XAPP766 (v1.0) July 8, 2004

Using High Security Features in Virtex-II Series FPGAs

Author: Ralf Krueger

Summary

This application note shows how a designer can very simply implement a battery with the Virtex™-II series FPGAs for high bitstream security. It shows a number of Xilinx recommended designs.

Introduction

All Virtex-II family members (Virtex-II, Virtex-II Pro™, and Virtex-II Pro X FPGAs) have an on-chip decryptor that can be enabled to make the configuration bitstream (and thus the whole logic design) secure. Xilinx implements a standard triple DES (TDES) scheme for securing a bitstream. TDES is considered very safe in industry, military, and government applications. This scheme is used daily by banks to transfer trillions of dollars around the world.

The user can encrypt the bitstream in the Xilinx software, and the Virtex-II chip then performs the reverse operation, decrypting the incoming bitstream and internally recreating the intended configuration. This method provides a very high degree of design security.

The Virtex-II device families store the internal decryption keys in a few hundred bits of dedicated RAM, backed up by a small, externally connected battery. This battery backed-up key is the most secure solution since the keys are erased if the FPGA is tampered with.

The key benefits of the Xilinx SecureChip security solution are summarized below:

- Battery-backed volatile keys provide the highest degree of security
- Simple, well-understood, and low-cost solution with widely available standard components

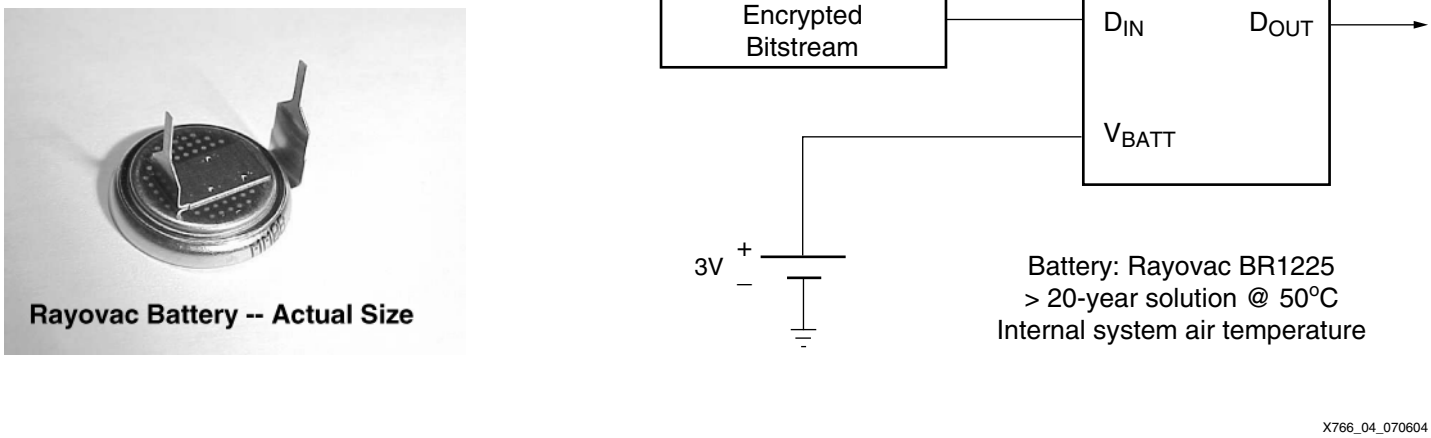

Figure 1: **Single Device Bitstream Security Reference Circuit**

Figure 1 shows an industrial-strength encrypted bitstream reference circuit using a Rayovac BR1225 lithium battery with a greater than 20-year lifetime for this application. The configuration device (for example, a Xilinx PROM) contains a TDES encrypted bitstream generated by Bitgen in ISE. Two sets of TDES keys for a total of six keys (each key is 56 bits) can be loaded in the FPGA. Keys to decrypt the bitstream upon configuration are loaded into the Virtex-II Series device via the JTAG port and are kept alive by the battery circuit when the system is unpowered. Most likely this process is done during manufacturing. In this application, the Rayovac BR1225 keeps the key alive for greater than 20 years, the lifetime of the battery, whether the system is powered on or not. The Rayovac BR1225 is priced just below $1.70 for quantities of 1000.

