RUST-Encoded Stream Ciphers on a RISC-V Parallel Ultra-Low-Power Processor

Location: Room **Durat**

Scheduled time: **11:30 – 12:15**

Speaker: Francesco Barchi

Adjunct professor at the University of Bologna, he conducts his research in the field of embedded systems. His research interests focus on using machine learning to optimise compilation phases and optimising problems for cyber-physical systems (CPS) composed of heterogeneous architectures. He obtained his PhD in Computer Engineering at the Polytechnic University of Turin. During his PhD, he worked on mapping Spiking neural networks on the SpiNNaker neuromorphic platform by developing an optimised communication middleware for the same architecture. He currently focuses his research on vertical applications of embedded architectures involving infrastructure monitoring and the development of middleware for RISC-V architecture-based SoCs for cyber-physical systems. Engaged in national and international research projects, he collaborates with several international research institutes.

Abstract

Nowadays, the development of security applications is a relevant topic in the Internet of Things (IoT) and cyber-physical systems (CPS) fields. Different embedded architectures have been adopted in these areas, but the RISC-V parallel ultra-low-power (PULP) architecture stands out as a particularly efficient system. However, it has never been proposed to enable cryptography. In the context of video stream security, stream ciphers enable an efficient solution to ensure data privacy, and the exploitation of the PULP multi-core accelerator cluster paves the way to an efficient implementation of these ciphers.

In this paper, we exploit the capability of the PULP architecture coupled with the code safety provided by the RUST programming language to design and implement an efficient stream encryption algorithm. We present a wrapper system between the development libraries of a PULP platform enabling the secure execution of a verified RUST-written implementation of ChaCha20 and AES-CTR, targeting a microdrones-based video surveillance system. Experimental tests have resulted in an encryption efficiency of ChaCha20 of 2.3

cycles per Byte (cB), placing the resulting implementation at the state-of-the-art, in direct competition with higher-class architectures like Apple M1 (2.0 cB).