Design Security for High Volume Applications

The Global Threat of Counterfeiting

- Growing rapidly at over 12% per year, all industries are affected by counterfeiting, including: consumer electronics, microprocessors, gaming controllers, routers and semiconductor devices
- In 2004 alone, the World Customs Organization estimated $512B in lost sales due to counterfeit products
- Most common security breaches are through reverse engineering, cloning, over building and tampering

The Xilinx Solutions

- With configuration-data protection and unexposed bitstream, the CoolRunner™-II CPLD provides the lowest-cost solution for design security
- The unique Device DNA serial number in the Extended Spartan-3A Family helps deliver a robust solution to deter reverse-engineering, cloning, tampering and overbuilding

The Critical Need for Design Security

Counterfeit products can severely damage a company's revenues and customer credibility. Quality issues resulting from sub-standard, cloned products can also seriously cripple a company's support structure, and adversely impact their financial bottom-line.

Top Security Breaches For Designs Today

Reverse-engineering occurs when individuals recreate a portion, or an entire design with the idea of selling it as an enhanced product, cheaper alternative, or both. Cloning is the illegal duplication of a design, then selling it under the same or a different label. Overbuilding refers to contract manufacturers making additional quantities of a designated product without authorization from the Original Equipment Manufacturers (OEM). Tampering means to modify or replace a design for devious objectives, such as gaining access to unauthorized services or sabotaging an application.

Xilinx's Comprehensive Security Portfolio

For the most severe threats, the Virtex™-5 family supports on-chip, 256-bit AES encryption/decryption technology, with a battery-backed key. In the high-volume market, served by CoolRunner-II CPLDs and Extended Spartan-3A Family FPGAs, technologies such as configuration-data protection, hidden bitstream, JTAG lockdown, and Device DNA Design Level Security, offer low cost, and yet highly robust solutions for protecting both hardware and software IP (Intellectual Property).

XILINX®

High Volume Security Solutions

With a wide range of available security technologies for CoolRunner-II CPLDs and Extended Spartan-3A Family FPGAs, customers have ultimate flexibility to customize solutions based on their unique design requirements.

Configuration-Data Protection

When enabled, the multi-bit, "read/write" protect feature in CoolRunner-II CPLDs helps prevent reading and writing of the configuration data. Buried under layers of metal, the security bits are extremely difficult to locate and tamper. The configuration data can also be protected in Extended Spartan-3A Family devices by hardwiring the select mode pins for Flash auto-configuration only.

Hidden Bitstream

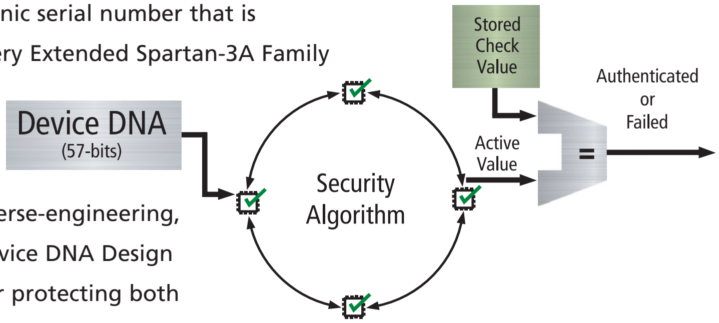
The configuration bitstream in CoolRunner-II CPLDs and Spartan-3AN FPGAs is stored in on-chip non-volatile memory and therefore, not exposed to the external world. The hidden bitstream helps protect designs against unauthorized "bitstream snooping," and subsequent cloning of the design.

JTAG Lockdown

JTAG provides a "backdoor" access to intruders who might steal design information and/or load unauthorized configuration files. Both CoolRunner-II CPLDs and Extended Spartan-3A Family FPGAs provide means to lock down the JTAG port, preventing configuration and "read back" functions.

Device DNA Design Level Security

Using Device DNA, an electronic serial number that is factory-programmed into every Extended Spartan-3A Family device, designers can implement a very low cost, and yet highly robust security solution to deter reverse-engineering, cloning and overbuilding. Device DNA Design Level Security can be used for protecting both hardware and software IP, and customers have complete flexibility in designing a security algorithm based on their unique application requirements. This technology also enables "try before you buy" and other royalty-based licensing models for IP vendors.



TAKE THE NEXT STEP

To learn more about how Xilinx Security solutions can protect your business, we invite you to visit us on the Web at *www.xilinx.com/security*

Corporate Headquarters

Xilinx, Inc.
2100 Logic Drive
San Jose, CA 95124
Tel: 408-559-7778
Fax: 408-559-7114
Web: www.xilinx.com

Europe Headquarters

Xilinx Ireland
One Logic Drive
Citywest Business Campus
Saggart, County Dublin
Ireland
Tel: +353-1-464-0311
Fax: +353-1-464-0324
Web: www.xilinx.com

Japan

Xilinx K K
Art Village Osaki Central Tower 4F
1-2-2 Osaki, Shinagawa-Ku
Tokyo 141-0032 Japan
Phone: +81-36744-7777
Fax: +81-3-5436-0532
Web: japan.xilinx.com

Asia Pacific Pte. Ltd.

Xilinx, Asia Pacific
5 Changi Business Park
Singapore 486040
Tel: +65-6407-3000
Web: www.xilinx.com

XILINX
www.xilinx.com

Printed in U.S.A.   PN 2034-1