Implementation of Security in Microsemi ProASIC and ProASIC^{PLUS} Flash-Based FPGAs

Table of Contents

Introduction

As more of the traditional ASIC market is being serviced by field programmable gate arrays (FPGAs), the need for security on programmable logic devices increases dramatically. A few years ago, FPGAs were viewed as primarily glue logic with devices often being used to interface between ASSPs or custom ASICs. Today, as FPGAs grow in density and handle faster clock speeds, they are becoming effective ASIC alternatives. Today, many systems have most, if not all, of the sensitive IP contained in an FPGA. A typical system might incorporate a processor/DSP, some memory, a few ASSPs, and one or more FPGAs. If the contents of the FPGA can be read the user can duplicate or enhance the function of the entire system because all other components are off-the-shelf. The vulnerability of FPGAs to copying puts the intellectual property of the system at risk. The system is only as safe as the FPGA or ASIC in the design. Given the continued rapid adoption of FPGAs, security is a growing problem. Microsemi ProASIC® and ProASIC^{PLUS}® devices contain circuitry to make the Flashbased devices secure after configuration. Care must be taken in the design to make the locking circuitry very difficult to defeat through electronic or direct physical attack.

Types of Security

Microsemi offers two types of security:

- FlashLock®

The FlashLock feature in ProASIC and ProASIC^{PLUS} works through a key mechanism, where the user locks or unlocks the device with a user-defined key. When the device is locked, functions such as device read, write, verify, and erase are disabled. Without the correct key, no one can copy or reverse engineer the design in the FPGA. First, the device must be unlocked using the correct key in order to gain access to the FPGA.

- Permanent FlashLock

The purpose of the permanent lock feature is to provide the highest level of security to the ProASIC^{PLUS} family of devices. The permanent FlashLock feature creates a permanent barrier preventing any access to the contents of the device. This barrier is created by breaking the key after the device is secured. After permanently locking the device, access to the device is not possible even with the proper key. The device is effectively rendered as one-time programmable and therefore is very secure.

Security Key

Within each ProASIC or ProASIC^PLUS device, there is a multi-bit user key. The number of bits depends on the size of the ProASIC or ProASIC^PLUS device. Table 1 and Table 2 show the key size of different ProASIC and ProASIC^PLUS devices. After secured, Read permission and Write permission can only be enabled by providing the correct user key to first unlock the device.

The key size varies depending on the size of the device being used in the design. The length of the key makes it virtually impossible to attack the key using direct Brute Force techniques.

Table 1 • **Key Size of ProASIC Devices**

Device	Key Size (Bits)	Key Size (Hex)
A500K050	55	13
A500K130	93	23
A500K180	118	29
A500K270	143	35

Table 2 • **Key Size of ProASIC^PLUS Devices**

Device	Key Size (Bits)	Key Size (Hex)
APA075	79	19
APA150	79	19
APA300	79	19
APA450	119	29
APA600	167	41
APA750	191	47
APA1000	263	65

Are the Keys Secure

To unlock, the correct key must be loaded through the JTAG programming port. The maximum clock frequency of the JTAG port is 20 MHz. An exhaustive search would take at least

2ks/20 x106 seconds, where ks = key size

Table 3 and Table 4 on page 3 lists how many years are needed to uncover the key for Microsemi Flash devices.

Even using parallel test setups, exhaustive testing of keys would take prohibitively long. Note that care must be taken to use nontrivial keys during key selection.

Table 3 • **Years Needed to Uncover the Key ProASIC Devices**

Device	Years to Uncover the Key
A500K050	57
A500K130	1.57×10^{13}
A500K180	5.27×10^{20}
A500K270	1.77×10^{28}

Table 4 • **Years Needed to Uncover the Key ProASIC^{PLUS} Devices**

Device	Years to Uncover the Key
APA075	9.58×10^{8}
APA150	9.58×10^{8}
APA300	9.58×10^{8}
APA450	1.05×10^{21}
APA600	2.97×10^{35}
APA750	4.98×10^{42}
APA1000	2.35×10^{64}

