A Holistic Approach Towards Online Monitoring of Integrated Circuits and Systems

RICE

Challenge:

Errors in integrated circuits and systems are difficult to eliminate:

- Design bugs
- Maliciously modified components ("trojans")

Hardware trojans are hard to detect in post-silicon testing

Solution:

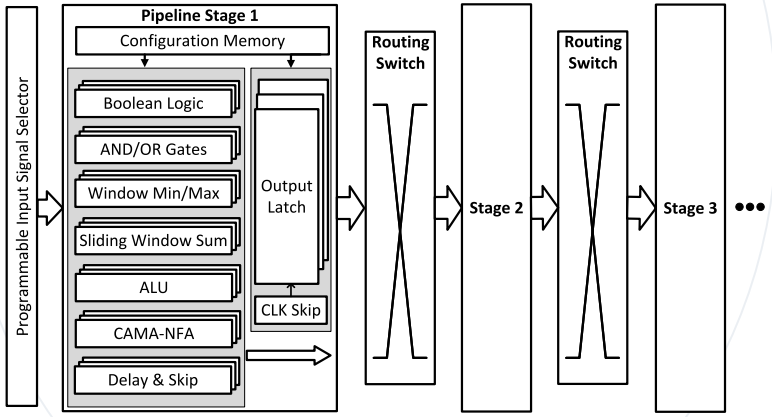
Online monitoring during normal deployment and operation.

- Specify monitor using a "hardware-friendly" formalism
- Compile specification to execute on a programmable hardware accelerator

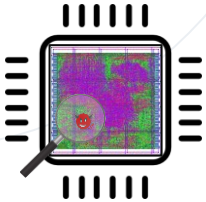
Formal specification of monitor

$$inc \coloneqq edge \wedge P_{[1,D]}edge$$
$$rst \coloneqq edge \wedge \neg P_{[1,D]}edge$$
$$c \coloneqq Count(inc, rst)$$
$$trigger \coloneqq (c \geq k)$$

Compiler



Programmable hardware accelerator for online monitors



Scientific Impact:

- Advances in specification-based runtime verification and online monitoring for hardware
- Novel hardware design for event detection and pattern matching over streams
- Monitoring benchmark for hardware trojans

Broader Impact and Broader Participation:

- Improve reliability, safety, and security of hardware
- Curriculum development
- Training of graduate and undergraduate students
- Mentoring of high-school students

Award # 2319572, Rice University
Konstantinos Mamouras (mamouras@rice.edu)
Kaiyuan Yang (kyang@rice.edu)