Introduction to the SmartFusion2 and IGLOO2 Security Model

November 2013

Introduction

If you have invested years and millions of dollars in the design of an embedded system (and in the creation of the Intellectual Property, or IP, that goes along with the design) it can be of critical importance to protect that system from unauthorized duplication or theft. The protection of an embedded system that uses FPGAs is particularly relevant since FPGAs have become the platforms of choice for innovation. Also, since FPGAs must be configured with a bitstream that defines their operation they can be particularly vulnerable to copying or outright theft.

FPGAs that use Nonvolatile Memory (NVM) for on-chip configuration storage are inherently more secure than devices that use on-chip SRAM configuration storage. Because SRAM-based FPGAs must load the configuration memory from off-chip storage on boot-up, it is a simple matter to capture the configuration bitstream and then copy or reverse engineer the design. Using on-chip NVM to configure the FPGA is a clear advantage over SRAM-based FPGAs from a security standpoint, but even more robust measures need to be taken to adequately protect the IP embedded in your design.

The protection of the design IP, commonly called Design Security, is the assurance that the IP (the FPGA design) programmed into a device is secure and operates as intended for the life of the product. The most important elements in creating robust Design Security for an FPGA are: a secure FPGA fabric, a secure configuration bitstream, and a secure key storage system. If these elements work together correctly they become inherent capabilities of the FPGA, are invisible to the designer, and secure the design IP from potential attacks.

Design Security in SmartFusion2 and IGLOO2 Devices

Several key architectural elements of SmartFusion®2 and IGLOO®2 devices work together to implement the security capabilities required to easiy protect your FPGA design from theft. These elements can be considered as a single unified security system, which is best understood at a high-level by viewing them as an integrated security model. A simplified overview of how SmartFusion2 and IGLOO2 security capabilities are used to secure your design IP is given in the following section.

Security Model Overview

Figure 1 on page 3 depicts the simplified security model used in both SmartFusion2 SoC FPGAs and IGLOO2 FPGAs. The system controller is the heart of the security system and manages all programming, verification, Design Security key-management, and related operations. It interfaces with the security keys, the embedded Nonvolatile Memory array, and the flash FPGA fabric configuration memory.

During normal operation it can also provide optional cryptographic user services. Let’s look at each of the key elements of the simplified security model in more detail, starting with the system controller.

