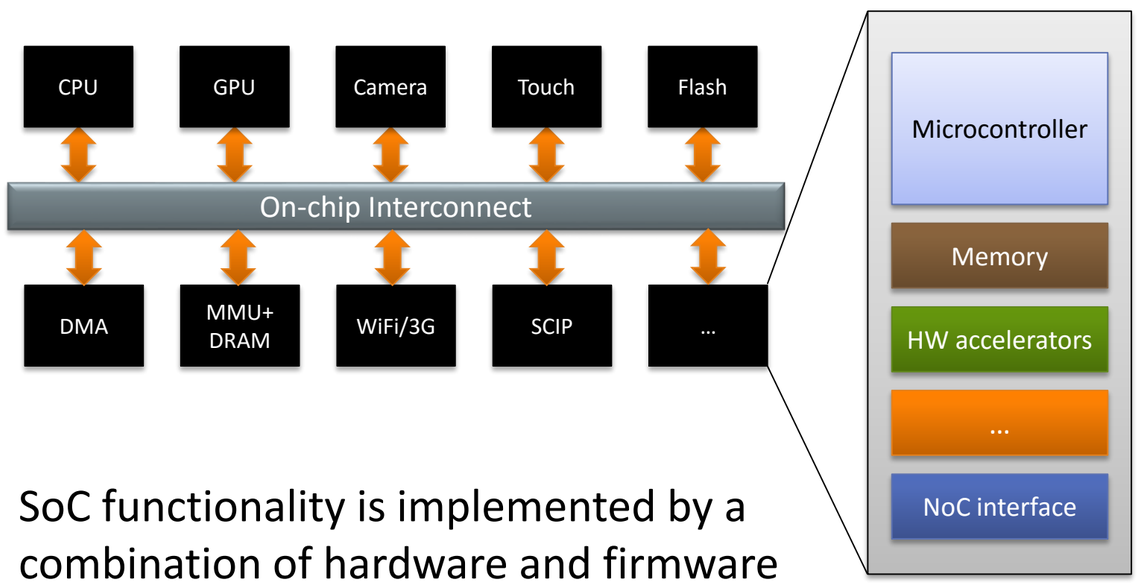
Specification and Scalable Verification of Security Properties in Contemporary SoCs

FMCAD 2015 Student Forum | Pramod Subramanyan | psubrama@princeton.edu | PRINCETON UNIVERSITY

System-on-Chip Verification



SoC functionality is implemented by a combination of hardware and firmware

Verification Challenges

- Verifying the complete HW+FW design is not scalable
- Separate verification of HW and FW misses bugs

