Read The Free Bitstream - Extracting Secrets from Protected Hardware

Amir Moradi, Alessandro Barenghi, Timo Kasper, Christof Paar
Ruhr-University Bochum, Germany

Abstract

Over the last two decades FPGAs have become central components for many advanced digital systems, e.g., routers, set-top boxes or military systems. In order to protect the manufacturer's (or the user's) intellectual property and to prevent cloning, many current FPGAs employ bitstream encryption. We describe a successful attack on the bitstream encryption feature of Virtex-II Pro FPGAs from Xilinx, a widespread device, using side-channel analysis. We are able to recover all three different keys used by its triple DES module from a single power-up of the device and a modest amount of off-line computation. 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 device can be cloned 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.