Setting Security Keys and Permanent Lock in Microsemi Designer Software

The security feature is selected in Microsemi Designer software tool menu. To set the security key click Bitstream to get the Bitstream/STAPL generation dialog box. The user checks off the locking security option box and then the user can supply a user security key or can use the Generate random key feature in software. Generate random key automatically generates a security key for the user. The Bitstream/STAPL file contains a header where the security selections are specified, along with the user security key. It is assumed that if a user has a Bitstream/STAPL, they have control over the design. It is the user responsibility to ensure the safety and security of the keys. A valid security key consists of at least 13 hexadecimal characters with the highest order bit being zero. Microsemi Designer software checks to make sure that the security key specified by the user is legal, otherwise the Bitstream/STAPL is not secured. For example, if the security key is not of the required hexadecimal character size for the selected device, the software gives an error message Silicon security key must consist of 0 to N hexadecimal digits, where N is the maximum number of hexadecimal digits. Figure 1 and Figure 2 on page 4 show the designer bitstream dialog box. To use permanent lock, the user needs to check the Use permanent lock option which makes Designer generate a programming file with permanent lock. Figure 3 on page 4 shows a designer bitstream dialog box with a permanent lock option.

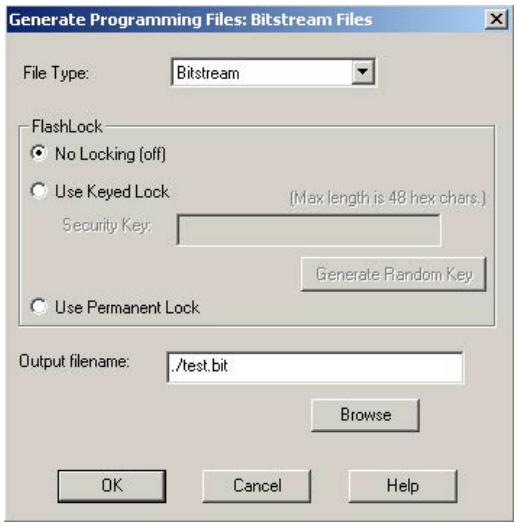

Figure 1 • **Default Settings for Bitstream Dialog Box**

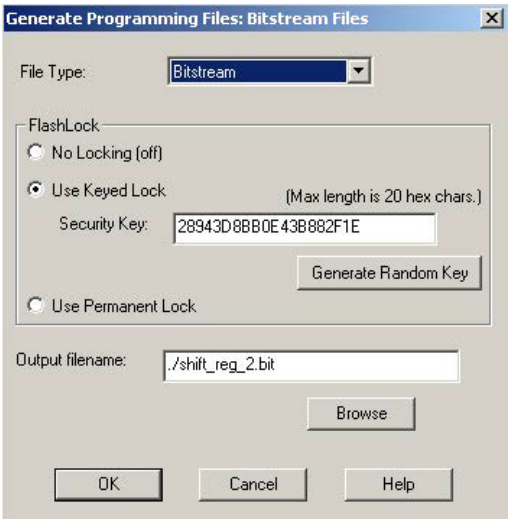

***Figure 2* • Dialog Box with Locking Selected, then Security Key is Selected**

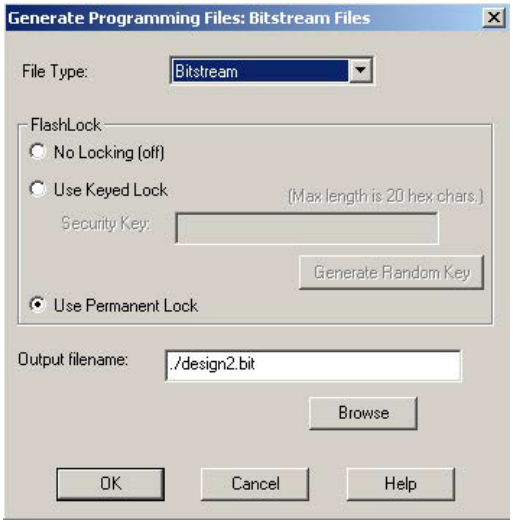

***Figure 3* • Dialog Box with Permanent Lock Selected**

Resultant Bitstream if the Security Key is Used

```
//BIT 6b2.42 apa
date Sun Aug 11 15:23:27 2002
user DastagirT
host Sun Aug 11 15:23:27 2002
pwd C:\APA\aa
design C:\APA\aa\test
package APA1000-BG456
architecture APA1000 1 1
jtag extended
security enable
key 2F743A351EBC3
```

```
tool map2bitstream 6b2.42
format 267 217
```

