Preventing Hardware Trojan Insertion through Logic Masking

Sophie Dupuis, Marie-Lise Flottes,
Giorgio Di Natale, Bruno Rouzeyre
Laboratoire LIRMM, Universite de Montpellier

Abstract

Due to the evolution in the Integrated Circuit (IC) supply chain, Intellectual Properties (IPs) and dies come from numerous, and possibly untrusted, sources. This loss of control over the entire production flow may thus lead to several threats including mask theft, overproduction, as well as the insertion of malicious alterations to the ICs, referred to as Hardware Trojans (HTs). To protect ICs from overproduction, their functionality can be masked so that only authorized customers can use them. Combinational logic masking is achieved by the addition of logic gates connected to an input key so that the ICs function properly iif the right key is applied.

In this talk, we present a logic masking method that makes more difficult the insertion of a HT. The goal of this method is to minimize the number of low controllable signals. The assumption is that a HT requires a stealthy triggering condition and that an attacker is then likely to attach this condition on signals with a low controllability. Minimize the number of low controllable signals is therefore supposed to make it harder for an attacker to exploit them to incorporate a HT's trigger.