Other benefits of the Xilinx SecureChip security solution are:

- Intrusion detection can turn off the battery
- Keys can be changed and reloaded for increased security, even across the network
- 1 – 6 DES keys for maximum protection (two TDES key sets)
- Can be directly connected to a battery system already on-board
- No “custom” FPGAs with full RMA support
- No maintenance required

Secure Reconfiguration

Programmable logic devices enable a system design methodology to remotely update systems securely and reliably. FPGAs are inherently capable of changing their functionalities with a new bitstream, for example, to make design corrections and feature upgrades in the field. Said bitstream can be secured by the Xilinx SecureChip technology, which is implemented based on the TDES standard. The encrypted bitstream can be simply shipped across the Internet and is then decrypted when loaded into the FPGA via the keys that were loaded during the manufacturing process. Figure 2 shows an example of a secure remote reconfiguration over the Internet using TDES.

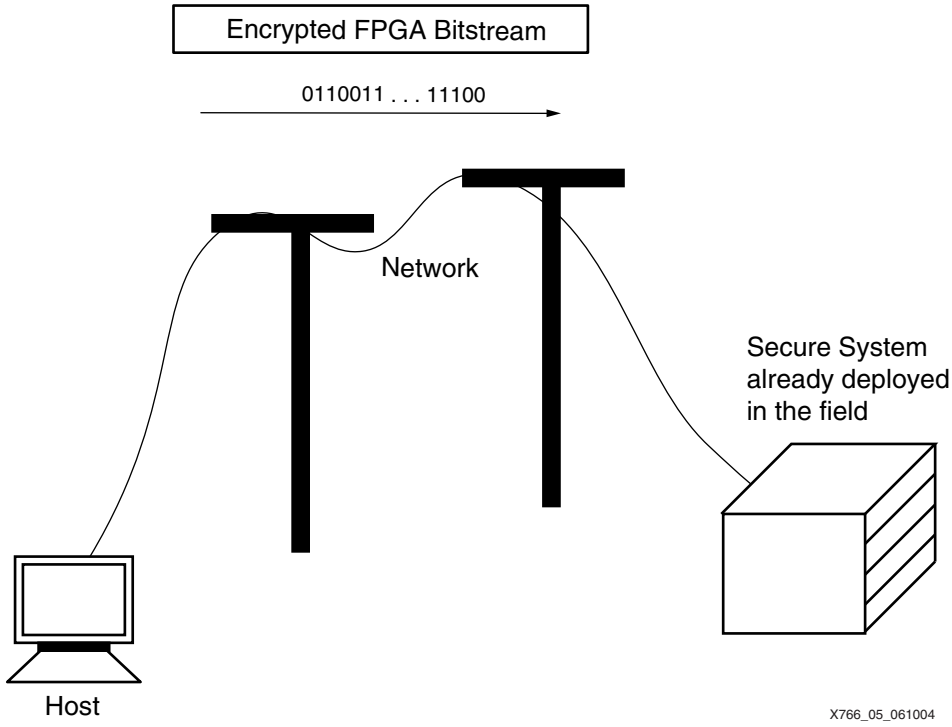

Figure 2: **Secure Reconfiguration over the Network**

Calculating the Rayovac Battery's Lifetime

All batteries "self discharge" when sitting idle, even with no load. Modern lithium batteries feature extremely low self-discharge rates. The Rayovac lithium battery shown in Figure 1 self-discharges at a rate of less than 0.3% per year. Even at higher temperatures, the self-discharge experiences only very minor deterioration. This example uses a conservative 0.6%. The capacity of the BR1225 is 50 mAh. For the Virtex-II Series reference circuit shown in Figure 1, the I_{BATT} current datasheet value is 50 nA (typical). The V_{BATT} signal is routed internal to the PCB to eliminate leakage currents. The self-discharge per hour is 34 nA.

34 nA + 50 nA = 84 nA

50 mAh / 0.000084 mA = 595238 hours = ~67 years

Thus a 20-year product life is easily achieved using this battery with a large margin.

Data Encryption Standard (DES)

Since the development of the Data Encryption Standard (DES), the DES algorithm has been used in countless applications. The Triple DES (TDES) algorithm was added to the standard in the late 1990s. The TDES algorithm performs three successive encryption-decryption-encryption operations using three different (56-bit) key sets and has never been cracked. TDES is a symmetric encryption standard supported by the National Institute of Standards and Technology (NIST) and the U.S. Department of Commerce. The term *symmetrical* simply implies that the same keys are used for decryption and encryption. DES and TDES can be used royalty free.

