

## Protecting the FPGA Design From Common Threats

*As counterfeiting and IP theft increase, concerns regarding design and IP security also are on the rise. In the case of FPGAs, this requires protection of the bitstream and configuration of the device. Cyclone III LS FPGAs offer security features on a low-power platform, allowing designers to meet constraints and ship products with confidence their IP is protected.*

### Introduction

The global estimated loss to counterfeiting is expected to exceed U.S.\$1.5 trillion in 2009. Counterfeiting impacts all businesses in all markets, from Gucci handbags to computer chips to proprietary algorithms. The threats to companies' intellectual property (IP) grow as the global supply chain becomes increasingly complex. Security and protection in the global supply chain is critical to maintaining a competitive advantage, while in some cases it is required just to stay in business.

The first step towards counterfeit equipment is tampering, which encompasses all forms of obtrusive efforts to gain access to the system design. Historically, tampering was associated with military equipment; however, due to the rise of counterfeit electronics, tampering is becoming a critical issue for all manufacturers. The purpose of anti-tamper is to deter reverse engineering of technology, which would otherwise allow technology transfer, alteration of system capability, and development of countermeasures.

Governments and corporations invest billions of dollars to develop critical networking infrastructures, sophisticated weapon systems, and secure banking systems. However, systems that are vulnerable to tampering can quickly deteriorate, resulting in loss of competitive advantage, lost revenue, brand dilution. The exploitation of electronic equipment is increasing due to the lucrative margins on counterfeit equipment. These vulnerabilities make the inclusion of anti-tamper more and more important.

There are four components to creating an anti-tamper solution:

- Tamper resistance is the ability to resist tamper attempts, and is achieved by specialized features.
- Tamper detection is the ability to make the system or user aware of the tamper event.
- Tamper response is the countermeasure procedure that a system must take once tampering is detected.
- Tamper evidence must be detectable so authorized personnel inspecting the system can identify whether the system has been tampered with.

The components of anti-tamper and a preview of Altera® solutions for each component are summarized in [Table 1](#).

*Table 1. Anti-Tamper Components and Altera Solutions*

| Anti-Tamper Components | Description          | Altera Cyclone III LS Solution                          |
|------------------------|----------------------|---|
| Tamper resistance      | Specialized features | Encryption key<br>JTAG-port protection                  |
| Tamper detection       | Awareness            | Programming failures<br>Cyclical redundancy check (CRC) |
| Tamper response        | Countermeasures      | Zeroization of all configuration memory                 |
| Tamper evidence        | Visible evidence     | Multiple unsuccessful programming                       |

### Threats to ASICs

The ASIC market is accustomed to protecting against tampering threats such as destructive analysis, over- and under-voltage analysis, and timing analysis. To reverse engineer an ASIC using destructive analysis, each layer of the device is captured to determine its functionality. Though this process requires expensive equipment and expertise,

there is little protection inherent to an ASIC to prevent such an act. Timing analysis and over- and under-voltage analysis do not require expensive equipment, but are very laborious and error prone, so are less frequently used to reverse-engineer complex ASIC designs. Also, timing analysis on an ASIC is deterministic, so the time taken from input to output can be determined by passing a signal through a multiplexer.

Once reverse engineered, the IP within the ASIC can be proliferated in any number of counterfeit systems. Counterfeit electronic equipment, specifically networking equipment, is on the rise across the globe due to the high resale value of the equipment. Counterfeiting is a relatively inexpensive method of generating equipment and therefore is a high-margin business. These factors make electronic equipment very attractive for IP theft. Unfortunately for original equipment manufacturers (OEMs), the result of counterfeit systems is lower revenue, lower profit ratios, and threatened brand image.

## Threats to FPGAs

The industrial market is moving towards FPGAs due to their benefits of reprogrammability and proof against obsolescence. The military market is moving towards commercial off-the-shelf (COTS) products with highly specialized applications, making FPGAs a perfect blend of COTS and customized product. Because online banking systems have multiple layers of security from locked doors to server locks, the banking industry is looking for means of pushing the security to lower levels, thus making security inherent to the system. The overall market is concerned with the proliferation of theft and black market/mislabeled products. While FPGAs are less vulnerable to the reverse engineering that threatens ASICs, these devices are susceptible to a different set of threats.

