Cryptology ePrint Archive: Report 2011/391

On the Portability of Side-Channel Attacks – An Analysis of the Xilinx Virtex 4 and Virtex 5 Bitstream Encryption Mechanism

Amir Moradi and Markus Kasper and Christof Paar

Abstract: This paper is a short summary of our real-world side-channel analysis of the bitstream encryption mechanism provided by Xilinx Virtex FPGAs. This work covers our results analyzing the Virtex 4 and 5 family showing that the encryption mechanism can be completely broken with moderate effort. The presented results provide an overview of a practical real-world analysis and should help practitioners to judge the necessity to implement side-channel countermeasures. We demonstrate sophisticated attacks on off-the-shelf FPGAs that go far beyond schoolbook attacks on 8-bit AES S-boxes. We were able to perform the key extraction by using only the measurements of a single power-up. Access to the key allows cloning and manipulating a design, which has been encrypted to protect the intellectual property and to prevent fraud. As a consequence, the target product faces serious threats like IP theft and more advanced attacks such as reverse engineering or the introduction of hardware Trojans. To the best of our knowledge, this is the first successful attack against the bitstream encryption of Xilinx Virtex 4 and Virtex 5 reported in the open literature.

Category / Keywords: implementation / Side-Channel Analysis

Date: received 19 Jul 2011

Contact author: amir moradi at rub de