

Is Your FPGA Design Secure?



After spending months on your design, the last thing you want is to find your design has been stolen. Say goodbye to “locks,” “fuses,” “antifuses,” and other contraptions. You can sleep peacefully when you design with Xilinx.

by Anil Telikepalli
Marketing Manager, Virtex Solutions
Xilinx, Inc.
anil.telikepalli@xilinx.com

With an increased focus on security and terrorism in the world, it is natural for you (and me) to worry about the security of our designs and products. Are your ICs really foolproof? Can someone steal your design inside the chip? What about cloning? Reverse engineering?

Here at Xilinx, we want you to rest at ease. All Xilinx devices (FPGAs and CPLDs) have robust security mechanisms that make it nearly impossible to steal designs. In particular, Virtex-II Pro™ Platform FPGAs have advanced Triple DES (Data Encryption Standard) security embedded in them. We are not talking about my grandmother’s “secure” peppermint box with its heavy lock that you or I could crack open with a toothpick. Triple DES algorithms provide the same security that the world’s financial institutions rely on every day for transactions involving trillions of dollars. With security mechanisms you can “bank” on, let’s get into the details of design security and how Xilinx protects your valuable proprietary designs.

Design Security

Consider the philosophy of theft. There is nothing such as absolute security in this world. A determined thief can break any barrier if given enough time and resources.

Our goal is to make it extremely difficult to break that barrier. Hence, we've raised that barrier to the state of the art. Breaking the Xilinx barrier is virtually impossible for the vast majority of pirates. To help you understand just how we do this, let's look at the three basic levels of attack on a security barrier.

Categories of Security Attacks

IBM™ defined three categories of security attacks in a paper published in 1991. Although the paper is somewhat dated, it still serves as a pretty good reference (Abraham, D., G. Dolan, G. Double, and J. Stevens, 1991. Transaction Security System. *IBM Systems Journal* 30(2): 206-229.).

1. Class I: This is a clever outsider and a curious person with negligible resources. Representative of the majority of the population of hackers, he is not interested in wholesale piracy. He simply wants a capability for personal use. Seemingly harmless, this class of thief can pose a significant, worldwide threat if he shares the ill-gotten information on the Internet.
2. Class II: This person is a knowledgeable insider with access to some sophisticated resources. Examples include university students and unscrupulous corporate employees with access to the Internet. However, the information provided by this class tends to be esoteric and only usable by the same class or higher.
3. Class III: This is a funded organization with a determined team of experts – people who can crack open literally anything. Examples include the FBI, CIA, NSA, and any other large commercial or governmental operation with unlimited funds for wholesale reverse engineering operations.

Class I and Class II attacks can be deterred; a good IC helps the designer

achieve this objective. Xilinx Virtex-II Pro FPGAs provide a redundant key structure to thwart even most Class III attacks.

Programmable Device Security

There are two major types of design theft – cloning and reverse engineering. Cloning is copying the design as-is. Reverse engineering is more sophisticated stealing, where the thief extracts the design implemented in a device and then improves, modifies, and disguises it so that it no longer looks like the original implementation.

ASICs and ASSPs implement a fixed function and are vulnerable to attack, because every via/connection represents real logic. An attacker can de-cap such

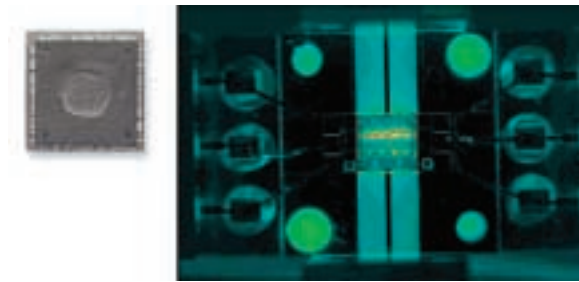


Figure 1 – An attacker can extract nonvolatile device die from a chip package and find security bits using thermal imaging.

chips to observe the vias and hack the design. Sometimes bogus logic is included to confuse the attacker, but the chips are still at risk. In general, the more fixed an IC is, the more the risk is. Plus, in a fixed IC, if you suspect that the security of one chip is compromised, then all the chips are compromised. With programmable ICs, however, if one chip is compromised, all the other chips can be reprogrammed.

