THESES PROPOSALS

Thesis proposals to be carried out at HEAPlab and/or in collaboration with other research groups at DEIB and external companies are listed below. Links to useful information are provided for each thesis proposal. You may contact me by e-mail for further discussion.

FPGA-BASED IMPLEMENTATION OF LATTICE-BASED POST-QUANTUM CRYPTOSCHEMES

Quantum computing is expected to break the traditional public-key cryptography solutions in the next decades, making it paramount to design new security solutions that can also resist attacks carried out by quantum computers.
Post-quantum cryptography (PQC) aims to design cryptoschemes that can be deployed on traditional computers and that can resist against both traditional and quantum attacks.
The deployed PQC solutions will have to satisfy not only security requirements, but also performance ones. Providing an effective hardware support is paramount to ensuring a wide adoption of post-quantum security solutions across scenarios ranging from HPC to edge devices.
CRYSTALS-Kyber and CRYSTALS-Dilithium are lattice-based PQC cryptoschemes, both part of the same CRYSTALS (Cryptographic Suite for Algebraic Lattices) family and based on hard problems over module lattices, accepted for standardization by USA's NIST.

The thesis foresees designing a hardware accelerator targeting FPGAs to support the CRYSTALS-Kyber key encapsulation mechanism and the CRYSTALS-Dilithium digital signature scheme in a single RTL design.

Tags: *hardware design, post-quantum cryptography, lattice-based cryptography, hardware acceleration, FPGA*

HARDWARE DESIGN OF A SUPERSCALAR AND/OR OUT-OF-ORDER CPU ON FPGA TARGETS

Superscalar processors can concurrently execute multiple instructions, i.e., they can simultaneously dispatch multiple instructions to different execution units, thus implementing instruction-level parallelism within a single processor.
Out-of-order processors can execute instructions out of the original order, looking ahead across many instructions to issue independent ones as fast as possible while satisfying the dependencies and thus guaranteeing that the program produces the expected result.

The thesis foresees designing a superscalar and/or out-of-order CPU for FPGA targets, starting from an existing FPGA design of a single-core, in-order RISC-V CPU.

Tags: *hardware design, CPU, superscalar, out-of-order, FPGA, RISC-V*

DESIGN OF HARDWARE CACHE COHERENCE ON MULTIPROCESSOR SOCS ON FPGA

Cache coherence is the uniformity of shared resource data stored in multiple local caches. When multiple processors in a multiprocessor system maintain caches of a shared memory resource, problems may arise with incoherent data.

The thesis foresees integrating a set of already-developed cores within a multiprocessor system on an FPGA target and developing a hardware mechanism for maintaining cache coherence within the multiprocessor, leveraging existing CPU and SoC developed in-house.

Tags: *hardware design, CPU, cache coherence, FPGA, RISC-V*

ML-DRIVEN EXPLORATION OF SYNTHESIS AND PLACE-AND-ROUTE DIRECTIVES OF COMMERCIAL EDA TOOLS

Synthesis is a process by which a register transfer level (RTL) description of the desired circuit behavior, specified in a hardware description language (HDL), e.g., Verilog and VHDL, is turned into a design netlist in terms of logic gates. *Place-and-route* consists in placing all the logic elements within the resources available on the FPGA (placement) and then connecting the placed components through the wires (routing).
The available commercial electronic design automation (EDA) tools provide an extensive set of directives to optimize different aspects of the hardware design, such as resources utilization, power consumption, and timing, within both the synthesis and place-and-route processes.

The thesis foresees exploring the different synthesis and place-and-route directives of a commercial EDA tool (Xilinx Vivado) and evaluating their impact on the hardware quality metrics when applied to a variety of IP components, such as CPUs, hardware accelerators, and HLS-designed cores, on a Xilinx FPGA target. The exploration will be driven by exploiting machine learning techniques.

Tags: *electronic design automation, synthesis, place-and-route, machine learning, FPGA*