# Secure Architecture in Microsemi FPGAs and SoC FPGAs—an Overview

November 2013

# Introduction

In order to create a secure embedded system design it is critical that the main devices used in the design have a secure technology on which to build a secure architecture. Without a secure technology the Intellectual Property (IP) created with the design can be copied, cloned, or reverse engineered, leading to significant financial loss and loss of consumer confidence. A secure technology allows an FPGA or SoC architecture to be built on top of a secure foundation, but the architecture must also include key security features and capabilities. Without a secure architecture, the secrets designed to be protected within the device can be subject to attacks that can discover secret data and compromise the integrity of the design. This overview will describe the various technologies and architectures used by Microsemi and illustrate how they are used to create the worlds most secure FPGAs and SoC FPGAs.

## The Need for a Secure Technology

The three main technologies available to FPGA manufacturers include antifuse, flash, and SRAM. Of these three technologies SRAM is by far the least secure. Because an SRAM device must be configured from an external memory every time they are powered up, this provides a multitude of opportunities for an attacker to 'snoop' or even copy the configuration bitstream. Reverse engineering of SRAM-based FPGAs is thus easy to do and there are even programs available to translate a configuration bitstream into HDL code to simplify such efforts. Some FPGAs attempt to encrypt the bitstream using on-chip cryptographic functions and a battery back-up to keep the devices operating after the design has been loaded. In addition to the extra cost and manufacturing overhead associated with this approach the security keys need to be loaded in 'plaintext' form during manufacturing. This gives an attacker an opportunity to capture the security key and then reverse engineer the design by capturing and decrypting the encrypted configuration bitstream. These weaknesses make it clear that SRAM-based FPGA devices are not an appropriate target for a system that needs to protect valuable Intellectual Property (IP) from even the simplest forms of copying or reverse engineering.

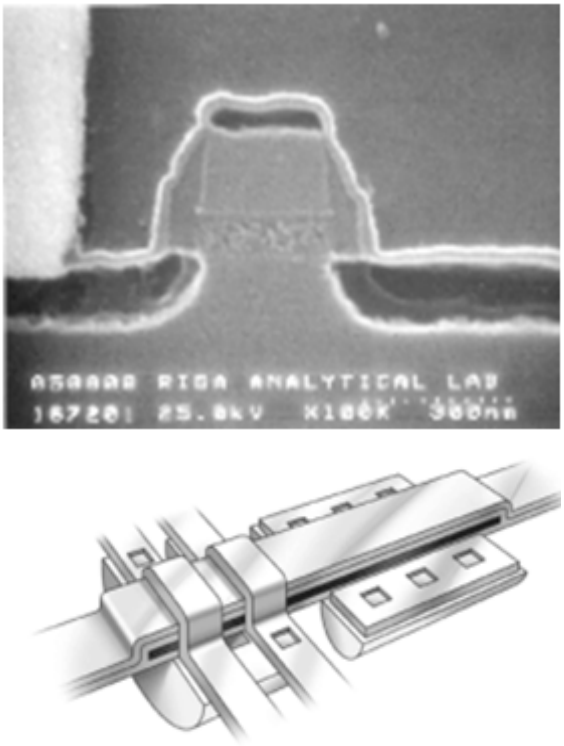

*Figure 1:* **Microsemi Flash FPGA Memory Cell Cross Section and Interconnect Structure**

## Security in Microsemi Flash-based FPGAs

Until the advent of the Microsemi families of flash-based FPGAs, there was no secure reprogrammable logic technology available for embedded systems designers. While antifuse is the most secure of all programmable logic solutions, because of the difficulty associated with trying to copy or reverse engineer the contents of a design, flash-based FPGAs provide both security and reprogrammability.

A typical Microsemi FPGA flash cell cross section is shown on the left side of Figure 1 on page 2. The interconnection to a typical cell is shown on the right side of the figure. These figures illustrate the difficulty an attacker, using physical probes, would have in probing specific cells. Additionally, even if probing was possible, determining the state of a switch is difficult, as micro-probing the switch will destroy the charge on the floating gate. To determine the state of millions of switches is so prohibitive as to be considered almost impossible. Consider that in most cases, if the cost to reverse engineer the design is more than the cost to develop it, the target device can be considered very secure.