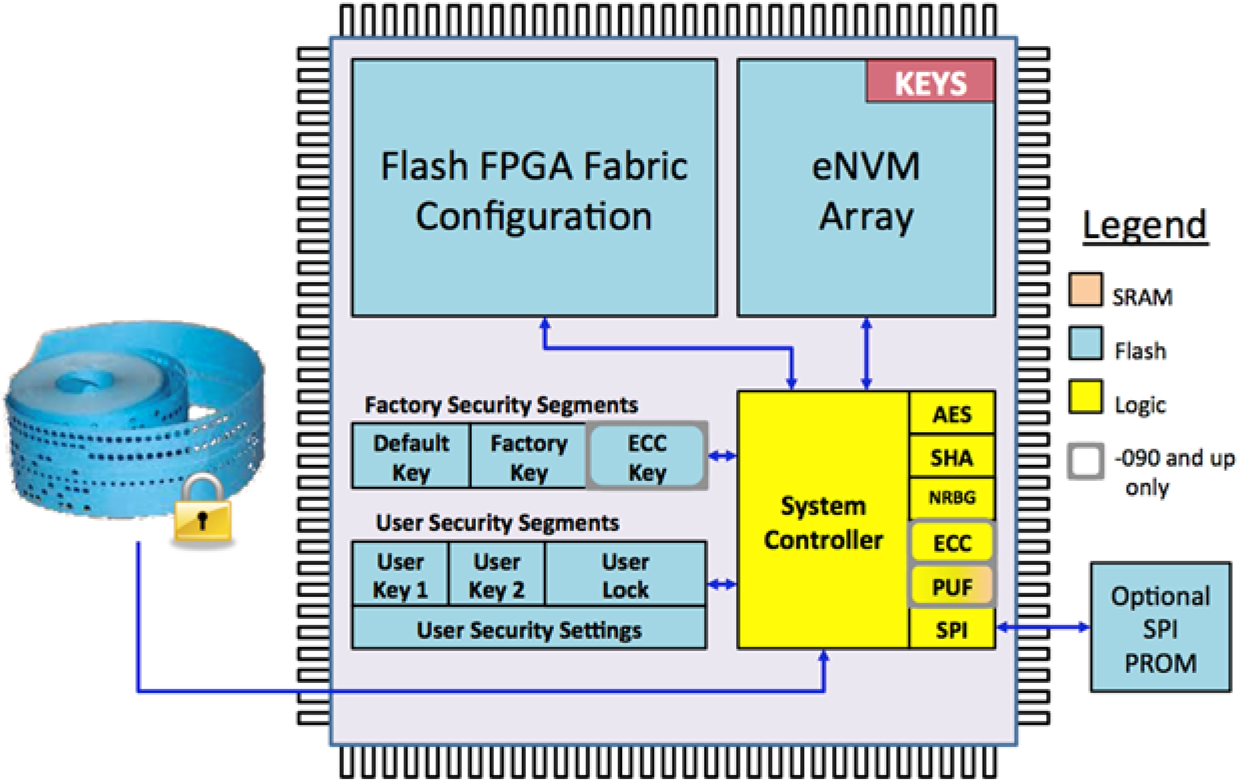

Figure 1: **Simplified Security Model for SmartFusion2 and IGLOO2**

System Controller

The system controller manages all programming, verification, Design Security key-management, and related operations. The system controller is a dedicated fixed-function hardened processor reserved for these functions, and is not reconfigurable in normal operation. Its programming and runtime operation are determined by a dedicated immutable metal-mask ROM. It also includes some dedicated scratch-pad SRAM, and hardware accelerators for specific cryptographic function support.

During programming, the system controller authenticates and decrypts incoming bitstreams, erases and writes the target flash memory segments, and responds to other external programming-related protocols, such as key verification. The system controller essentially programs what the bitstream tells it to in a secure, authenticated fashion. If the bitstream contains only an eNVM image then that’s what gets programmed. Possible bitstream configurations are:

- FPGA fabric only
- Entire eNVM only; Portion of an eNVM
- Security keys and settings
- Combinations of the above

During normal runtime operation, the system controller is instrumental in powering up the device. It also provides optional cryptographic services for advanced Data Security users.

These services can include functions such as an Advanced Encryption Standard engine, a SHA-256 Secure Hash engine, a Non-deterministic Random Bit Generator (NRBG), Elliptic Curve Cryptography, and SRAM-PUF. You can learn more about each of these services from the resources listed in the "To Learn More" section on page 6.

Security Segments

The heart of the security system is the robust storage of security keys. SmartFusion2 and IGLOO2 devices have several features that make it easy to create a robust key storage function. There are three user security segments (“User Keys 1”, “User Keys 2”, and “User Lock”). The first holds a user bitstream encryption key (UEK1). It can be the root key for encrypting and decrypting bitstreams, and for authentication of bitstreams. This segment also holds the FlashLock® passcode. It is used to unlock access to the three user security segments, if re-entered and matched correctly. A correct match allows the user to update the segment contents. It also unlocks many of the user lock-bits, until such time as the device is reset; allowing operations such as programming or verification to continue that may have been disallowed by the stored lock-bit settings.

The second user keys security segment stores a second user encryption key (UEK2). This can be used interchangeably with UEK1. This segment has its own passcode, which allows overwriting of the key and passcode, after the passcode is successfully matched (and before the device is reset). This passcode does not unlock anything in the User Key 1 or User Lock segments. Use of the second user keys segment is strictly optional. Having a second user key can facilitate use models that would be difficult to implement with just one user key, such as using the secondary key to program or update a subset or class of products versus all products that may be in the field.

The User Lock segment holds the majority of lock-bits for setting user security options. These include options for configuring both Design and Data Security. Many of the lock-bits are overridden if the FlashLock passcode is matched (assuming that other security options allow the FlashLock passcode to be active).

The FlashLock passcode is programmed as part of the initial user key injection procedure, and is stored in the user key security segment in hashed form. If it is re-entered and matched later, it will temporarily unlock the three user segments, allowing changes to the keys, passcodes, and security settings (for example, lock- bits) stored there. The unlocked state returns to the normal locked state (as defined by the lock-bit settings) on the next device or JTAG reset, or power cycle. This is also when any permanent changes written to the security NVM segments will take effect.

Finally, the Permanent FlashLock mode can be used to turn a SmartFusion2 or IGLOO2 device into an OTP device. This mode is considered quite secure because it disables most programming, verification, and debug operations. There are additional optional, layered, security settings (for example, additional lock-bits) that when used in conjunction with Permanent FlashLock mode can provide even higher levels of security:

- The factory test mode can be permanently disabled.
- The programming ports can be partially disabled:
  - The JTAG boundary scan instructions can be disabled (EXTEST, SAMPLE/PRELOAD, CLAMP, HIGHZ, and EXTEST2).
  - Virtually all JTAG and SPI programming instructions can be disabled so they are ignored when parsed, even before other lock-bits (for example, for disallowing overwriting of the NVM) are checked.

Secure FPGA Fabric

Unlike Flash On the Side (FOS) architectures (where on-chip Flash configuration storage is located outside the SRAM-based FPGA fabric), Microsemi flash-based FPGA configuration memory cells are located within the FPGA fabric and directly control the routing switches and look-up tables used to implement user logic. This means there is no turn-on delay due to moving configuration data from nonvolatile memory to control these resources (instant-on).