Because of its key strength ($3.7*10^{50}$), TDES is considered absolutely secure and is used in highly sensitive applications. For example, it is used in bank transactions around the world in home banking systems and the Secure Electronic Transaction (SET) used by MasterCard and Visa. Large parts of the internet rely on TDES. The Internet Protocol Security (IPsec) standard implements this solution for providing enhanced security features by creating a Virtual Private Network (VPN) tunnel between any pair of sites connected to the network.

For further information on DES and TDES, refer to the following links:

- http://www.xilinx.com/bvdocs/whitepapers/wp115.pdf
- http://www.xilinx.com/xcell//xl36/xl36_26.pdf
- http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
- http://csrc.nist.gov/cryptval/des/desval.html
- http://www.laynetworks.com/des.htm
- http://www.infomosaic.net/Encryption.htm
- http://www.ams.org/notices/200003/fea-landau.pdf
- http://www.bletchleypark.net/crypt/des.html

Data Encryption in Virtex-II FPGAs

All members of the Virtex-II families implement TDES. Once a key is loaded into the device and power is cycled, the key cannot be read back under any circumstance. Immediately after the key is programmed, it can be read back for verification. However, a new key can be loaded at any time, replacing the existing key. This also clears the configuration memory. Bitstream readback and partial reconfiguration are disabled. An unencrypted design can be loaded into the FPGA, which supports production test and the RMA process. The DES descriptor is not accessible by the FPGA fabric or any other means. Only the DES descriptor can read from the battery-backed memory. In addition, the decrypted bitstream is protected by a CRC computed upon configuring the FPGA. Thus, a transmission error or incorrect bitstream is detected, preventing the part from starting up and preventing any damage to the device.

Batteries to Secure 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. Storing keys in volatile memory is very secure. Remove the power, and the keys are gone. In fact, this scheme is so secure that the U.S. Government requires it for its secured modules (FIPS PUB 140-2):

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

A non-volatile (NV) key management cannot meet these requirements. The keys are permanently stored on the device, powered or not. Flash-based NV storage can be overwritten, but it needs a series of active operations from the processor. The battery solution provides an easy, fast, and mechanical zeroization of the keys and is the best solution for key protection.

Volatile storage makes the life of the adversary who tries to attack your system much harder than hardcoded key management schemes, both in time and price. Attempting a physical attack on a system that must be continuously powered is not only time-consuming and costly, but also requires a large supply of powered parts that have the same key in them. Consequently, the attack becomes uneconomical, because it costs more than the value of the information protected by the keys. The security lies only in the key (Kerckhoffs' assumption), which is what the attackers are trying to find.

Another option for attackers who want to break a system is a brute-force attack on TDES. However, with current technology and without large government backup, this endeavor is futile.

For extra protection, a design can be enclosed in the system such that, in case of tampering, the power is disconnected, leaving the would-be attacker with a useless piece of hardware.

The use of batteries to secure applications has also found its way into commercial products. For example, consider set-top boxes and cable descramblers. Cable companies often want the highest degree of security to make it impossible to alter their boxes. Cable descramblers are manufactured in high volumes and must be extremely reliable. Figure 3 shows one provider's set-top box system that uses a lithium battery to secure information. Batteries can be soldered directly onto the board for reliability. They have a very low FIT rate (50 or less).

Figure 3: **Set-Top Box System**

Other Methods of Storing Keys in Non-Xilinx Devices

An alternate method of storing a key is to add non-volatile memory cells to the FPGA. Using Flash memory is prohibitively expensive since it adds many layers to the process or might not even be available in the most advanced process technology.

A laser fuse technology can be used to program the key prior to packaging. However, this method requires the key to be handed over to the manufacturer. In addition, these types of structures are relatively large and can be easily reverse engineered.

Another method is to use programmable fuses (eFUSEs) in CMOS. A sufficient number of eFUSE cells can be used to program and hold the key. The key can then be programmed at any time after the chip has been packaged, eliminating the problem of not controlling the key. However, eFUSE structures still have large footprints and can be easily reverse engineered. Figure 4a shows a fuse before programming, and Figure 4b shows a fuse that has been programmed. The high programming current requires large structures that are easily identified on the chip.