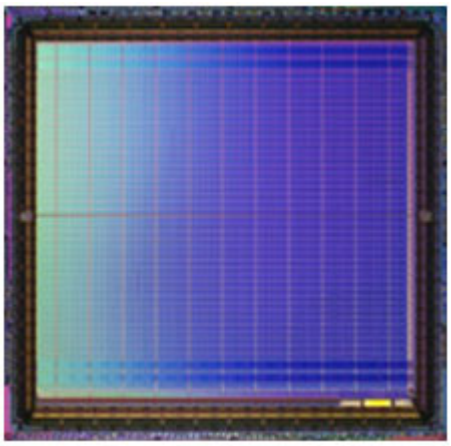

*Figure 2:* **Uniform Flash FPGA Structure Makes Locating Probe-points Difficult**

A photomicrograph of a Microsemi flash FPGA is shown in Figure 2. The uniform (homogenous) nature of flash FPGAs makes it exceptionally difficult to identify specific probe points during a physical attack. Other device technologies, without such a uniform layout, make it much easier to locate specific configuration elements within the fabric. For those types of devices, techniques that use thermal or light emitting dye can be used to determine configuration of cell contents and are then much more easily mapped back to the logic structure defined by the observed configuration values.

## Secure Architecture in Microsemi Flash-based SmartFusion2 and IGLOO2 FPGAs

Using the secure flash technology as a starting point, Microsemi SmartFusion®2 SoC FPGAs and IGLOO®2 FPGAs add the worlds most secure architecture. Just a few examples of these features are sufficient to illustrate this point. Programming of SmartFusion2 and IGLOO2 devices is ONLY done using a bitstream that is authenticated and encrypted by using security keys stored on the device. Security keys are stored in encrypted form within SmartFusion2 and IGLOO2 devices, so that even if the keys are discovered another level of attack would need to be performed to actually use the keys to decrypt secret information—thus the door isn't just locked, access to the key that unlocks the door is locked too! Secret keys are further protected by a variety of features, including protection from advanced security attacks like Differential Power Analysis (DPA). Keys are further secured by using redundant circuit design techniques that protect these keys from corruption or unauthorized changes (tampering). Anti-tampering features are also included so that secret information can be quickly erased (‘zeroized’) when a temper event is detected. A variety of special security Lock-Bits are available to the user to define ‘security barriers’ so that features can be only used when authorized. For example, segments of NVM can be ‘locked’ to be read only so that they are secure from writing by unauthorized routines or corruption from a ‘bug’ in the design (Bugs are notorious for providing attackers on otherwise secure designs with opportunities to ‘hack’ even the most carefully secured design).

SmartFusion2 and IGLOO2 devices have a wealth of additional features that help create a secure architecture. Refer to the white papers listed in the "To Learn More" section at the end of this document for additional examples.

## Secure Architecture in Microsemi ProASIC and ProASIC$^{PLUS}$ FPGAs

ProASIC and ProASIC$^{PLUS}$ FPGAs build on the secure flash technology by providing additional security capabilities at the architecture level to protect designs from other types of attacks. The FlashLock® feature, for example, can be used to prevent unauthorized users from being able to read back the contents of a Microsemi ProASIC or ProASIC$^{PLUS}$ FPGA. Additionally, special security keys are hidden throughout the fabric, preventing internal probing and overwriting. They are located such that they cannot be accessed or bypassed without destroying the rest of the device, making both invasive and more subtle non-invasive attacks ineffective against Microsemi flash FPGAs.

## Security in Microsemi Antifuse FPGAs

Industry experts regard antifuse as the most secure of all programmable logic solutions because of the difficulty associated with trying to copy or reverse engineer the contents of a design. Because of this, antifuse FPGAs have long been used by the military and other OEMs, who demand the highest security available. Microsemi's presence and rich tradition in these markets is a powerful testimonial to the merit of Microsemi's products for customers who value security.

