

Lock Your Designs with the Virtex-4 Security Solution

Virtex-4 FPGAs provide an up-to-date AES encryption scheme to prevent IP or microchip design theft.



by Chen Wei Tseng
Configuration Product PAE
Xilinx, Inc.
chenwei.tseng@xilinx.com

Because of the necessary configuration of FPGAs on each power up, as their popularity increases so do design security concerns. Without proper protections, attackers could easily clone or reverse-engineer the bitstream during FPGA configuration.

All Xilinx® Virtex-4™ devices have an on-chip decryptor that can be enabled to make the configuration bitstream secure. Virtex-4 has implemented the Advanced Encryption Standard (AES) scheme for securing the bitstream.

Modern Security Design

Xilinx has replaced the Triple DES encryption scheme implemented in the Virtex-II™ architecture with AES. Although both encryption schemes provide a high level of security, AES offers both increased security and throughput over Triple DES by replacing three 56-bit keys with one 256-bit key and allowing configuration clocking frequencies as high as 100 MHz.

Let's review some key benefits of the Xilinx Secure Chip solution.

1. AES is an official government standard, FIPS-197, supported by the National Institute of Standards and Technology and the U.S. Department of Commerce. The NSA has also certified AES' ability to protect classified communication to the top secret level.
2. The AES key can only be programmed through the JTAG interface. This allows you to monitor any unwanted activities on the JTAG lines both externally and internally with the BSCAN_Virtex4 primitive.
3. A battery-backed volatile key provides the maximum protection against hostile hacking.
4. This low-cost solution includes widely available standard components such as a Rayovac™ lithium battery.
5. Encryption key storage (Figure 1) has a long life span (20+ years).

Advanced Encryption Standard (AES)

Although the Triple DES algorithm remains effective against attacks, AES is now replacing DES in many applications as the most secure encryption scheme. As specified by FIPS-197, AES has the NSA-approved cryptographic algorithm that can be used to protect electronic data.

AES employs a cipher block that eliminates symmetry in the behavior of the cipher to overcome shortcomings of the DES' key. The non-linearity of the AES key expansion practically eliminates the possibility of equivalent keys.

Because of its key strength, AES is suited for applications such as banking, defense, government, and sophisticated technical applications such as ATM, HDTV, broadband ISDN, voice, and satellite.

Data Encryption Support

The Virtex-4 AES system comprises software-based bitstream encryption and on-chip AES (Rijndael) decryption with cipher block chaining (CBC) to decrypt the incoming bitstream. The AES key is stored in dedicated memory, powered by

either an auxiliary power supply (V_{CCAUX}) or an externally connected battery.

To combat a brute-force software attack such as key search, Virtex-4 devices feature a 256-bit AES key system that enables 1.1×10^{77} possible key combinations. To program the key, the device must enter "key-access mode" in IEEE1532 flow via JTAG. Once in this mode, the previous encrypt-

configuration interface as SelectMAP to access configuration logic internally so that you can partially reconfigure the device for extra design security.

In addition to ICAP, Virtex-4 devices can monitor activities on the external JTAG pins with the internal BSCAN_Virtex4 primitive. The BSCAN_Virtex4 primitive mirrors the activity on the TDI pin and

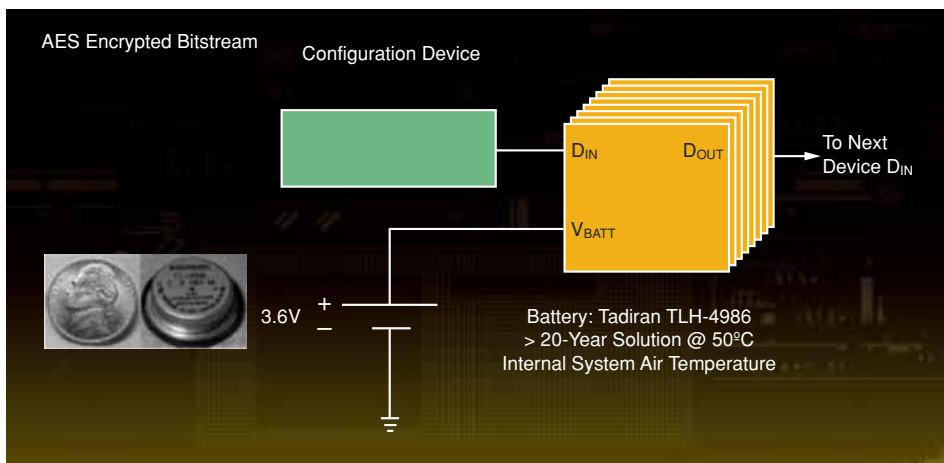


Figure 1 – Encrypted bitstream reference circuit for system-level applications

tion key will be cleared to prevent readback of the key. (Further flow details are documented in the Virtex-4 1532 BSDL files.) If the encryption keys are compromised, you can update the design with new keys and new encrypted bitstreams.

