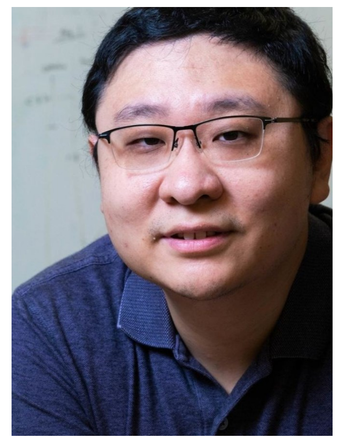
FMitF: Track I:
A Holistic Approach Towards Online Monitoring of Integrated Circuits and Systems



Konstantinos Mamouras (PI) and Kaiyuan Yang (co-PI), Rice University

https://www.nsf.gov/awardsearch/showAward?AWD_ID=2319572

Overview and Challenges

Integrated circuits and systems go through a rigorous process of verification and testing, yet errors remain hard to eliminate. There are various sources of errors:

- Unintentional design bugs
- ***Maliciously*** modified hardware components ("trojans")

Design-time verification and testing cannot eliminate bugs or malicious modifications introduced during fabrication. Moreover, hardware trojans are hard to detect in post-silicon testing.

Approach

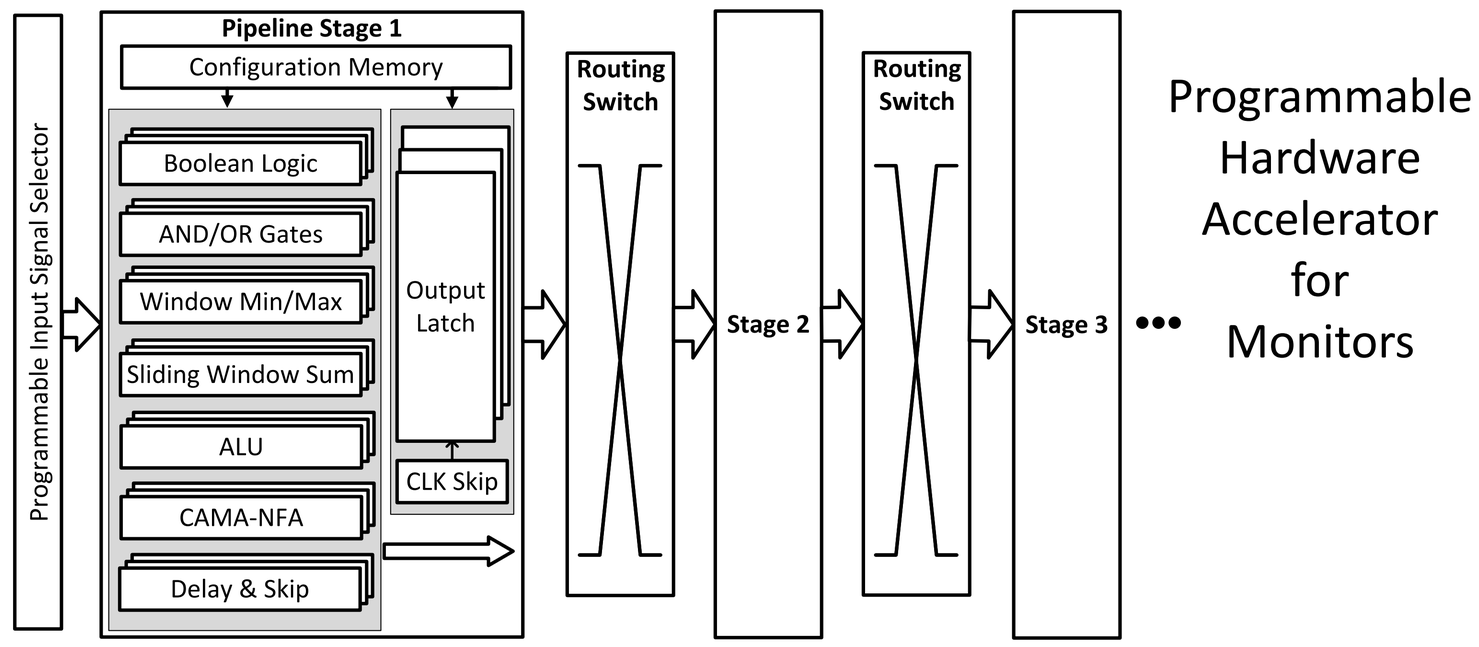
Introduce a "last line of defense": ***online monitoring*** of fabricated hardware components during normal deployment and operation:

- Detect conditions that violate the system's integrity and security
- Detect the activation of trojans
- Enable higher-level corrective actions

Formal specification of online monitor

$inc \coloneqq edge \wedge P_{[1,D]}edge$
$rst \coloneqq edge \wedge \neg P_{[1,D]}edge$
$c_1 \coloneqq Count(inc, rst)$
$trig_1 \coloneqq (c_1 \geq k)$
$c_2 \coloneqq CountWnd(edge, k \cdot D)$
$trig_2 \coloneqq (c_2 \geq k)$
$trigger \coloneqq trig_1 \vee trig_2$

Specification to Hardware Compiler



Main Objectives

❑ Theoretical/Software Foundations
- Design of high-level monitor specification languages
- Design of hardware-friendly computational primitives
- Compilation from specifications to hardware

❑ Scalable and Programmable Hardware Accelerator
- Design of ultra-efficient circuits for computational primitives
- Creation of hardware programming toolchain
- Prototyping of full-stack systems

❑ Testbed Development and Applications
- Chip fabrication and testbed development
- Benchmarks for maliciously modified hardware (e.g., A2 trojan)
- Suite of monitoring benchmarks

Scientific Impact

❑ The project advances specification-based runtime verification and online monitoring for hardware
- New algorithms for monitoring a specification formalism that combines Metric Temporal Logic (MTL) with regular expressions.

❑ Novel hardware design for event detection and pattern matching over streams
- Hardware acceleration for patterns with nondeterminism & succinct counting using NFAs with counters and bit vectors

❑ Monitoring benchmark for hardware trojans

Broader Impact on Society

- Improve the reliability, safety, and security of the hardware that forms the basis of modern computing infrastructure
- Bring trust to international cooperation for hardware design and fabrication

Broader Impact on Education

Curriculum development to integrate material on online monitoring and hardware-accelerated pattern matching in existing courses.

Broader Impact on Participation

- The project has been providing training to graduate and undergraduate students
- The PIs organize summer research experiences for Houston-area high-school students