The reprogrammable architecture of the FPGA acts as an inherent barrier to a straightforward tampering attempt to reverse engineer the design. Due to its volatile nature, decapsulating and deprocessing the die provides a blank map of the FPGA architecture. However, a different set of tampering activities can affect FPGAs, such as copying and cloning the bitstream during configuration, manipulating the design through JTAG, and initiating single event upsets (SEUs) to cause functional changes to the design.

### *Configuration Threats*

While reprogrammability is a benefit for the designer, it also creates concern because an external device is required for configuration. The entire design must be stored in a system memory external to the FPGA, and upon power-up, transferred from the memory to the FPGA. Designers concerned about IP protection can embed the traces used for configuration within PCB layers, but this may create other problems in the complex PCB design. Therefore, there are very few solutions to protect a FPGA design from being copied during configuration.

### *Encryption Solution*

Altera's Cyclone® III LS FPGAs protect the bitstream during configuration by including a 256-bit AES encryption engine using a volatile key. Therefore, even if the bitstream is monitored, the encryption key is necessary to reverse engineer the design. The specific implementation of the encryption key in a Cyclone III LS FPGA never allows read-back of the encryption key, so once programmed, the key remains safely stored in the FPGA. Because the encryption key is volatile, any attempt at destructive analysis results in permanent loss of the key. In addition, Altera has taken several steps to help protect the integrity of the encryption key:

- The key storage is placed under layers of metal to resist physical attacks.
- The key is obfuscated before it is stored in the FPGA memory.
- The key bits are distributed among other logic.
- The volatile key can be erased via JTAG if a tamper event is detected.

To reverse-engineer an FPGA design protected by design security, the key must first be obtained to decrypt the configuration file. However, the key is stored securely within the FPGA, which makes it extremely difficult to obtain the key. With the volatile key, the user can clear the key when a tamper event is detected. Even if a key was somehow obtained and the configuration file decrypted, the next step would be to map that configuration file to the device

resource level, which tells what logic elements (LEs), interconnects, memory blocks, and I/Os are used. Altera uses a confidential configuration bitstream format, making it difficult to understand the configuration file information.

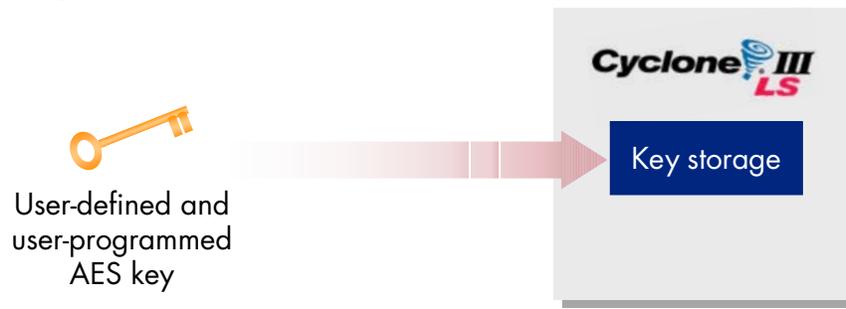
Additionally, none of Altera's FPGAs, including Cyclone III LS devices, allow read-back of the FPGA configuration through any means. Therefore, once the design is loaded into the FPGA, there is no mechanism to stream the data out again. The combination of configuration encryption and the lack of read-back circuitry restricts direct copying of the design, giving manufacturers the confidence that designing with Altera FPGAs will keep their valuable IP safe.

### Design Security Process

Altera's design security process involves three steps.

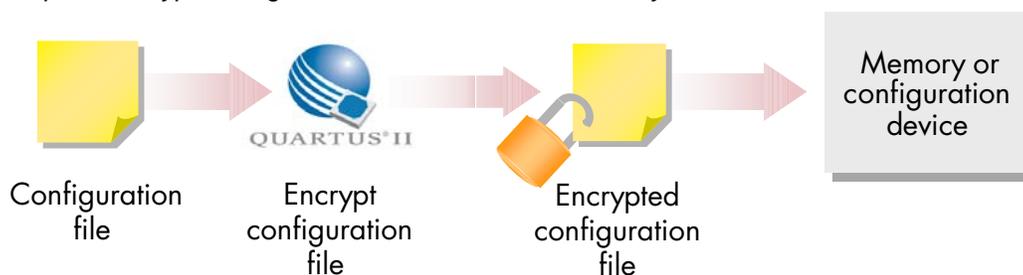
1. The user must first choose a 256-bit key and program it into the FPGA via the Cyclone III LS JTAG interface (Figure 1). Note that the key is chosen and programmed by the user, and that Altera is not involved in this process.