SRAM-based FPGAs configured through off-chip flash, even if the bitstream is encrypted, are vulnerable to side-channel attacks (side-channel attacks are explained in more detail in the "Improved Security for Key Storage" section below) since the bitstream must be loaded and decrypted on each power-up. Even though Microsemi FPGAs only need to be configured once during manufacturing, or during very infrequent field updates, as an added layer of security they only accept encrypted bitstreams. This prevents attacks attempting to reverse engineer bitstream configuration files. Researchers claim, and history confirms, that plaintext bitstreams can and will be reverse engineered. Allowing only encrypted bitstreams makes it much more difficult for the bitstream format to be reverse engineered by researchers, malicious users, or adversaries.

Protected Storage in the eNVM Storage Array

The embedded Nonvolatile Memory (eNVM) storage array within SmartFusion2 and IGLOO2 devices provides additional security capabilities to the designer. This memory array can be organized as separate pages each configured for specific functions. For example, pages can be designated as write-protected to make it easy to control sensitive data. Additionally, a novel NVM integrity check mechanism can be used to check the reliability and security of a device automatically upon power-up, or upon demand. The contents of all the nonvolatile configuration memory segments, FPGA fabric configuration, plus any eNVM pages declared as write-protected are digested (hashed) using the SHA-256 algorithm. The results are compared to values stored in dedicated non-volatile memory words located in each segment. If the contents are unchanged from when the digests were computed and stored during the original programming steps—that is, if the current and stored digests match, the test will pass; otherwise a failure is flagged. This test provides assurance against both natural and maliciously induced failures. These security features make it easy to provide higher levels of security without additional design effort or the use of additional user logic.

Improved Security for Key Storage

The use of security keys stored within SmartFusion2 or IGLOO2 device, is critical to all the major security operations implemented within the device. If these keys can be subject to an attack that can determine their values, the entire system can be compromised. Unfortunately, advanced cryptoanalysis techniques can be used to do just that by using the concept of a side-channel. A side-channel is the unintended ‘leakage’ of information about a security system due to the real world implementation of actual systems (as opposed to the clean ‘theoretical’ mathematical constructs security systems are conceived to operate within).

A simple example of a familiar side-channel is the one used by a safe cracker to determine the combination of a safe. By listening to the sounds made by the tumblers while manipulating the combination lock a skilled safe cracker can determine ‘side-channel’ information that can assist in cracking the otherwise very secure safe. Advanced safe designs will use mitigation techniques (sound dampening or false tumblers) to complicate this side-channel attack.

Electronic cryptographic systems also produce side-channels of information that can be observed by a determined attacker and used via cryptoanalysis to determine the value of security keys stored within a device. Power analysis is a very common attack. The attacker observes the power consumption (side-channel) used by the device during cryptographic activities. The power consumption varies depending on the value of the security key being used.

This can provide a determined attacker, if they have access to power measurements of multiple cryptographic operations, with enough data to significantly narrow the range of possible security key values and thus much more easily determine their actual value.

The use of this Differential Power Analysis (DPA) technique is so powerful that an extensive set of mitigation techniques has been developed by Cryptographic™Research Inc. (CRI, a division of Rambus). CRI owns a series of fundamental patents covering a variety of side-channel mitigation techniques.

Nearly all the secure microcontrollers used in smart cards, set-top boxes, SIM cards for GSM phones, and Trusted Platform Modules (TPM) for personal computers are built under license to CRI, amounting to over 7 billion chips per year in total.

Microsemi is the only FPGA manufacturer who has licensed the CRI patent portfolio, and SmartFusion2 and IGLOO2 devices both use extensive DPA mitigation techniques to protect security keys and the associated algorithms from side-channel attacks. You can learn more about Side-Channel Analysis from the resources listed in the "To Learn More" section below.

Conclusion

The world is on an unstoppable march towards open communications and automation. This is not new, this trend has been going on since time immemorial. What is new is that the pace of innovation is accelerating and this makes the need for Design Security more important than ever before. Microsemi FPGAs, which now have mainstream FPGA features like high-speed DSP blocks and 5 Gbps serial transceivers, are the only FPGAs on the market that have been designed with security in mind and implement key features that dramatically simplify the creation of secure embedded systems. The use of on-chip flash-based secure configuration memory, the inclusion of advanced features for robust secure key storage, DPA resistant hardware, and a variety of security services and options to protect design IP over the entire system life cycle dramatically simplify the creation of secure embedded systems. Microsemi FPGAs make it easy to provide a level of protection for your designs that no one else can match.

Microsemi has a wealth of information available on its Security website. To learn more about security topics related to those explored in this paper, explore the items listed below or other items available on our Security website.

To Learn More

1. Protect FPGAs from Power Analysis
2. Overview of Design Security Using Microsemi FPGAs and SoC FPGAs
3. Overview of Data Security Using Microsemi FPGAs and SoC FPGAs
4. SmartFusion2 and IGLOO2 Cryptography Services
5. Securing Your Embedded System Life Cycle
6. Securing Your Supply Chain Life Cycle

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