EPFL-Inria
INTERNATIONAL LAB

EPFL Inria

Workshop EPFL-Inria
November 23 and 24, 2023, Lyon

***Clement Pit-Claudel*,** EPFL
" Building systems that we can trust: compilers, semantics, and tooling for end-to-end verified systems-cost Privacy-aware Decentralized Learning »

Abstract:
Computer systems play a crucial role in our lives yet cannot be fully trusted, in part due to the persistence of software and hardware bugs. Beyond costs and lost revenue, these bugs put our privacy, our well-being, and sometimes even our lives at risk.

Writing systems in high-level programming languages increases developer productivity and eliminates common sources of errors, but compilers for these languages often produce relatively slow code. As a result, critical systems are still typically written in low-level languages - and remain full of bugs.

In this talk, I will discuss my efforts to build fast systems verified from end to end, starting from requirements formulated in high-level mathematical terms and deriving assembly code with uncompromising performance, backed by machine-checked proofs of correctness. The key component of this approach is a new way of phrasing program compilation as an existentially quantified proof-search problem; this enables users to customize their compilers and build systems in expressive languages without paying steep performance penalties.

Then, because pure-software verification cannot protect against hardware bugs, I will describe recent efforts to characterize the semantics of rule-based hardware-design languages and develop compilers, verification technology, and simulators for hardware systems.

Finally, as part of a vision to make verification and formal methods a standard part of critical software and hardware development, I will describe my efforts to make verification work more approachable, focusing on tools to help developers craft and comprehend mechanized proofs.