Threshold Voltage-Defined Switches for Programmable Gates

Researchers at the University of South Florida have developed a novel switch that turns ON/OFF, based on the threshold voltage asserted on it. This switch is opaque to attackers thus, making the configuration secure.

Camouflaging is a technique of hiding the circuit functionality of a few chosen gates in semiconductor supply chains in order to make reverse engineering or piracy impossible, if not, extremely difficult. Camouflaging gates using dummy contacts may hide the functionality of circuit, but it doesn’t force exhaustive reverse engineering by the attacker. The existing methods are either costly, leave layout clues, or offers limited resistance to reverse engineering.

Inventors at USF have developed a novel switch that can be used in conjunction with nominal threshold voltage transistors to camouflage the gate. Transistor threshold voltage-defined switches can camouflage a logic gate both logically and physically to resist against reverse engineering and IP piracy. A camouflaged gate can function as one of NAND, AND, NOR, OR, XOR, or XNOR robustly using threshold-defined switches. The camouflaged design operates at a nominal voltage and conforms to conventional reliability requirements. The design of a circuit can be personalized using camouflaged gates during manufacturing. Apart from mainstream electronics and services, this technology can find applications in military electronics, used in mission critical systems and intelligence agencies.

ADVANTAGES:
- Switch leaves no layout trace
- Helps resist Reverse Engineering (RE)
- Resist intellectual property piracy
- Logic gates are visually identical but not functionally

Camouflages Gates Both Logically and Physically to Resist RE and IP Piracy

Tech ID # 16A005 Patent #: 10,177,768