Implementation of Security in Actel's ProASIC and ProASIC^{PLUS} Flash-Based FPGAs

FlashLock™

Introduction

As more and more of the traditional ASIC market is being serviced by FPGAs, the need for security on programmable logic devices increases dramatically. A few years ago, FPGAs were viewed as primarily glue logic. They were considered relatively small devices that were often used to interface between ASSPs (Application Specific Standard Product) or custom ASICs. Today, as FPGAs grow in density and can handle ever faster clock speeds, they are increasingly used as ASIC alternatives. Many systems today 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, you can duplicate (or enhance) the function of the entire system since all other components are off-the-shelf. The vulnerability of FPGAs to copying puts the intellectual property of the system at risk. Given the continued rapid adoption of FPGAs, security is a growing problem. Actel's ProASIC and ProASIC^{PLUS} devices contain FlashLock™ circuitry to lock the device by disabling the programming and readback capabilities after programming. Care has been taken to make the locking circuitry very difficult to defeat through electronic or direct physical attack.

Security Key

Within each ProASIC and 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, respectively. Once 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 with the size of the device being used. The key length makes it difficult to attack the key via external brute force techniques.

Table 1 • *Key Size of ProASIC Devices*

Device	Key Size (bits)	Key Size (Hex)
A500K050	55 Bits	14
A500K130	93 Bits	24
A500K180	118 Bits	30
A500K270	143 Bits	36

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

Device	Key Size (Bits)	Key Size (Hex)
APA075	79 Bits	20
APA150	79 Bits	20
APA300	79 Bits	20
APA450	119 Bits	30
APA600	167 Bits	42
APA750	191 Bits	48
APA1000	263 Bits	66

Are the Keys Secure?

To unlock the device, the correct key must be loaded via the JTAG programming port. The maximum clock frequency of the JTAG port is 20 MHz. An exhaustive search would take at least $(2^{ks} * ks)/20x10^6$ seconds, where ks=key size.

Table 3 and Table 4 show how many years are needed to unlock the Actel Flash devices through an exhaustive key search.

Even you employ parallel test setups, exhaustive testing of keys would take an extremely long time. Therefore, care must be taken that trivial keys are not used during key selection.

Table 3 • *Years Needed to Unlock ProASIC Devices through an Exhaustive Search*

Device	Years to Unlock
A500K050	$3.1x10^4$
A500K130	$1.5x10^6$ Billion
A500K180	$6.21x10^{13}$ Billion
A500K270	$2.5x10^{21}$ Billion

Table 4 • *Years Needed to Unlock ProASIC^{PLUS} Devices through an Exhaustive Search*

Device	Years to Unlock
APA075	76 Billion
APA150	76 Billion
APA300	76 Billion
APA450	$1.2x10^{14}$ Billion
APA600	$5.0x10^{28}$ Billion
APA750	$9.5x\ 10^{35}$ Billion
APA1000	$6.2x10^{55}$ Billion

How to Set Security Keys in Actel Designer Software

The security feature is selected in the Designer Software tool menu. To set the security key, click bitstream to get the bitstream/STAPL generation dialog box. Then check the locking security option box and supply a user security key. The bitstream/STAPL file contains a header where the security selections are specified, along with the user security key. Assuming that you have a bitstream/STAPL file, then you have control over the design – no precautions are made to encrypt the bitstream/STAPL file. It is your responsibility to ensure the safe and secure keeping of keys.

A valid security key consists of at least 14 hexadecimal characters. Actel's 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 more than the required hexadecimal character size for the selected device, the software will give the following error message "silicon security key must consists of 0 to N hexadecimal digits," where N is the required number of hexadecimal digits. Figure 1 and Figure 2 show the Designer Software bitstream dialog box.

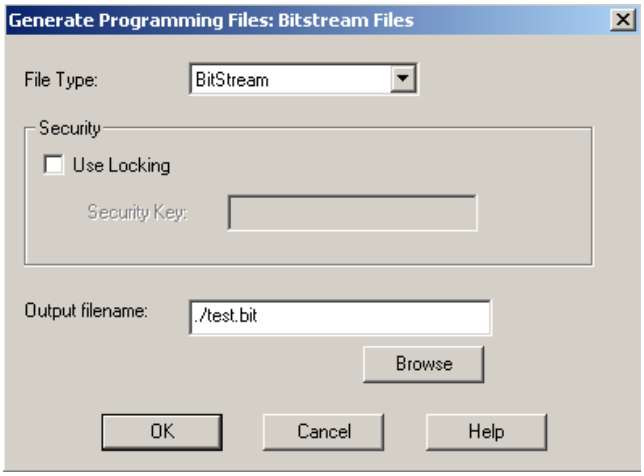

Figure 1 • *Default Settings for Bitstream Dialog Box*

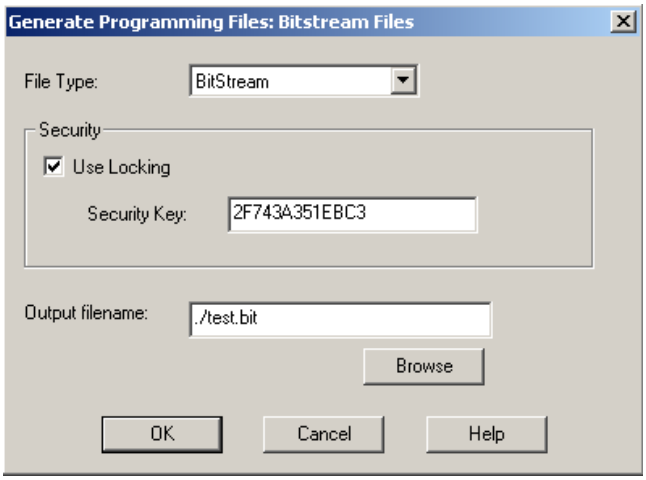

Figure 2 • *Security Lock Setting Dialog Box*

Resultant bitstream for the Figure 2 on page 2 dialog box entry is as follows:

```
//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
```

