Cryptology ePrint Archive: Report 2011/390

On the Vulnerability of FPGA Bitstream Encryption against Power Analysis Attacks – Extracting Keys from Xilinx Virtex-II FPGAs

Amir Moradi and Alessandro Barenghi and Timo Kasper and Christof Paar

Abstract: Over the last two decades FPGAs have become central components for many advanced digital systems, e.g., video signal processing, network routers, data acquisition and military systems. In order to protect the intellectual property and to prevent fraud, e.g., by cloning an FPGA or manipulating its content, many current FPGAs employ a bitstream encryption feature. We develop a successful attack on the bitstream encryption engine integrated in the widespread Virtex-II Pro FPGAs from Xilinx, using side-channel analysis. After measuring the power consumption of a single power-up of the device and a modest amount of off-line computation, we are able to recover all three different keys used by its triple DES module. Our method allows extracting secret keys from any real-world device where the bitstream encryption feature of Virtex-II Pro is enabled. As a consequence, the target product can be cloned and manipulated at will of the attacker. Also, more advanced attacks such as reverse engineering or the introduction of hardware Trojans become potential threats. As part of the side-channel attack, we were able to deduce certain internals of the hardware encryption engine. To our knowledge, this is the first attack against the bitstream encryption of a commercial FPGA reported in the open literature.

Category / Keywords: implementation / Side-Channel Analysis

Date: received 19 Jul 2011, last revised 22 Jul 2011

Contact author: amir moradi at rub de

Available formats: PDF | BibTeX Citation

Version: 20110722:071954 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]