Figure 1. Step 1—Program Cyclone III LS FPGA With 256-bit Key



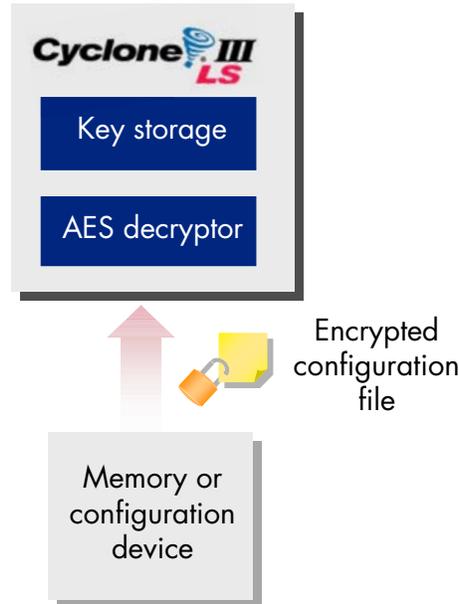
2. The next step is to take the configuration bitstream file (also called the programmer object file or **.pof**) and encrypt it with the same key used in Step 1, using Altera's Quartus® II design software (Figure 2). The Quartus II software generates the encrypted **.pof**, which the user then stores in the configuration flash device (this can be an EPC or EPCS device or an industry-standard flash device).

Figure 2. Step 2—Encrypt Configuration File and Store in Memory



3. Finally, the encrypted **.pof** is downloaded into the Cyclone III LS FPGA during configuration (Figure 3). The AES decryptor inside the FPGA decrypts the **.pof** using the stored key, and configures the FPGA. Even if an adversary is able to copy the encrypted **.pof** from the flash device or while the file is transferring to the FPGA, the **.pof** cannot be used to program another Cyclone III LS FPGA because the AES key is unknown.

Figure 3. Step 3—Receive and Decrypt Encrypted Configuration File



### JTAG Threats

Another type of threat makes use of the JTAG port. Although the port is meant for board connectivity and basic system-functionality testing, the flexibility of JTAG can be misused to determine the configuration of the FPGA. Because in most FPGAs, JTAG is always enabled, uses dedicated pins, and overrides any other configuration mechanism, it can be used to exercise the design systematically to reverse engineer the functionality, thereby stealing the design. However, like timing analysis on an FPGA, this is an extremely laborious, time consuming, and rote process, though it requires no specialized equipment.

### JTAG-Port Protection Solution

Recognizing the susceptibility of JTAG, Cyclone III LS FPGAs take extra precautions by restricting access to the JTAG port. Traditionally, the JTAG port always was enabled on FPGAs, and any instructions received on the JTAG I/O pins would execute immediately. In Cyclone III LS FPGAs, the native state of JTAG is restricted to only those instructions required for compliance to the IEEE specification. The JTAG port can be reset to accept the full instruction set. However, resetting the JTAG port causes the Cyclone III LS FPGA automatically to erase all configuration within itself (including the volatile AES key, if used), before allowing full access on the JTAG pins. Therefore, a user cannot use the JTAG port to test or modify the design in any way.

### Protection Beyond Today's Threats

The security features in Cyclone III LS FPGAs go beyond the immediate needs of the market to protect the bitstream during configuration and to protect the design from the JTAG port. In addition to these features, Cyclone III LS FPGAs provide tamper-detection capabilities to identify advertent and inadvertent bitwise manipulation of the design using cyclic redundancy check (CRC) circuitry. The CRC circuit continuously checks the configuration of the FPGA for single- or multiple-bit changes to the configuration due to a soft error (or SEU) caused by atmospheric neutrons. In the case of an error, the system is notified immediately to take corrective action. This ultimate control over system behavior allows various activities such as error logging or a graceful shutdown. The CRC feature can also act as an additional layer of anti-tamper protection, alerting the user if the memory contents have changed since the FPGA was last configured.