Programming Security Bit

Two device programmers, Silicon Sculptor and Flash Pro, are available for ProASIC and ProASIC^PLUS devices. If the programming file contains the security key, Silicon Sculptor programming software will automatically enable the "secure" option and will program the security key. Figure 3 and Figure 4 on page 4 show the default settings for the Actel Silicon Sculptor programming software, if the programming file contains the security key. Additionally, lash Pro software automatically enables the "security" option during programming. Figure 5 on page 4 shows Actel's Flash Pro device programming software settings, which allows you to program the security key. Once the part is programmed with the lock feature, it is not readable, writeable, erasable, or reprogrammable without the user security key (in the bitstream/STAPL file). With the user security key, the part can be erased and reprogrammed.

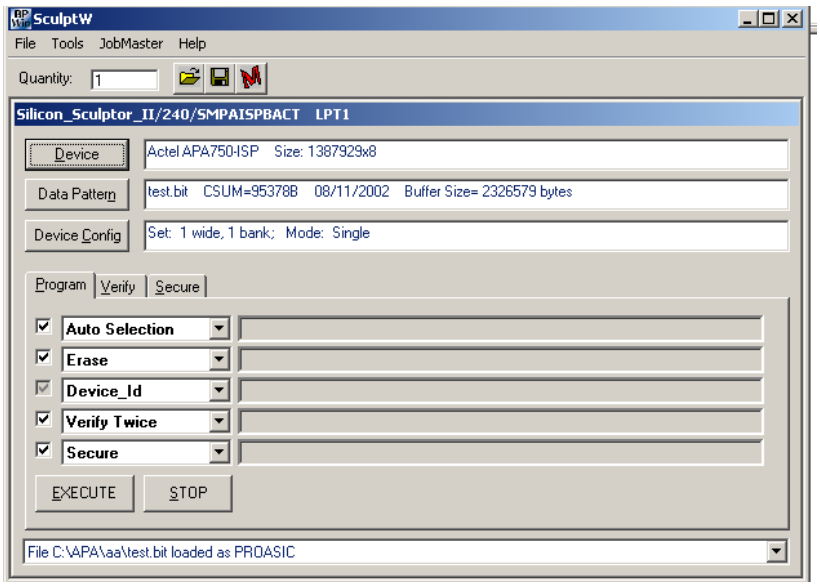

Figure 3 • *Silicon Sculptor Windows Software to Program Security Key*

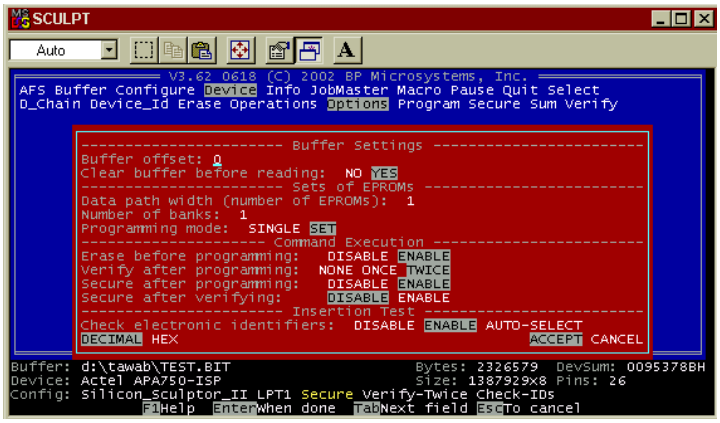

Figure 4 • *Silicon Sculptor Dos Software to Program Security Key*

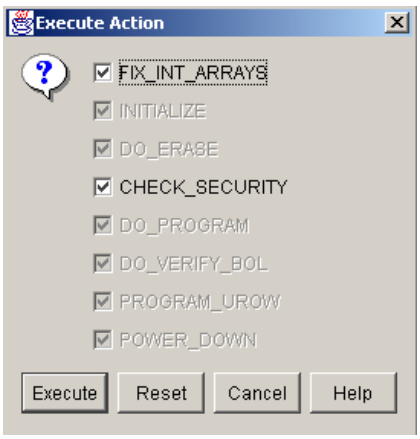

Figure 5 • *Flash Pro Software to Program Security Key*

Conclusion

ProASIC and ProASIC^PLUS Flash FPGAs are more secure against attack than SRAM FPGAs and satisfy an increasingly important system requirement. These devices are architecturally designed to prevent attack on a programmed device with a programmer or other electronic means. The programming security key ensures the design or IP in the FPGAs are protected from being "cloned" or reverse engineered.

http://www.actel.com

Actel Europe Ltd.
Maxfli Court, Riverside Way
Camberley, Surrey GU15 3YL
United Kingdom
Tel: +44 (0)1276 401450
Fax: +44 (0)1276 401490

Actel Corporation
955 East Arques Avenue
Sunnyvale, California 94086
USA
Tel: (408) 739-1010
Fax: (408) 739-1540

Actel Asia-Pacific
EXOS Ebisu Bldg. 4F
1-24-14 Ebisu Shibuya-ku
Tokyo 150 Japan
Tel: +81-(0)3-3445-7671
Fax: +81-(0)3-3445-7668

5192722-0/8.02