Analysis of Lightweight Register Hardware Threat

Authors : Yang Luo, Beibei Wang

Abstract : In this paper, we present a design methodology of lightweight register transfer level (RTL) hardware threat implemented based on a MAX II FPGA platform. The dynamic power consumed by the toggling of the various bit of registers as well as the dynamic power consumed per unit of logic circuits were analyzed. The hardware threat was designed taking advantage of the differences in dynamic power consumed per unit of logic circuits to hide the transfer information. The experiment result shows that the register hardware threat was successfully implemented by using different dynamic power consumed per unit of logic circuits to hide the key information of DES encryption module. It needs more than 100000 sample curves to reduce the background noise by comparing the sample space when it completely meets the time alignment requirement. In additional, an external trigger signal is playing a very important role to detect the hardware threat in this experiment.

Keywords : side-channel analysis, hardware Trojan, register transfer level, dynamic power
Conference Title : ICCIT 2017 : International Conference on Computing and Information Technology
Conference Location : Singapore, Singapore
Conference Dates : May 04-05, 2017