Programmable devices (FPGAs and CPLDs) come in two types – nonvolatile (antifuse/flash) and volatile (SRAM) devices. There are many differences between them, each with unique advantages.

For our discussion on security, we will only focus on the security of the programming/configuration bits. Nonvolatile devices retain the configuration bits and do not need to load the bitstream from an external PROM every time they are powered up. In the past, the external PROM

was a cause for security concerns and non-volatile devices had a slightly upper hand.

But that was before the debut of the industry's first secure SRAM FPGAs in 2000 – the Xilinx Virtex™-II Platform FPGAs with Triple DES encryption.

Nonvolatile Programmable Devices

Let's take a look at today's nonvolatile programmable logic devices (PLDs) that include both FPGAs and CPLDs from competing vendors. These devices provide a test mode to observe the internal circuit to improve yields as well as a read-back mode for customers to inspect the programmed bits.

Both these modes expose the devices to attacks. To prevent such attacks, fixed security bits are built with antifuse or flash gates to prevent read/write from the device after it is ready. Here is the weakness: An attacker can implement a simple circuit in two identical devices – one secured and the other not. The security bits have fixed locations and can be distinguished by observing both the devices using thermal imaging (Figure 1). Once distinguished, the security bits can be disabled with a high-intensity light source impinging on the die to allow read-back. Any circuit implemented in that particular device is now available to the thief.

As device size increases in programmable devices, the configuration bitstream size increases. When key size also increases with the device size, it indicates a fixed location pattern of security bits. We can conclude that if one such device is cracked, the security of devices of all densities is cracked. Sounds scary? You bet.

Xilinx CoolRunner™-II CPLDs use flash technology, but they are different from other nonvolatile devices. CoolRunner-II CPLDs add multiple layers of security, with read/write-protect security bits that are hard to find. The bits are placed among the programming bits deep under several layers of metal.

The security bits are also placed in such a way that requires a specific sequencing of signals to set and clear

Figure 2 – Several metal layers in CoolRunner-II CPLDs prevent the theft of your design.



them, as well as charge pumping. In addition, four or five layers of metal (Figure 2) rule out direct exposure of top die to laser/electrical tampering.

Two CoolRunner-II CPLD technologies – DualEDGE and DataGATE – are schemes that also confuse attackers with double data operation and input signal locking under internal macrocell control. Furthermore, the legendary low power operation of CoolRunner-II CPLDs makes it difficult to see anything under thermal imaging. For more information on CoolRunner-II security, see the white paper “CoolRunner-II CPLDs in Secure Applications” at www.xilinx.com/publications/whitepapers/wp_pdf/wp170.pdf.

Volatile Programmable Devices

Volatile SRAM FPGAs lose the configuration bitstream whenever the power goes off, and thus they need an external memory to hold the bitstream. A typical application includes an external PROM next to the FPGA. The bitstream between the PROM and the FPGA is a cause for security concern for some designers.

To alleviate these concerns, Xilinx embedded Triple DES encryption technology into Virtex-II FPGAs three years ago.

The second generation of this technology is now embedded in the latest Virtex-II Pro FPGAs. With this scheme, the PROM contains the encrypted bitstream, which is decrypted inside the FPGA. No

read-back is allowed. Any form of attack on the FPGA erases the design. The best an attacker can do is to intercept the design between the PROM and the FPGA – but all he will obtain is the triple DES encrypted bitstream.

Security You Can Bank On

Triple DES is the pre-eminent encryption standard that is used by financial institutions for millions of transactions every day involving trillions of dollars.

This same technology is used to provide security for your designs in Xilinx FPGAs. Although there have been reports of the older DES standard being cracked, Triple DES is yet to be cracked.