Resultant Bitstream if the Permanent Lock is Used

```
//BIT 4_6_0.01 apa
date Tue Jan 28 17:53:13 2003
user DastagirT
host Tue Jan 28 17:53:13 2003
pwd E:\APA
design design2
package APA150-PQ208
architecture APA150 1 1
jtag extended
security permanent
key 158699d368f596367f757
tool map2bitstream 4_6_0.01
format 83 65
```

Programming Security and Permanent Lock

There are three programming solutions available for ProASIC and ProASIC^{PLUS} devices: Silicon Sculptor FlashPro, and FlashPro Lite. If the programming file contains the security key and permanent lock, the Silicon Sculptor programming software automatically enables the Secure(key_lock) and Secure(per_lock) option. Figure 4, Figure 5 on page 6, and Figure 6 on page 6 shows the default settings for the Microsemi Silicon Sculptor programming software, if the programming file contains a security key and permanent lock. FlashPro software also automatically enables the Security and Permanent lock option during programming. Figure 7 on page 7 and Figure 8 on page 7 shows Microsemi FlashPro programming software settings in order to program security key and permanent lock. Once the part is programmed with the security feature, it is not readable, writeable, erasable, or reprogrammable without the user security key in the Bitstream/STAPL file. With the user security key in the Bitstream/STAPL file, the part can be erased and reprogrammed. As mentioned before, if the permanent lock feature is used, the device can never be programmed or erased even with a proper key.

