Toward Trusted 3rd-Party Microprocessor Cores: A Proof Carrying Code Approach

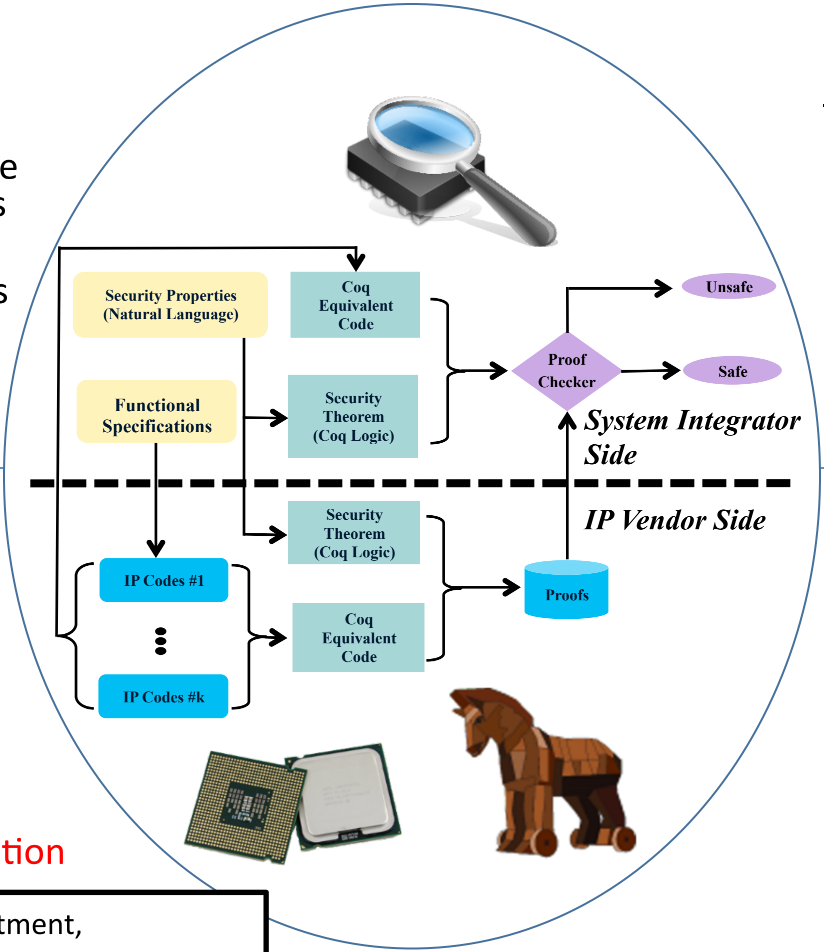
Challenges:

- Increasing number of third-party vendors have raised security concerns in soft IP industry.
- Existing formal methods are often not scalable.

Solutions:

- Hardware-Software Boundary Elimination
- Hierarchy-Preserving Formal Verification
- Theorem Proving and Model Checking Integration

NSF-1319105, PI: Dr. Yier Jin, ECE Department, University of Central Florida, yier.jin@eecs.ucf.edu
NSF-1318860, PI: Dr. Yiorgos Makris, EE Department, University of Texas at Dallas, yiorgos.makris@utdallas.edu



Scientific Impact:

- Provide formal proofs for microprocessors and SoCs security validation.
- Prevent various hardware-level attacks.

Broader Impact:

- Protect the whole SoC design flow from malicious attacks.
- Increase the security awareness of IP/IC users.
- Undergraduate research opportunities and hardware security courses development (graduate and undergraduate).