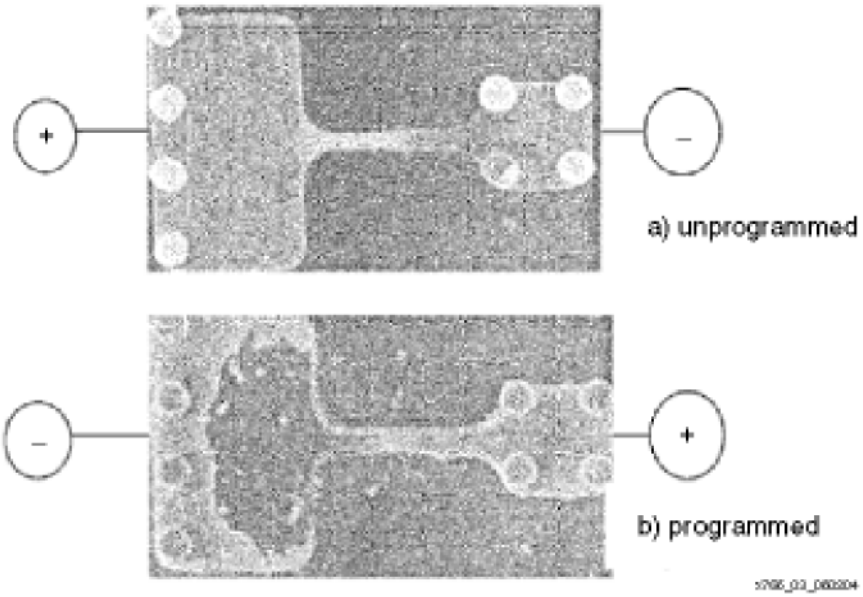

Figure 4: **eFUSE Layouts**

Design Example

For Tadiran lithium batteries, the self-discharge current varies with both background current (external load) and temperature. Typical self-discharge values for the TLH-4986 battery are shown in Table 1. Check with Tadiran to get the latest TLH-4986 self-discharge values at http://www.tadiran.com/home.php.

Table 1: **TLH-4986 Typical Self-Discharge Values for Different Background Currents (bc) and Temperatures**

bc, µA	-30°C	-20°C	-10°C	0°C	10°C	20°C	30°C	40°C	50°C	60°C	70°C
0.7	0.28	0.29	0.31	0.32	0.34	0.35	0.53	0.70	1.05	1.40	2.10
1.25	0.31	0.32	0.34	0.35	0.37	0.39	0.58	0.77	1.155	1.54	2.31

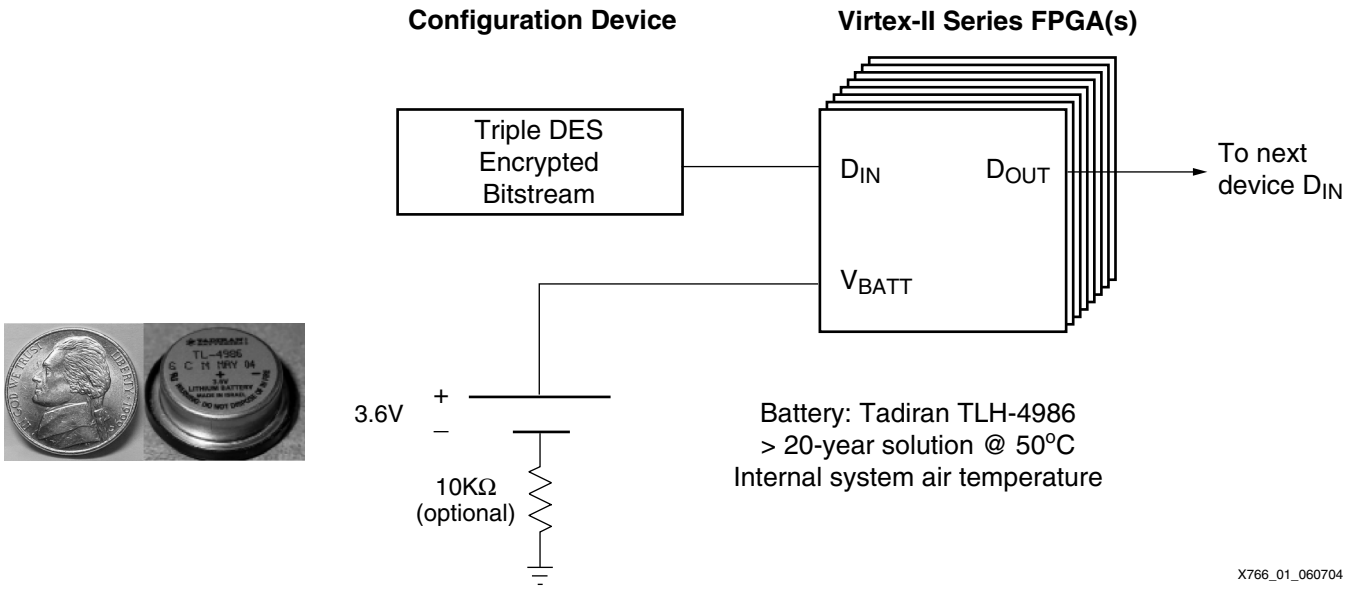

Figure 5: **Encrypted Bitstream Reference Circuit for System-Level Applications**