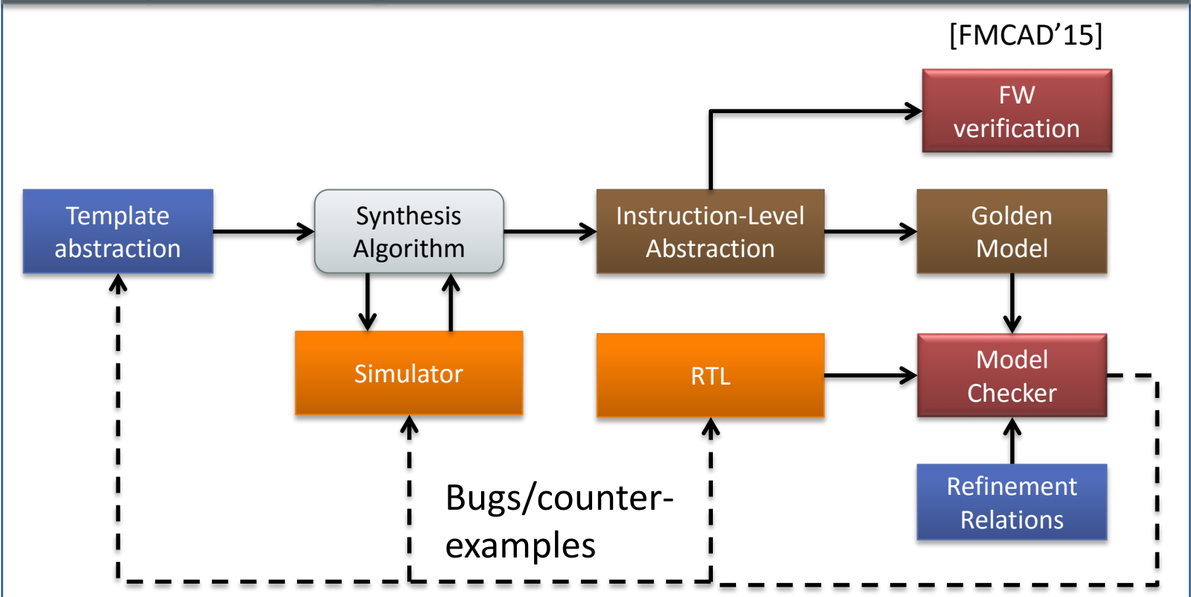
Verification of Security Properties

Confidentiality	Sensitive values must not leak to untrusted entities
Integrity	Untrusted entities must not influence sensitive values
Availability	Untrusted entities must not be able to render the system non-functional

Difficult to specify confidentiality and integrity in LTL because they are not predicates of state; instead they refer to information flow

Synthesizing Instruction-Level Abstractions

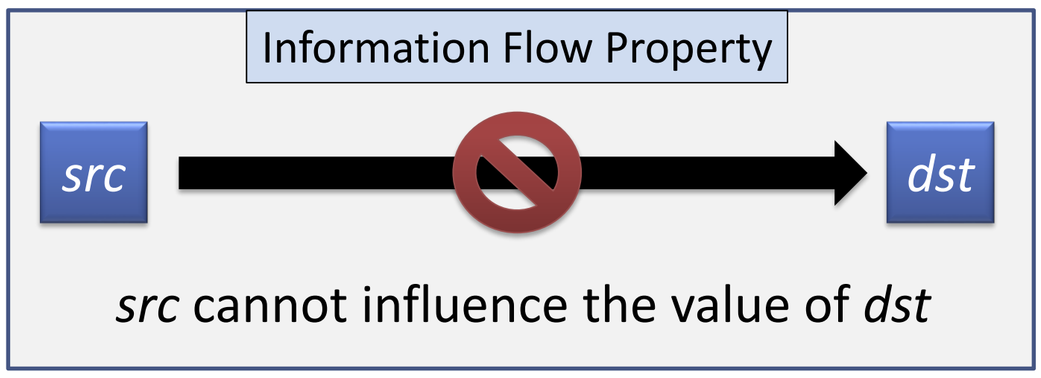
[FMCAD'15]



Key ideas

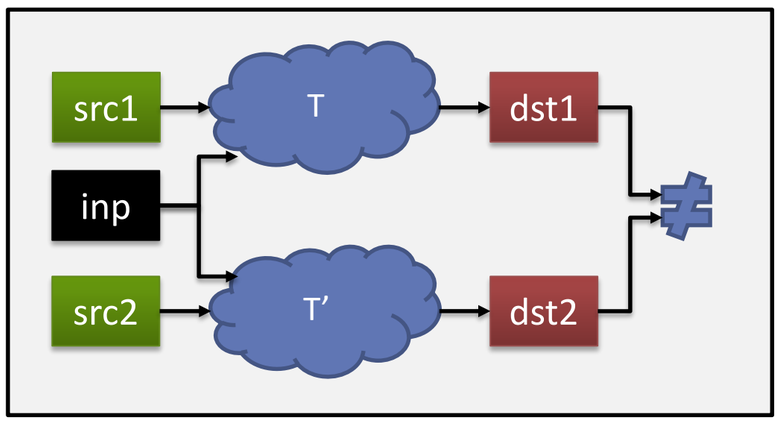
- Construct abstraction at **instruction-granularity**
- **Synthesize** abstraction from a template
- Verify correctness: ensure ILA matches RTL

Specifying Information Flow Properties on the ILA



- Can capture both confidentiality and integrity
- We specify properties on an ***augmented*** ILA
  - High-level system state such as user/su mode, current thread and VM ids, and son
  - Convert events such as user/su state-transitions into state variables

Verifying Information Flow Properties



Can different values at the source result in different values at the destination?

- Naïve method requires two "copies" of the transition system; this is avoidable
- Use dynamic taint propagation and CEGAR; refine the taints with the more precise formulation only when this is required

Conclusions

Two main challenges in verifying security properties in SoCs are:

- Considering HW+FW issues together
- Specifying and verifying security properties like confidentiality and integrity

- Template-based synthesis of ILAs solves the HW+FW verification problem
- Specification language and verification techniques for information flow properties solve the security verification problem!