

Low-Cost Security Solutions with Spartan-3A and Spartan-3AN Platforms

Could your low-cost FPGA design be more secure? Check out what Xilinx has to offer with the newest additions to the Spartan-3 generation.

by Maureen Smerdon
Strategic Marketing Manager
Xilinx, Inc.
maureen.smerdon@xilinx.com

Security has become a hot topic: whether boarding a plane, closing the front door, or beginning a next-generation circuit design, security is a significant issue. For designers, the greatest threat comes from the alarming amount of counterfeited products on the market as a result of design thefts. According to the Anti-Counterfeiting Coalition, the estimated dollar exchange associated with counterfeiting throughout the United States in 2003 was \$287 billion, or 63% of the total \$456 billion of counterfeit products sold annually worldwide.

In this article, I'll describe Xilinx® security measures that can protect your low-cost FPGA designs.

The Top Three Security Threats

The most common security breach in electronics design is reverse engineering. This occurs when a thief attempts to recreate or rebuild a product with the intent of selling it on the open market at a lower cost. Through reverse engineering, thieves can build designs much faster without incurring the expense of R&D, quite probably at a lower cost.

Today, as companies have moved to outsource manufacturing, they are subject to new security breaches called overbuilding and cloning. In overbuilding, the outsourced manufacturer simply manufactures more units than the OEM (original equip-

ment manufacturer) ordered. These additional units are sold without authorization from the OEM.

Cloning is when a thief creates a duplicate of your design, IP, or product under the same (or another) label. Again, cloners do not incur any R&D costs. Both overbuilt and cloned products have a drastically reduced time to market.

What remains unknown are the intangibles associated with such security breaches. Whether a product is reverse-engineered, overbuilt, or cloned, it means a substantial revenue loss for the OEM. In addition to the loss of revenue, there is also a cost associated with quality in the form of returns. This could affect the brand image and potentially add to the OEM's bottom line due to increased RMAs (return materials authorizations) or technical support to determine what the issue is and how to resolve the end customer's problem. Ultimately, it may be

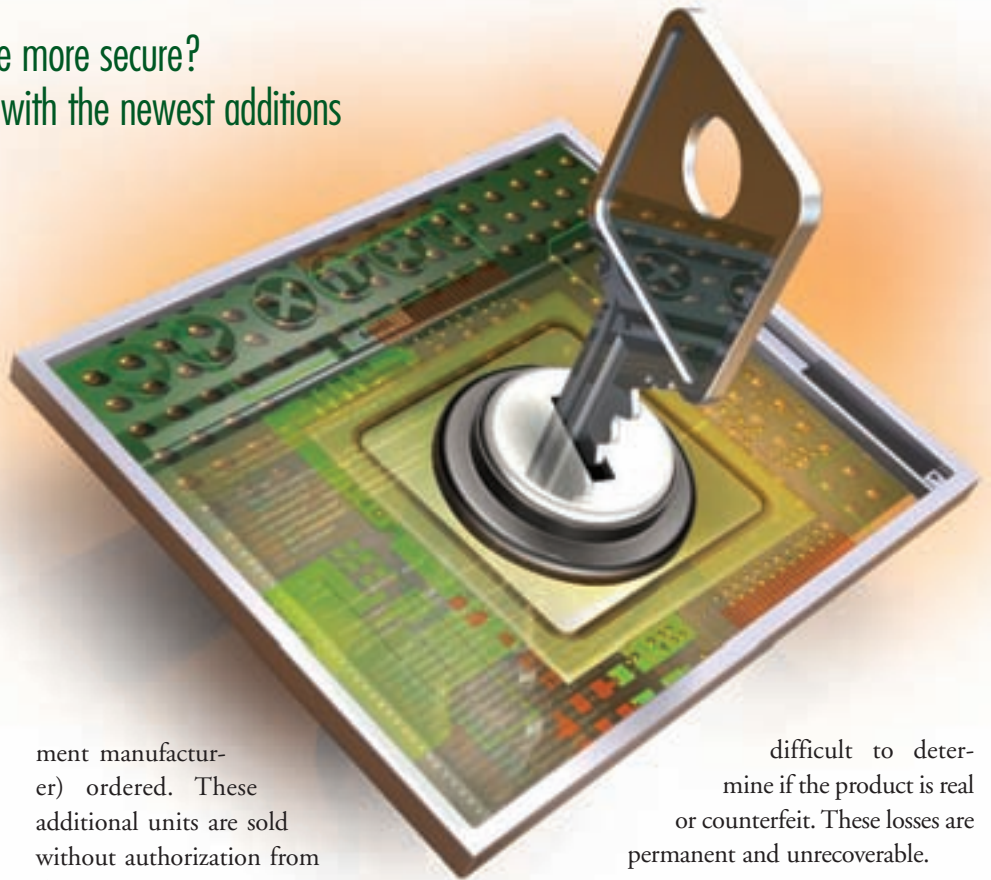
difficult to determine if the product is real or counterfeit. These losses are permanent and unrecoverable.

