On-chip security circuit against hardware tampering

Technology #cu14190

Computer security is a key issue for consumers, government agencies, and industry. While much of the focus has traditionally been centered on software, hardware-based security is necessary for a completely secure system. This technology describes a beacon circuit that provides hardware protection by alerting users to malicious tampering in design and fabrication. The beacon is integrated into the hardware itself and detects any changes in components or circuitry not intended by the user and provides alerts via unique power signature readouts. Beacon-based security provides a unified approach for protecting hardware from design to fabrication and beyond.

Unified approach to hardware security using beacon circuit is capable of detecting tampering in hardware design and fabrication

This technology provides hardware security by integrating the beacon into the circuit itself. An auditor can then query the beacon with a customizable key signal, to which the beacon will produce a unique output, such as a power signature, in response. Since the circuit will be inoperable without the beacon, a foundry intending to insert malicious backdoors in the hardware will be unable to circumvent this security feature. Additionally, protections against third party components can be implemented in the design, thus bridging the gap between hardware security against foundry and third party IP injected backdoors.

A prototype of the technology has been tested and its efficacy was verified for at least three hardware designs.

Lead Inventor:
Simha Sethumadhavan, Ph.D.

Applications:
- Hardware security for microprocessor designers and manufacturers
• Protection against IP theft
• Protection for government agency hardware
• Hardware memory security
• Hardware security for mobile device and video game console components

Advantages:

• Offers protection against tampering in a design by foundries and manufacturers in addition to backdoors inserted by third party components
• Does not require “golden designs” for comparison
• Uses confidential, customizable query signal for auditing hardware
• Beacon is entangled with circuit design to ensure circuit will not operate after tampering
• Integrates security at design and fabrication level

Patent Information:

Patent Pending (US 20160314300)

Tech Ventures Reference: IR CU14190

Inventors

Lakshminarasimhan Sethumadhavan