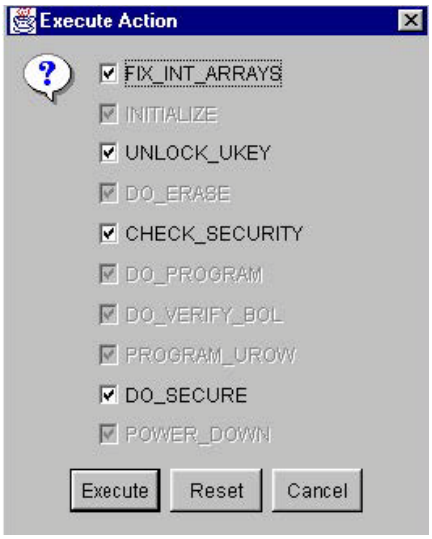

***Figure 4* • Silicon Sculptor Windows Software to Program Security Key**

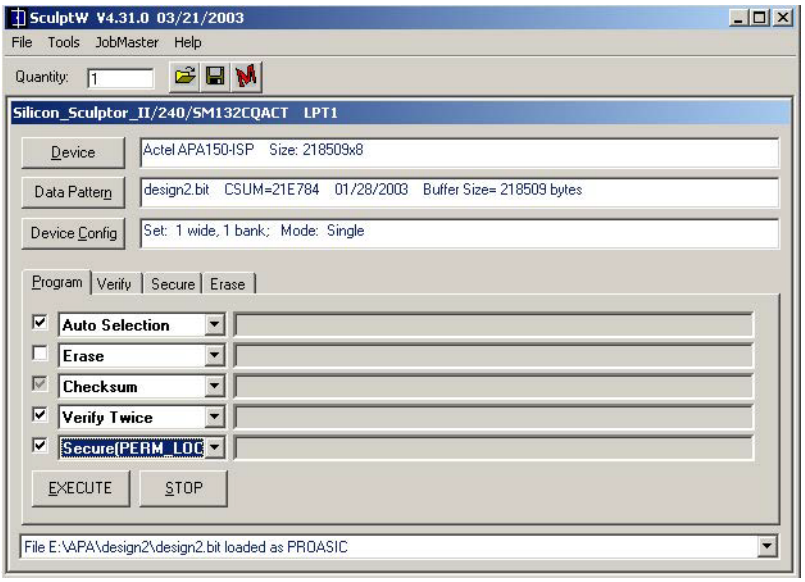

***Figure 5* • Silicon Sculptor Windows Software to Program Permanent Lock**

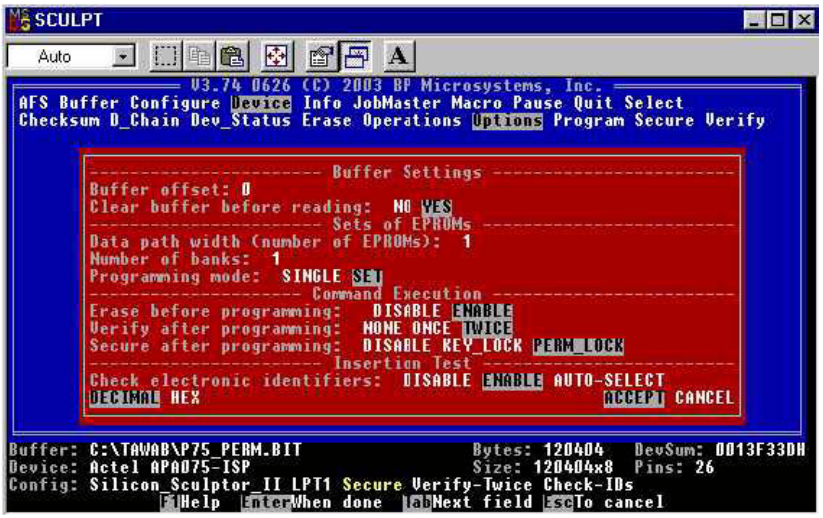

***Figure 6* • Silicon Sculptor DOS Software to Program Permanent Lock**

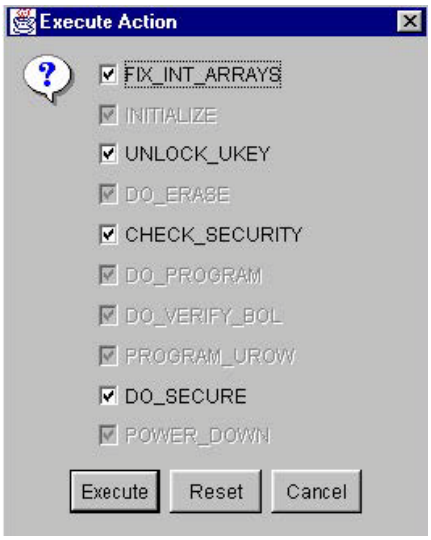

***Figure 7* • FlashPro Software to Program Security Key**

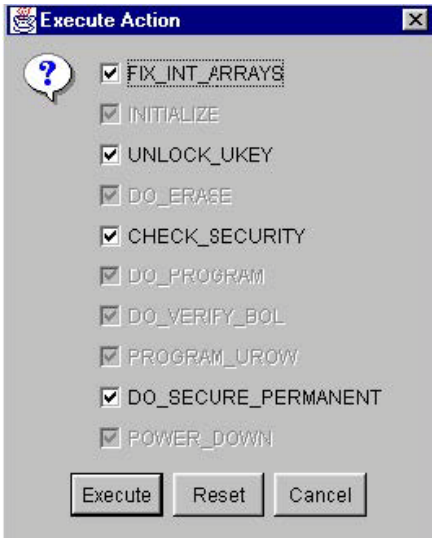

***Figure 8* • FlashPro Software to Program Permanent Lock**

Conclusion

ProASIC and ProASIC^{PLUS} Flash FPGAs are more secure against malicious attacks than SRAM FPGAs, which satisfies an increasingly important system requirement. These devices are architecturally designed to prevent attacks on a programmed device using either a programmer or any other electronic means. Programming the security key ensure the designer that the design or IP in the FPGAs is protected from being Cloned or reverse engineered.

List of Changes

The following table shows important changes made in this document for each revision.

Revision	Changes	Page
Revision 2 (June 2016)	Non-technical updates.	N/A
Revision 1 (September 2003)	Initial release	N/A

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo,
CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
E-mail: sales.support@microsemi.com
www.microsemi.com

About Microsemi

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; enterprise storage and communication solutions, security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 4,800 employees globally. Learn more at www.microsemi.com.

5192722-2/06.16