Triple DES is an official NIST (National Institute of Standards and Technology) and American National Standards Institute (ANSI) X9.52 standard. AES (Advanced Encryption Standard) is the next generation of encryption that will be adopted by the industry if and when Triple DES is cracked. Encryption gurus are already working on developing future versions of AES in a constant effort to keep hackers at bay. With trillions of dollars at stake, millions of financial transactions, and perhaps thousands of hackers at work on various types of attacks, Triple DES has held its ground to date. This is why Xilinx chose Triple DES as the best encryption capability to use in its flagship Virtex-II Pro product line.

Triple DES is a symmetric encryption algorithm, which means the keys used to encrypt and decrypt are the same. The security of the data lies in the key – in contrast to public key systems such as RSA or PGP. Triple DES uses three keys and the encryption algorithm is repeated for each key for added security. Each key is 56 bit wide and encrypts 64-bit blocks at a time. For more information on the Triple DES standard, go to: www.itl.nist.gov/.

Triple DES in Virtex-II Pro FPGAs

Virtex-II Pro devices have an on-chip decryption engine that can be enabled to secure the configuration bitstream, and hence the FPGA. You can encrypt the bitstream in the Xilinx software with a set of keys, and the Virtex-II Pro device decrypts the incoming bitstream internally using the same set of keys (Figure 3).

Once the design is placed and routed in ISE tools, the encrypted configuration bitstream is generated using the ISE’s BitGen program with user-selected keys (Figure 4). The same keys are loaded into the FPGA through the JTAG port using the ISE iMPACT tools (Figure 5).

To program the keys into the device, the device has to be put into a key access mode, which automatically erases the FPGA – including any old keys and the actual bitstream. This also provides protection from attacks.

After the device is programmed with

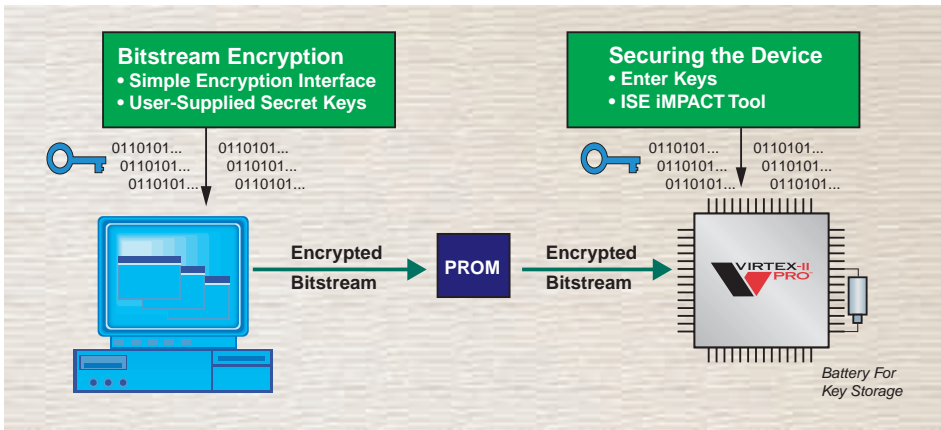


Figure 3 – Design security in Virtex-II Pro FPGAs using Triple DES encryption/decryption

keys, it can be configured with the encrypted bitstream. Once an encrypted bitstream has been programmed into the FPGA, it cannot be reconfigured, or partially configured, or read-back by unintended or intended tampering or snooping. Any attempt to steal a design automatically erases the FPGA completely. (Note that non-encrypted bitstreams may be programmed into an FPGA loaded with keys to facilitate test and debug.)

The keys reside in a special Triple DES block at the corner of the device. An external battery is used to hold the keys when the board is powered off. Any standard battery between 1V and 4V can be used, yielding a 15-year life.

Although nonvolatile PLD security bits disable read/write into the device, Virtex-II Pro Triple DES provides real security using encryption. Even though the location of the Triple DES block

in Virtex-II Pro FPGAs is known, the keys cannot be observed without erasing the chip.