For the Virtex-II Series reference circuit shown in Figure 5, the I_{BATT} current datasheet value is 50 nA (worst case). The V_{BATT} signal is routed internal to the PCB to eliminate leakage currents. Fourteen Virtex-II Pro FPGAs can be supported with a battery background current of 700 nA.

14 * 50 nA = 700 nA

Assuming a typical end-product operating environment of 30°C ambient with a 20°C temperature rise inside the system yields a battery temperature of 50°C.

From Table 1, there is an additional 1.05 µA of self-discharge current at 50°C. The total current is then 0.7 + 1.05 = 1.75 µA. The application lifetime is 400 mAh/0.00175 mA = 228,571 hours, or 26 years, at 50°C.

Using Table 1, the battery maintains the DES keys in the Virtex-II device for 41 years at a 40°C battery temperature and 18 years at a very high 70°C battery temperature.

The battery backed-up RAM (BBRAM) array in the FPGA requires either V_{CCAUX} or V_{BATT} to keep the key programmed. Please reference the DC and Switching Characteristics datasheet of the Virtex-II device for V_{BATT} and I_{BATT} specifications. Once the V_{CCAUX} power for the Virtex-II device is applied, the BBRAM is no longer powered from the V_{BATT} pin. However, the leakage specification (I_{BATT}) still applies, as leakage results primarily from secondary structures rather than from the BBRAM itself.

The optional 10 KΩ resistor allows the current sourced by the battery to be measured and monitored in manufacturing. Since each part is expected to draw no more than 50 nA for 14 FPGAs, no more than 0.7mV can be expected for a test voltage.

Figure 6 shows a secure system incorporating a Tadiran lithium battery.

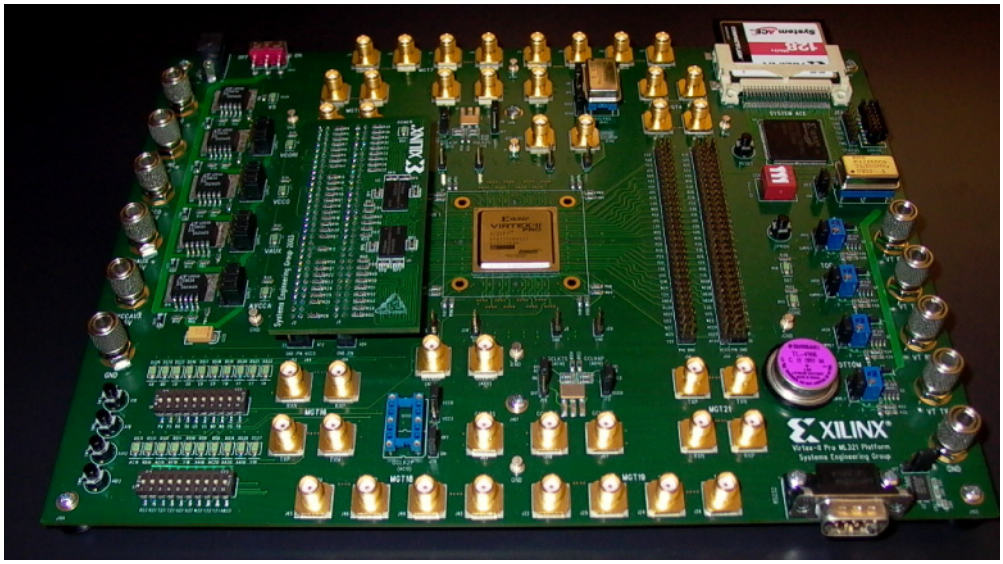

Figure 6: **Secure System with Tadiran Battery**

Conclusion

This application note describes the Xilinx SecureChip security solution and shows that the Virtex-II series of FPGAs with a variety of batteries can provide a secure configuration bitstream.

Revision History

The following table shows the revision history for this document.

Date	Version	Revision
07/08/04	1.0	Initial Xilinx release.