv.org/`.

[Ext2] Morten Borup Petersen. Ripes. 2020. `https://github.com/mortbopet/Ripes`.

[Ext3] RISC-V. Spike RISC-V ISA Simulator. 2020. `https://github.com/riscv/riscv-isa-sim`.

[Ext4] Codasip. RISC-V processor verification. 2020. `https://www.testandverification.com/wp-content/uploads/2017/Verification_Futures/Marcela_Zachariasova_Codasip.pdf`.