New side-channel attack against scan chains

Jean Da Rolt, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre
Universite Montpellier II, CNRS UMR 5506, France

Abstract

Insertion of scan chains is the most common technique to ensure observability and controllability of sequential elements in an IC. However, when the chip deals with secret information, the scan chain can be used as back door for accessing secret (or hidden) information, and thus jeopardize the overall security. Several scan-based attacks on cryptographic functions have been described and shown the need for secure scan implementations. These attacks assume a single scan chain. However the conception of large designs and restrictions in terms of test costs may require the implementation of many scan chains and additional test infrastructures for test response compression. In this paper, we present a new generic scan attack that covers a wide range of industrial test infrastructures, including spatial response compressors.