

Secure Your Consumer Design with CoolRunner-II CPLDs

CoolRunner-II CPLDs offer unique features to ensure a more secure design and reduce the risk of reverse engineering.

by Rob Schreck
Senior Marketing Manager
Xilinx, Inc.
rob.schreck@xilinx.com

Product designs are a major investment. However, if a design is stolen (known as reverse engineering), that unique product can then be copied and sold for a lower price. The company that originally designed the product loses revenue and market share. Consumers may benefit in the short term, but in the long run companies will decide against major product designs and consumers will ultimately pay the price.

Xilinx CoolRunner-II™ CPLDs offer a great way to protect consumer designs from reverse engineering. Of course, Xilinx CPLDs are non-volatile, so it's not necessary to configure the device at start up. But let's discuss more important security measures.

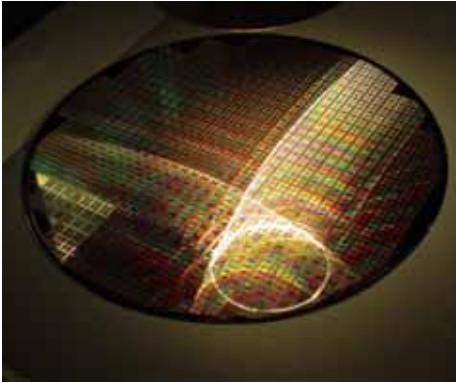


Figure 1 – CPLD wafer

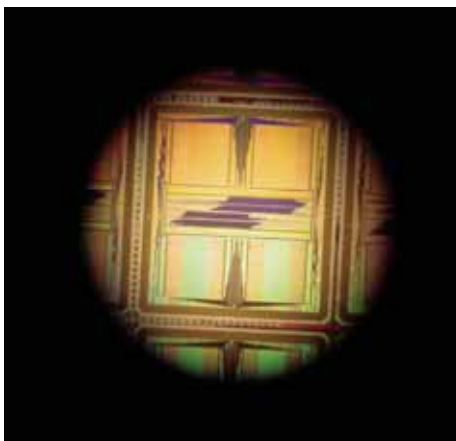


Figure 2 – Wafer below the top routing layers

Elusive Security Bits

Xilinx offers a unique capability in CoolRunner-II CPLDs: multiple security bits. These security bits are electrically erasable cells scattered throughout the device. You set the security bits by simply selecting the action within the Xilinx iMPACT programming software dialog box when the design is finished. Once these bits are programmed, the internal pattern remains fixed in the device and the program is protected from theft.

Somewhere above the substrate but beneath the metal are floating gates that hold the nonvolatile memory bit contents (Figure 1). If another company wanted to reverse engineer the design, they would have to de-program the security bits. To do that, they would first have to look through four or five metal layers to find them.

Even if they could see through four or five metal layers (Figure 2), they still couldn't "see" the bits because they are interspersed among the programming bits. Plus,

they would have to figure out which ones are the security bits and which ones are the program bits. Figure 3 shows the underlying configuration cells beneath the architecture of CoolRunner-II devices.

So for someone to read-back the design, they would have to find the security bits (a very difficult task) and then erase them. If they attempted to erase them with a laser, they would have to know where to aim and how to erase each of them without erasing any other bits. They would also have to disconnect key signals for the chip operation and bit read-back. It would take many costly, time-consuming experiments to arrive at a solution.

Additional Protection Measures

After erasing the security bits, reverse engineers would still need to issue the correct demands and reverse the JEDEC file. The entire project would require a long, costly trial-and-error process, and would not be economically prudent.

Even after reading the JEDEC file, reverse engineers still need to understand the design. There are various tricks that you, as the original product designer, can use to make such an analysis prohibitively time-consuming. For example, double-data rate designs make analysis much more difficult to understand. You can also design using state machines, which are less predictable than processors. You can even build

a unique CryptoBLAZE processor, based on the Xilinx PicoBlaze™ soft processor, with its own instruction set, non-volatility, and tricky timing. That would be a particularly difficult device to reverse engineer.

Additionally, the CoolRunner-II DataGATE feature can be used as a response to tampering. DataGATE is designed to dynamically and selectively block switching input signals that can draw power within CoolRunner-II devices. To increase design security, you can use the DataGATE feature to lock up the device when someone attempts to read the program.

For example, you can use a serial password from an external source, such as a keypad. If the password is correct, the device will run; if not, DataGATE will block all inputs and deny additional password attempts.

Conclusion

Considering how important maintaining design security is to your company, CoolRunner-II CPLDs offer an easy-to-implement solution to make reverse engineering CPLD designs nearly impossible. See for yourself how you can take advantage of this unique feature for your next project.

For more information about CoolRunner-II devices, visit www.xilinx.com/cr2. For a Quick Start presentation on security issues with Cool-Runner-II devices, visit www.xilinx.com/products/cpldsolutions/module/cr2_security.pps. ❧

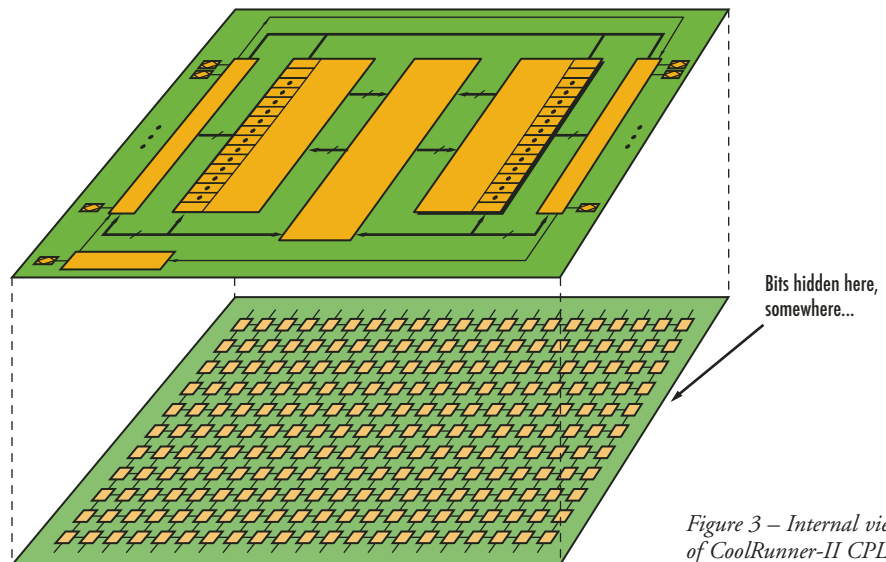


Figure 3 – Internal view of CoolRunner-II CPLD