The Cyclone III LS FPGA goes beyond specialized features for tamper resistance, to provide an active tamper response. The safest method of response is to clear all sensitive data from the system before it is compromised.

Though the definition of zeroization involves a clear plus verification that all data was cleared, most applications will benefit from a zeroization which clears all memory cells of the FPGA. The Cyclone III LS zeroization solution breaks out the clear function and the verification function to provide the maximum design flexibility to the user. By default, the clear function clears the configuration RAM, which contains the design itself, and the embedded RAM, which contains any design specific data. Additionally, the AES encryption key can be cleared independently of the rest of the device.

This zeroization capability provides the designer with the ability to trigger corrective action in the case a tamper event is detected. The zeroization can be triggered by any design input, giving the user maximum flexibility to control the tamper response of the system, and making it difficult to disable the capability before a zeroization can be completed. In order to complete zeroization, the verification process involves reloading a benign design, a reconfiguration cycle, and a subsequent CRC cycle to ensure successful reconfiguration. This benign design can be set to do anything from creating markers for tamper evidence to continuing the zeroization operation on external system components.

Furthermore, Cyclone III LS FPGAs offer an uninterruptible clock source through an internal oscillator. This ensures that if the system clock or input clock to the FPGA is manipulated, the system can still perform health checks, monitor the FPGA configuration through the CRC, and initiate or perform corrective action if an unexpected event compromises the security of the design. The existence of an internal clock source gives designers full control over systems in the field, ensuring that the designs can protect themselves in the event of a threat.

## Conclusion

As counterfeiting and IP theft increase, concerns regarding the security of the design and IP are also on the rise. In the case of FPGAs, this requires protection of the bitstream and configuration of the device. At odds with the concerns for security are the economic factors of size, power, and time to market. Cyclone III LS FPGAs were created to bring these two objectives together. Cyclone III LS FPGAs offer security features for a complete anti-tamper solution on a low-power platform, allowing designers to meet constraints and ship product with confidence that the IP is protected.

## Further Information

- Cyclone III FPGAs—Security:  
[www.altera.com/products/devices/cyclone3/overview/security/cy3-security.html](http://www.altera.com/products/devices/cyclone3/overview/security/cy3-security.html)
- Literature: Cyclone III Devices:  
[www.altera.com/products/devices/cyclone3/literature/cy3-literature.jsp](http://www.altera.com/products/devices/cyclone3/literature/cy3-literature.jsp)
- *Enabling Design Separation for High-Reliability and Information-Assurance Systems*:  
[www.altera.com/literature/wp/wp-01110-design-separation.pdf](http://www.altera.com/literature/wp/wp-01110-design-separation.pdf)
- Quartus II Subscription Edition Software:  
[www.altera.com/products/software/quartus-ii/subscription-edition/qts-se-index.html](http://www.altera.com/products/software/quartus-ii/subscription-edition/qts-se-index.html)

## Acknowledgments

- Juwayriyah Hussain, Sr. Product Marketing Engineer, Low-Cost Products, Altera Corporation
- Paul Quintana, Sr. Technical Manager, Military Business Unit, Altera Corporation



101 Innovation Drive  
San Jose, CA 95134  
[www.altera.com](http://www.altera.com)

Copyright © 2009 Altera Corporation. All rights reserved. Altera, The Programmable Solutions Company, the stylized Altera logo, specific device designations, and all other words and logos that are identified as trademarks and/or service marks are, unless noted otherwise, the trademarks and service marks of Altera Corporation in the U.S. and other countries. All other product or service names are the property of their respective holders. Altera products are protected under numerous U.S. and foreign patents and pending applications, maskwork rights, and copyrights. Altera warrants performance of its semiconductor products to current specifications in accordance with Altera's standard warranty, but reserves the right to make changes to any products and services at any time without notice. Altera assumes no responsibility or liability arising out of the application or use of any information, product, or service described herein except as expressly agreed to in writing by Altera Corporation. Altera customers are advised to obtain the latest version of device specifications before relying on any published information and before placing orders for products or services.