Politecnico di Torino

ELECTRICAL, ELECTRONICS AND COMMUNICATIONS ENGINEERING

Maxim Integrated Products - RISC-V Cores for low-power embedded systems for consumer applications

Funded By	Maxim Integrated Products Ltd [P.iva/CF:02639670963]

Supervisor	MASERA GUIDO - guido.masera@polito.it

Contact	MASERA GUIDO - guido.masera@polito.it Fraternali Fabrizio

Context of the research activity	The aim of the research is to study technology solutions for the adoption of low-end RISC-V micro-controllers in consumer applications. Although this market is currently being served by both x86 and Arm architectures, industry is showing a growing interest towards a viable, open processor alternative. However, the real adoption of RISC-V cores in commercial products requires adequate support in terms of stability, protected execution, and tool chain availability.

	The proposal of RISC-V cores has marked a significant departure from traditional closed-source processor designs. First, the RISC-V proposal is an open-source ISA, which is freely available for anyone to use, modify, and implement. This element fosters collaboration and innovation in processor development. Second, the RISC-V design is modular, scalable and customizable. This structure enables designers to implement architectures precisely tailored around their specific application needs. This adaptability is particularly advantageous in diverse computing environments where one-size-fits-all solutions may fall short. Moreover, the open-source design allow developers getting around the long negotiates on licenses and intellectual property, so enabling a faster time-to-market for new products. Finally, the availability of a worldwide community of contributors facilitates the fast and continuous improvement of RISC-V technologies. In this scenario of rapid growth and innovation, the primary objective of the PhD is to follow and contribute to two European projects related to the development and applications of RISC-V cores in the industrial field: TRISTAN and ISOLDE. The EU-funded TRISTAN project aims to expand and develop RISC-V architecture in Europe so that is able to compete with existing commercial alternatives. This open specification eliminates the need to learn and create unique ecosystems for each processor architecture, increasing productivity, security and transparency. The ISOLDE Project will develop high

Objectives	performance RISC-V processing systems and platforms at least at TRL 7 for the vast majority of building blocks, demonstrated for key European application domains such as automotive, space and IoT. A second major research objective of the PhD program is to investigate on a RISC-V Trusted Execution Environment. A large number of applications require some level of customization to better fit their application in terms of data processing or data transfer, once the silicon is on the market. The best answer to this need is to leave the customers the possibility to write their own code to be executed by the embedded micro-controller. However, such RISC-V applications require strong hardware security, and hardware-enforced software-defined separation for secure domains, with full control over data, programs and peripherals. A Trusted Execution Environment (TEE) is a technology that provides hardware-enforced isolation within a processor allowing an application to run in a separate and protected execution area. A third research topic is the design of a RISC-V ECDSA (Elliptic Curve Digital Signature Algorithm) authentication system. Symmetric authentication systems rely on secret keys, which must be exchanged and protected. A better alternative is based on systems where all participating devices have a pair of keys called “private key” and “public key.” The private key is used by the originator to sign a message, and the recipient uses the originator’s public key to verify the authenticity of the signature. If a message is modified on its way to the recipient, the signature verification fails because the original signature is not valid for the modified message. Starting from an existing ECDSA hardware accelerator, it is intended to design a RISC-V-based authentication unit capable of improve the system flexibility, while offering the required performance level. Additionally, the designed authentication unit will share processing and storage resources with other functions of the overall system.

Skills and competencies for the development of the activity	In order to effectively contribute to the research activity, the candidate should have a good back ground in the following fields: 1-Digital circuit design 2-ASIC design flow 3-Computer architecture and micro-controllers 4-Firmware development.