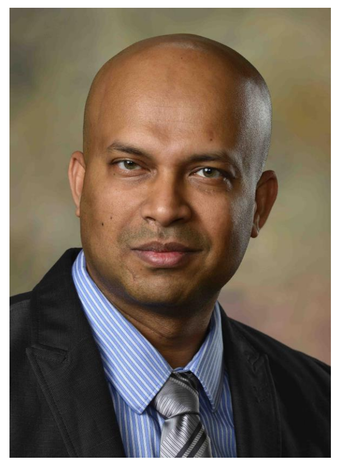
CRII: SaTC: Robust Design-for-Security (DFS) Architecture for Enabling Trust in Integrated Circuits (IC) Manufacturing and Test



Ujjwal Guin

http://www.eng.auburn.edu/~uguin/research.html

- Attacks and solutions for Logic Locking

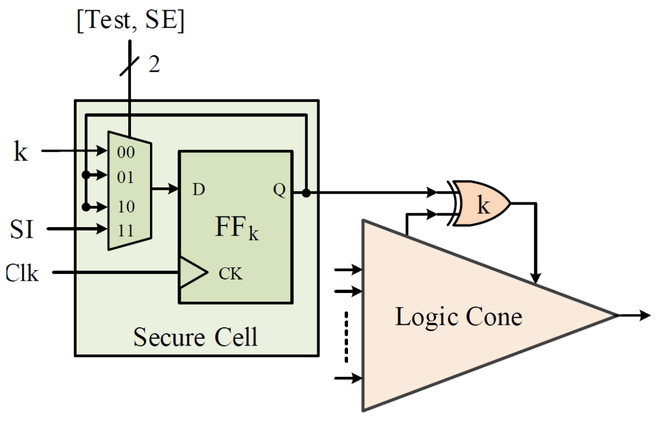


Fig. 1. Secure cell architecture to thwart SAT attack.

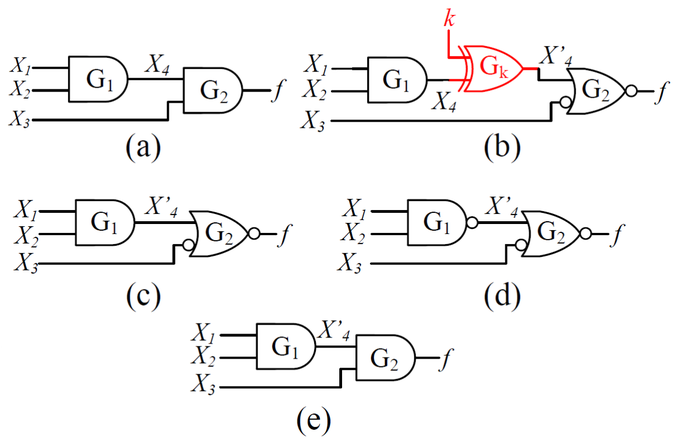


Fig. 2. Topology-guided attack (TGA) using equivalent unit function (EUF) search. (a) Original netlist. (b) Locked netlist with key value k = 1. (c) EUF for hypothesis key k_h= *0*. (d) EUF for hypothesis key k_h = *1* (Case-I). (e) EUF for hypothesis key k_h= *1* (Case-II).

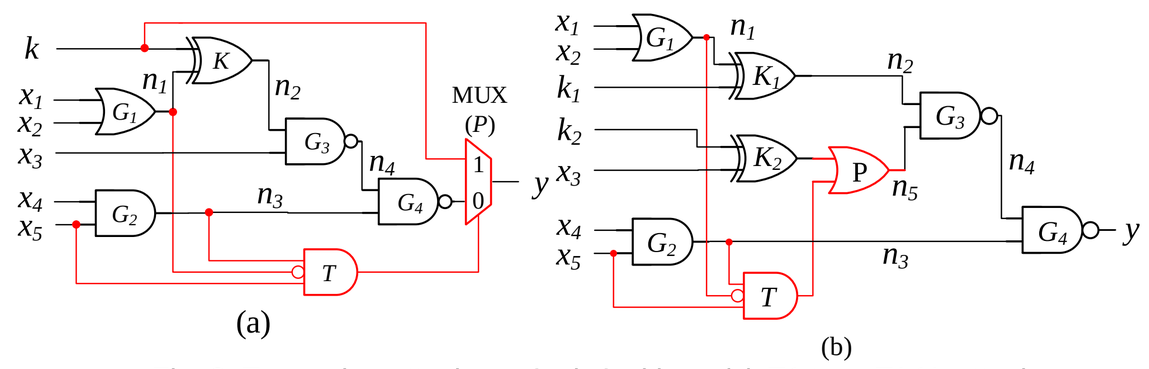


Fig. 3. Tampering attacks on logic locking. (a) *T1 type TAAL attack,* where a *Type-3* combinational Trojan is inserted for key extraction directly from the connection between key gate and tamper-proof memory, (b) *T3 type TAAL attack,* where a *Type-3* combinational Trojan is inserted for the secret key extraction.

- Key Problems
  - Boolean satisfiability (SAT)-based algorithms have been shown to effectively determine the obfuscation key and break the any logic locking mechanisms.
  - The design should support manufacturing tests at the foundry before activation of the chips.
  - Prevent the logic key from being exposed through the scan chain.
  - Logic locking was designed to address the threat from untrusted manufacturing, a foundry has many more effective means to extract the secret key from a locked ICs without using SAT.
- Proposed Solution
  - We presented a design for security architecture that uses a novel secure cell (SC), which prevents the obfuscation key from being captured in internal flip-flops of a chip and disables scan access after functional mode.
  - The SC provides a complete protection against SAT-based and other existing attacks and allows manufacturing tests to be performed before the activation of chips at an untrusted site.
  - Demonstrated a tampering attack with hardware Trojans to break any logic locked circuit. Design for combinational and sequential Trojans has been proposed to evade manufacturing tests.
- Scientific Impact
  - A novel design for security (DFS) architecture to prevent existing state-of-art SAT-based attacks on logic locking by disabling scan access.
  - Demonstrated for the first time to use a hardware Trojan to break logic locking. The secret key can be directly exposed to the primary output, once the Trojan is activated.
  - The novel topology-guided attack to determine the secret key using unit function search, which does not require an oracle. This helps to evaluate the security of logic locking techniques through topological analysis of a locked netlist.
  - Demonstrated a novel topology-guided attack (TGA) which is based on equivalent unit function search to evaluate the attack resistivity, and its countermeasure is also proposed.
  - Other solutions –implementation of blockchain for supply chain security and IoT security, detection and avoidance of recycled ICs, and prevention of system-level cloning – have been resulted from this CRII project.
- Broader Impact (on society)
  - Serve a critical need for the industry and government by enabling trust in untrusted IC manufacturing and tests.
  - Bridge existing gaps in trust between SoC design houses and foundries.
  - Prevent IC overproduction and IP piracy.
- Broader Impact (education and outreach)
  - Developed two new hardware security courses -- Hardware Security I and II.
  - Promoting research among undergraduate and under-representative students.
  - Participate standardization activities of the SAE G-19A, and G-32.
- Broader Impact (quantify potential impact)
  - Security metrics for logic locking.
  - Open source software for implementation, test and security evaluation of logic locking.
  - Publications at reputed journals and conferences.