SEMICONDUCTORS & MICROELECTRONICS

AI-DRIVEN HARDWARE SECURITY

University of Arizona researchers develop innovative AI-driven strategies to secure the semiconductor supply chain and post-CMOS computing, safeguarding microelectronics from design to post-deployment threats and vulnerabilities.

The fabless semiconductor model, while accelerating innovation, exposes integrated circuits (ICs) to critical risks, including hardware Trojan (HT) insertion, IC counterfeiting, and IP cloning. Emerging memristive devices, such as magnetic random access memory (MRAM) that promise to enable energy-efficient AI hardware accelerators, are vulnerable to process variations and suffer from reliability issues. We focus on automated design-for-trust frameworks to secure next-generation microelectronics—from design, to foundry, to system deployment and beyond.

Applications and impact

Our research addresses semiconductor security challenges from design to final fabrication. We develop AI-driven frameworks to detect and mitigate threats to protect next generation of hardware accelerators, as well as automate secure chip design flows to strengthen trustworthiness across the semiconductor ecosystem.

AI-assisted semiconductor supply chain security

In the era of global manufacturing, a secure supply chain is a pressing challenge which we address through two complementary innovations: HT-SCAM and OASIC. **HT-SCAM** reveals a novel threat vector where standard cell libraries, assumed trustworthy, are weaponized with stealthy HTs (**Figure 1**). By exploiting overlooked vulnerabilities at the standard cell level, HT-SCAM highlights the critical need for upstream trust validation. **OASIC** introduces an automated, AI-assisted defense-in-depth mechanism by inserting optimized, MRAM-based reconfigurable interconnect and logic (RIL) blocks into IC designs. These RIL blocks offer high resilience against reverse-engineering attacks and power side-channel leakage, while maintaining low power and area overheads. OASIC can dynamically adjust configurations based on security metrics and design constraints (**Figure 2**). These advancements position AI as a useful tool to secure the supply chain against emerging threats.

Secure AI hardware design leverages post-CMOS technologies

Emerging devices, such as spin-orbit torque magnetic RAM (SOT-MRAM), enable energy-efficient machine learning (ML) accelerators through in-memory computing architectures. However, their sensitivity to fabrication variations introduces cascading security vulnerabilities across the device, circuit, and system levels (**Figure 3**). Our approach, **S-TUNE**, reveals that SOT-MRAMs, despite high-speed and low-power advantages, are highly susceptible to manufacturing threats. Our gray-box threat model simulations show that a global oxide thickness shift of less than 5% can induce stealthy bit-flips in accelerator crossbar weights. Read currents can exceed switching thresholds due to accumulated process variations, resulting in reliability degradation and covert inference errors (**Figure 4**). S-TUNE provides the foundation to mitigate such threats to ensure reliable, trusted, and energy-efficient computing systems for edge AI, autonomous vehicles, and defense-critical applications.

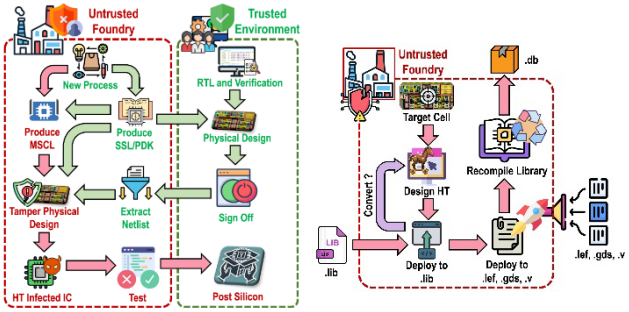

Figure 1: HT-SCAM threat. Untrusted foundry exploits standard cell libraries for stealth Trojan insertion.

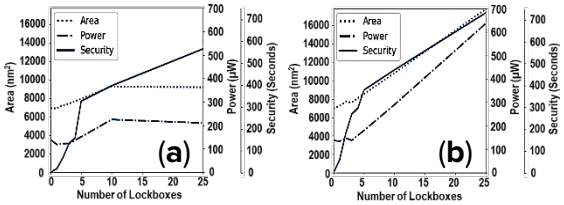

Figure 2: Power-area-security tradeoff of locking an AES core using OASIC. SAT-Attack: (**a**) 8×8 (**b**) 8×8×8 RIL blocks.

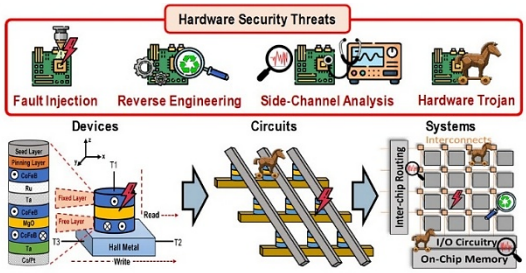

Figure 3: Security threats associated with manufacturing. Fault injection, reverse engineering, and side-channel analysis can propagate across the supply chain.

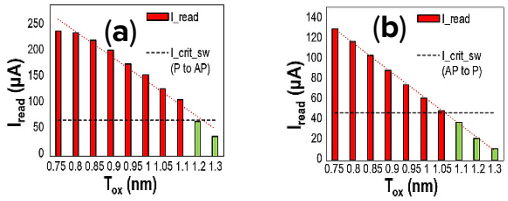

Figure 4: SOT-MTJ device read current (I_{read}) variation. Oxide thickness variation impact on (**a**) 'AP' to 'P', and (**b**) 'P' to 'AP' read current compared to critical current.

Soheil Salehi, PhD | Assistant Professor
Electrical & Computer Engineering | ssalehi@arizona.edu

Soheil's research interests are hardware and AI-enabled security in IoT, GenAI for secure hardware design, neuromorphic AI hardware, spin-based devices, low-power and reliability-aware VLSI circuits, digital twins, and mixed reality for workforce education.