Nine layers of metal pose yet another barrier to would-be thieves. Any attempt to use thermal imaging to find the security bits buried inside Virtex-II Pro FPGAs is destined to failure, because there isn't even hard wiring involved to store the security bits.

Each Virtex-II Pro device provides six separate keys, thus allowing two sets of Triple DES keys. You can program the devices up-front with both sets of keys. This provides security even against Class III attacks. For example, if the first key set

is compromised, you can remotely reprogram devices in the field with a bitstream using the second set of keys.

In addition, some of our customers use this technique for new business strategies and pricing models – one key set bitstream enables a low-price, low-feature service, and the other set activates a high-price, high-feature service.

Export Considerations

Encryption standards are tightly controlled in the U.S. by the Department of Commerce. The decryptor on the chip can only decrypt the incoming bitstream and is not available as a design block; hence, Virtex-II Pro FPGAs have been classified as field programmable logic

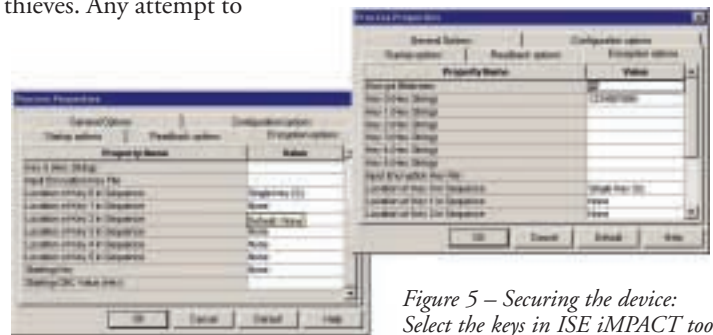



Figure 5 – Securing the device: Select the keys in ISE iMPACT tools.

devices (3A001.a.7), the same as any other FPGA. The software has been classified under ECCN# 5D002 and can be exported globally – with the exception of countries banned by the Department of Commerce. The bottom line is that no changes to your current export practices are necessary to include Virtex-II Pro FPGAs in your system.

Conclusion

Xilinx FPGAs and CPLDs provide unparalleled security for your designs, helping you achieve your design goals while maintaining the highest design security you can get.

This dedication to the protection of your designs is one of the reasons why Xilinx has become the largest vendor of programmable logic devices in the world. We offer the highest performance, lowest cost solutions with maximum design security so you can rest easy. 

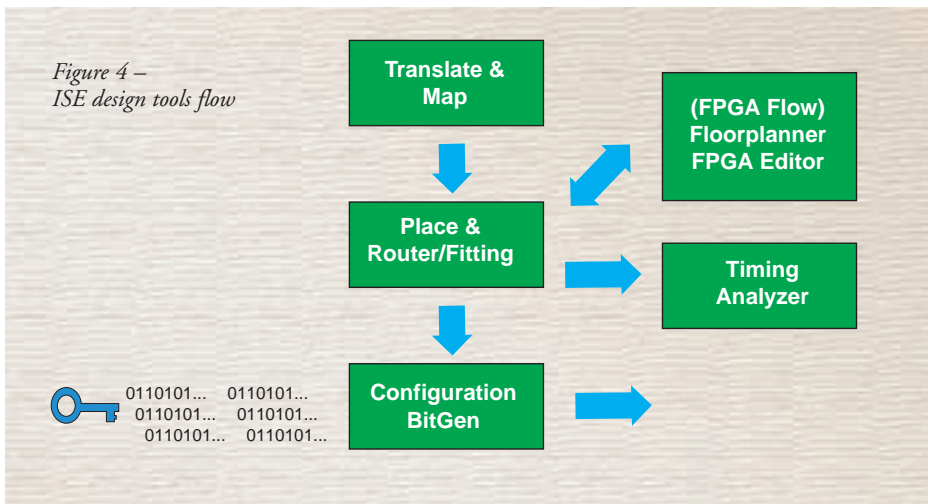


Figure 4 – ISE design tools flow