Security Using DeviceDNA

Traditionally, FPGAs use some kind of bit-stream encryption to guard against reverse engineering and cloning. In yesteryear's model, this worked well. It will not, however, protect you in today's world against overbuilding.

As a designer, how can you protect your design against all three security thefts? Xilinx has a few solutions, recently introducing the Spartan™-3A and Spartan-3AN device families with DeviceDNA to help you fend off cloners, overbuilders, and reverse engineers.

The DeviceDNA design-level security protects the design, the IP, and the embedded code. DeviceDNA is a specific 57-bit ID that is unique to each device. This 57-bit ID is contained in an area on the FPGA and is fixed or set at the Xilinx factory; it



cannot be altered. Both Spartan-3A and Spartan-3AN FPGAs contain a unique ID in each device shipped.

This ID is then combined with a designer's personalized algorithm and stored on the FPGA. The algorithm is basically an arithmetic equation that defines how to take the DeviceDNA and create a result. The result can then be stored anywhere, such as in the external memory or in flash. The algorithm is the secret to the security because only the designer knows it. Although it is stored on the FPGA, to an onlooker it just looks like part of the bitstream.

Spartan-3A Security

For Spartan-3A devices, the algorithm compares the result using DeviceDNA to the result stored in the flash after the device has been configured. If they match, the design is authorized. If they do not match, then the design can be set up to behave in a variety of ways, from slight to severe functional impairment.

Let's look at an example of authentication in our daily life. Say you stop at a local fast food restaurant for a snack. You are out of cash and are forced to use your ATM card (DeviceDNA), which only you are authorized to use. You place your order and then swipe the card. The machine asks for your PIN number (personalized algorithm). The system then compares the PIN number you entered with the number stored at the bank. If it matches, you get your snack. If not, you will go hungry.

The potential weakness is if someone has both your ATM card and your PIN number. The PIN authorization algorithm number, once learned, is easily cloned. This is why the authorization algorithm is incorporated into the design itself. The algorithm is placed in the most secret location inside of programmable logic, with millions of configuration options.

Spartan-3AN Security

For the Spartan-3AN platform, our new non-volatile FPGA, the process is almost the same – with a few enhancements. The first security enhancement is that the bitstream is hidden inside the FPGA. This makes it more difficult for someone to monitor.

The second security enhancement that the Spartan-3AN FPGA has are two unique serial numbers, the DeviceDNA and a factory flash ID, found in flash memory. The two unique IDs give more than 70 bytes of serial numbers, resulting in a large number of algorithmic possibilities and therefore increasing the amount of time it would take to breach the authentication algorithm. Now the design is specifically tied to both the FPGA and the flash IDs.

Applying the earlier analogy, having two unique IDs is like requiring two different ATM cards to get a snack.

not breached. Because the algorithm is unknown, it is the key to the design-level security. The algorithm is implemented in the fabric of the FPGA; therefore, it becomes a handful of bits within the millions of configuration bits in the FPGA. Unless you know how the bits fit together or what the algorithm is, it looks like just a mass of numbers. Figure 1 outlines a possible flow using Spartan-3AN devices.