As illustrated by Figure 3 and Figure 4, the differences between a programmed antifuse and an unprogrammed antifuse is very difficult to determine, even if the fuse is cut precisely in half and photographed, resulting in a perfect cross section. The difficulty in trying to make enough cross sections like this is unimaginable.

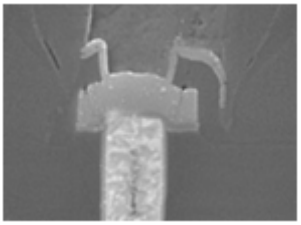

*Figure 3:* **A Programmed Antifuse Cross Section**

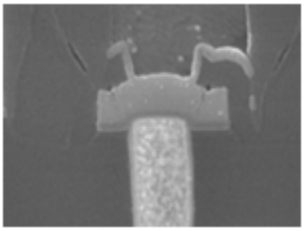

*Figure 4:* **An Unprogrammed Antifuse Cross Section**

Even if the millions of needed cross sections and photographs were generated, determining the state of a single switch is very difficult since the physical change created by programming the fuse is very difficult to detect.

To determine the state of millions of such antifuses is clearly prohibitive, even for the most tenacious and well-funded attacker. At some point it would just be less costly to recreate the design (or just by the entire company!).

A number of additional factors complicate attempts to compromise a Microsemi antifuse FPGA. The microscopic size and sheer number of antifuse make it essentially impossible to locate each fuse and identify its programming state. For example, a single AX2000 FPGA from Microsemi contains approximately 53,000,000 antifuses with only 2-5% programmed in an average design. Invasive probing to evaluate each fuse would most likely result in the destruction of the programmed states needed to trace the design.

# Secure Architecture in Microsemi Antifuse FPGAs

Once programmed, an antifuse device is inherently nonvolatile, which allows the device to retain its configuration indefinitely without requiring an external configuration device. This means that there is no bitstream susceptible to interception, eliminating the potential for in-system errors or data erasures that might occur during download.

The Microsemi FuseLock® architectural feature ensures that unauthorized users will not be able to read back the contents of a Microsemi antifuse FPGA. An additional architectural feature, is the special security fuses that prevent internal probing and overwriting and are hidden throughout the fabric of the device. They are located such that they cannot be accessed or bypassed without destroying the rest of the device, making both invasive and more-subtle noninvasive attacks ineffective against Microsemi antifuse FPGAs.

# Conclusion

Microsemi FPGAs and SoC FPGAs use fundamentally secure technologies on which secure architectures can be created. In contrast to SRAM-based FPGAs, which start from an inherently unsecure technology, Microsemi devices provide the level of security needed to protect your designs from copying, reverse engineering, and even the most aggressive internal and external forms of attack. When security is non-negotiable, Microsemi is your only solution.

To find out more visit the Microsemi Security website and explore the "To Learn More" material listed below.

## To Learn More

1. Security Glossary
2. Securing Your Embedded System Life Cycle
3. Securing Your Supply Chain Life Cycle
4. SmartFusion2 and IGLOO2 Cryptography Services

### Secure Boot

1. Overview of Secure Boot with Microsemi SmartFusion2 SoC FPGAs
2. Overview of Data Security Using Microsemi FPGAs and SoC FPGAs

**Microsemi Corporate Headquarters**
One Enterprise, Aliso Viejo CA 92656 USA
Within the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996

Microsemi Corporation (NASDAQ: MSCC) offers a comprehensive portfolio of semiconductor solutions for: aerospace, defense and security; enterprise and communications; and industrial and alternative energy markets. Products include high-performance, high-reliability analog and RF devices, mixed signal and RF integrated circuits, customizable SoCs, FPGAs, and complete subsystems. Microsemi is headquartered in Aliso Viejo, Calif. Learn more at **www.microsemi.com**.



55900163-0/11.13