Security Analysis of the Bitstream Encryption Scheme of Altera FPGAs

Amir Moradi, David Oswald, Christof Paar, Pawel Swierczynski

Abstract

Altera provides custom logic solutions and is, besides Xilinx, one of the biggest vendors in their sector. Altera's Field Programmable Gate Arrays (FPGAs) are SRAM-based devices and thus volatile, which implies that they load their configuration from a configuration device or a flash memory at each new power-up. The FPGA designs are given in the form of a bitstream. In order to protect such a configuration design from being intercepted and thus cloned or modified, a solution called design security is offered. It is a feature based on the Advanced Encryption Standard (AES) encryption, and is available for the low-cost Cyclone III LS FPGAs, for the midrange FPGAs Aria II, and especially for the high-end FPGAs Stratix II, Stratix III, Stratix IV, and Stratix V. The design security is offered in two versions: A non-volatile variant that stores a one-time programmable AES key or a volatile solution based on a backup battery, allowing to re-program the AES key or to erase it.

The utilized AES engine is embedded on the FPGA as an additional unit. Its task is to decrypt previously encrypted configuration designs while they are downloaded from an external source. Stratix II and Stratix II GX FPGAs use AES-128, while all other solutions provide AES-256. From a mathematical point of view, algorithms like AES or 3DES are highly secure. However, recently, it was shown that the bitstream encryption feature of several FPGA product lines is susceptible to side-channel attacks that monitor the power consumption of the cryptographic module.

In this work, we present the first successful side-channel attack on the bitstream encryption of the Altera Stratix II FPGA, which uses the non-volatile solution. For this, we reverse-engineered the details of the proprietary and unpublished Stratix II bitstream encryption scheme

(and that of Stratix III) from the Quartus II software. Based on this information, we present how we obtained the full 128-bit AES key of a Stratix II by means of side-channel analysis with 30,000 measurements, which can be acquired in less than three hours.
The complete unencrypted configuration bitstream of a Stratix II that is (seemingly) protected by the design security feature can hence fall into the hands of a competitor or criminal - possibly implying system-wide damage if confidential information such as proprietary encryption schemes or keys programmed into the FPGA are extracted. In addition to lost Intellectual Property (IP), reprogramming the attacked FPGA with modified code, for instance, to secretly plant a hardware trojan, is a particularly dangerous scenario for many security-critical applications.