Virtex-4 FPGAs also embed the memory holding the key under layers of metal. Because the key is stored in volatile memory, disrupting the power supply for the key memory during hardware attacks will result in key loss.

You can always use a non-encrypted bitstream to configure the device regardless of the presence of the key. For example, when loading a non-encrypted bitstream, you should be careful when generating the bitstream. The proper security level should be set if you want readback of the non-encrypted bitstream. Reconfiguring the encrypted bitstream, however, would require you to toggle the PROG pin, cycle power, or issue one of two JTAG instructions: JPROG or JSTART.

Internally, you can use the internal configuration access port (ICAP) to reconfigure the device. ICAP provides the same

outputs several JTAG tap controller states, such as Test-Logic-Reset or Update-DR. Tampering with the JTAG during a "side channel" attack can be detected. You can then take countermeasures such as cutting power to the FPGA – including V_{BATT} – or erasing and writing a new encryption key by once again entering the key access mode.

Moreover, you can return any faulty part to Xilinx for testing without having to provide the encryption key for returned material analysis.

Software Integration

Xilinx ISE™ version 7.1i will have full software support for encrypted bitstream and key creation. Generating an encrypted bitstream requires only two additional bitgen options. For example, "bitgen -g encrypt: yes -g key0:AA995566 top.ncd top.bit" will automatically create an encrypted bitstream (top.bit) and the encryption key (top.nky) with the key of "AA995566." You must then load the top.nky file into the device through the JTAG interface before loading the encrypted bitstream.

Designing secure systems incorporating batteries for volatile storage is a proven method in multiple markets that is recognized as the highest form of security...

As for the GUI, Xilinx Project Navigator offers encryption options in the Generate Programming File command. You can set preferences for allowing readback, partial reconfiguration, and encryption.

iMPACT, the Xilinx programming tool, allows you to program just the key or the encrypted bitstream with the key. For independent programming applications, the detailed steps to download the encryption key are documented in the Virtex-4 IEEE1532 BSDL files, which are installed in the Xilinx/Virtex4/data directory with ISE installation, or downloadable from www.xilinx.com/support/sw_bsdll.htm.

Battery-Secured Systems

Designing secure systems incorporating batteries for volatile storage is a proven method in multiple markets that is recognized as the highest form of security and is required by the U.S. government for its secured modules (<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>).

Several misconceptions exist related to battery use – some believe that batteries will require additional maintenance cycles. These fears are unfounded: maintenance and lifetime are of no concern for most applications, and the lifetime of the battery will usually far exceed the useful lifetime of the product.

All batteries “self discharge” when sitting idle, even with no load. Modern lithium batteries feature extremely low self-discharge rates. Rayovac lithium batteries self-discharge at a rate of less than 0.3% per year. Even at higher temperatures, the self-discharge experiences only very minor deterioration – in this example, let’s use a conservative 0.6%. The capacity of the BR1225 is 50 mAh.

Assume that the Virtex-4 I_{BATT} current value is 50 nA. The V_{BATT} signal is routed internally to the PCB to eliminate leakage currents. The self-discharge per hour is 34 nA.

$$34 \text{ nA} + 50 \text{ nA} = 84 \text{ nA}$$

$$50 \text{ mAh} / 0.000084 \text{ mA} = \\ 595238 \text{ hours} = \sim 67 \text{ years}$$

Thus, a 20-year product life is easily achieved using a battery.

For more information about battery life expectancy calculations and design considerations, see Xilinx XAPP766, “Using High Security Features in Virtex-II Series FPGAs,” at <http://www.xilinx.com/bvdocs/appnotes/xapp766.pdf>.

Conclusion

Virtex-4 devices provide the most up-to-date security option for your designs. With the ease of integrated software flow, minimal board space requirements, and maximum security through AES, the Virtex-4 Secure Chip AES security solution is ideal for keeping hackers from your designs.

For more information about the Advanced Encryption Standard, please visit:

- <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- <http://csrc.nist.gov/encryption/aes/rijndael/>
- <http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf>
- <http://csrc.nist.gov/encryption/aes/>
- <http://csrc.nist.gov/encryption/aes/round2/r2report.pdf>
- <http://csrc.nist.gov/encryption/aes/round2/NSA-AESfinalreport.pdf>

Let Xilinx help you get your message out to thousands of programmable logic users worldwide.

That’s right ... by advertising your product or service in the *Xilinx Xcell Journal*, you’ll reach more than 70,000 engineers, designers, and engineering managers worldwide.

The *Xilinx Xcell Journal* is an award-winning publication, dedicated specifically to helping programmable logic users – and it works.

We offer affordable advertising rates and a variety of advertisement sizes to meet any budget!

Call today :
(800) 493-5551
or e-mail us at
xcelladsales@aol.com

Join the other leaders
in our industry and advertise
in the *Xcell Journal*!

**XILINX**®