The Spartan-3AN design-level security shown in Figure 2 is a completely self-contained security solution. The flash contains both the FPGA configuration bitstream and a previously generated

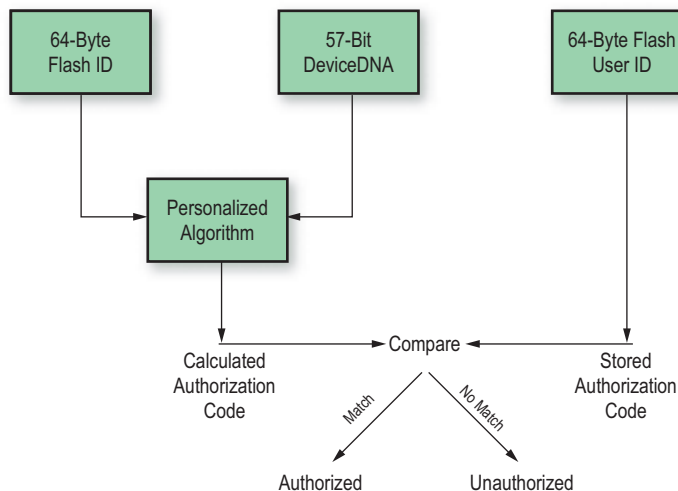


Figure 1 – Possible security setup with Spartan-3AN FPGAs

The third improvement is in the stored authorization code. On the Spartan-3AN platform, the authorization code can be stored on-chip in a special one-time programmable 64-byte register called the Flash User Field. This allows the complete security system to be self-contained. With no need for external interfaces or storage, overall security increases and reverse engineering is more difficult.

The authentication algorithm is user-defined, allowing you to implement the right level of security within your design budget. The authentication algorithm is also the primary secret in the security system. Something in the authentication process must be a secret so that security is

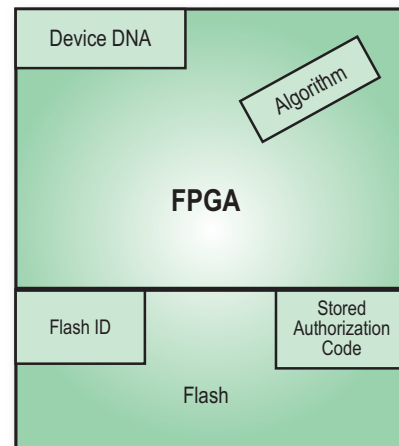


Figure 2 – Spartan-3AN device with security

authorization code. This code is stored in the one-time programmable Flash User Field by a trusted/secured manufacturer or registration process.

At power up, the FPGA configures normally. Once configured, the FPGA application includes circuitry that validates the design authorized to operate on the associated Spartan-3AN FPGA. The DeviceDNA and factory flash ID will be read by the authentication algorithm, which in turn generates an active authorization code that is compared to the previously generated authorization code stored in the Flash User Field. If both codes are equal, the device is authenticated. Otherwise, the device is illegitimate and unauthorized.

Access Denied

The handling of failed authentication is another one of the strengths of the DeviceDNA design-level approach. Authentication can be completely integrated into the design. Thus, multiple responses can result from an unauthorized design, such as:

- No functionality – the design completely stops functioning
- Limited functionality – primary or key circuits are disabled or bypassed
- Time bomb – full functionality for only a limited period of time
- Active defense – the system monitors activities and defends against attack

- Permanent self-destruction – erases all flash content and permanently lock-downs flash to all zeros

The design-level security described here is the basic level of security that can be achieved within the Spartan-3A and Spartan-3AN platforms.

Conclusion

The security measures in Spartan-3A and Spartan-3AN platforms provide many ways to protect from reverse engineering, overbuilding, and cloning. To learn more about securing your low-cost FPGA designs, see the Spartan Generation Configuration User Guide at www.xilinx.com/bvdocs/userguides/ug333.pdf.

Stay Ahead!

Xilinx® Virtex™-5 LX FPGA
A new generation of performance

Analog I/O, Camera Link, LVDS, FPDP-II, RS485/422 & L-Band Receiver options
Fast, integrated I/O without bottlenecks

Multiple banks of fast memory
DSP & I/O optimized memory architecture

PCI-X Interface with multiple DMA controllers
More than 1GB/s bandwidth to host

Libraries and Example Code
Easy to use with head-start time-to-market

with the PMC-FPGA05 Range of Virtex-5 based PMCs

Processing & FPGA Input/Output Data Recorders & Storage Bus Analyzers

For more information, please visit <http://virtex5.vmetro.com> or call (281) 584-0728

VIMETRO
Innovation deployed