Opal Kelly

Opal Kelly Incorporated
13500 SW 72nd Ave, STE 100
Portland, OR 97223

ZEM5310 Security Features

February 07, 2021

Overview

In certain applications it is necessary to protect the intellectual property configured on your FPGA. It has been shown in research that reverse engineering of the vender tool-chain allows you to convert the configuration bit-stream back into a net-list representation [1]. Software has even been created that does just that [2]. Close examination of the net-list can bring you back to the original RTL representation.

The configuration bit-stream can be extracted by simply capturing the data pins by external means from the non-volatile memory configuration device on power up. Even more simply, JTAG can perform this same function by driving the configuration device pins from the FPGA and sensing the response. After consideration, this may be an issue in your deployment.

The Cyclone V onboard the ZEM5310 has the ability for AES encryption of the configuration bit-stream using a 256-bit non-volatile key. This encrypted bit-stream is a significant layer of protection when it's programmed into the flash memory module onboard. A tamper protection mode is also available which limits JTAG instructions that are more prone to malicious exploitation [3].

Caution:

Using these features on the Cyclone V has irreversible results. The non-volatile key and tamper protection mode are implemented using fuses. Once programmed, the fuses rupture in a controlled manner which permanently set your device [4]. This functionality is implemented to provide further security. The following limitations result from implementing these features:

- With the tamper protection mode set, external JTAG programming no longer works. ZEM5310 supports AS and PS configuration and must be used instead of JTAG.
- Only basic, mandatory, JTAG testing instructions are allowed in tamper protection mode. You can read about the allowed instructions in citation [4]. You can unlock 'JTAG Secure mode' by issuing an 'unlock' instruction only from the internal JTAG interface.
- In tamper protection mode, only encrypted bit-streams are accepted, and will only ever be accepted. If this mode is not set, your Cyclone V will accept configuration from unencrypted bit-streams as well as encrypted bit-streams with the correct key.

Details

- Requires that you have an Altera Quartus License file (standard or pro editions). Quartus lite does not support this feature [5].
- To set the tamper protection bit, a 'quartus.int' file must be created with 'PGM_GEN_KEY_SECURE_EKP=ON' inserted. This file is used when creating the AES key programming file. More information at citation [4].

The following information for implementing these features is taken from AN 556: Using the Design Security Features in Intel FPGAs [4]:

1. The Intel® Quartus® Prime software generates the design security key programming file and encrypts the configuration data using the user-defined 256-bit security key.
2. Store the encrypted configuration file in the external memory.
3. Program the AES key programming file into the Cyclone® V device through a JTAG interface.
4. Configure the Cyclone® V device. At the system power-up, the external memory device sends the encrypted configuration file to the Cyclone® V device.

[1]https://www.researchgate.net/publication/200065272_From_the_bitstream_to_the_netlist

[2]https://ieeexplore.ieee.org/document/6339165

[3]https://www.intel.com/content/www/us/en/programmable/documentation/sam1403481100977.html#sam1403479091182

[4]https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/an/an556.pdf

[5]https://www.intel.com/content/www/us/en/programmable/support/support-resources/download/licensing/q-and-a.html#c_05