Protecting Intellectual Property Through FPGA Design Security

With heightened competition and distribution into global markets, designers increasingly need to safeguard their innovations. Your valuable intellectual property (IP)—your "secret sauce"—needs protection so you can differentiate your product to stand out in the crowd and make you a leader in your market. SRAM-based FPGAs offer design security, plus a unique combination of performance, programmability, fast time-to-market and flexibility, to create an ideal secure solution for commercial and military applications.

What FPGAs provide design security?

Altera's Stratix® II and Stratix II GX devices are the industry's only high-performance, high-density FPGAs that provide a non-volatile design security solution to protect designs. This design security features offers a unique competitive advantage, allowing you to test-market your innovation and move to production without risking your valuable IP.

How do Stratix II and Stratix II GX FPGAs ensure design security?

SRAM-based FPGAs are volatile and require a configuration bitstream to be sent from an external memory device to the FPGA at power up. To prevent the configuration bitstream from being intercepted during transmission, Altera® Stratix II and Stratix II GX devices use 128-bit advanced encryption standard (AES)—an industry-standard encryption algorithm—and a non-volatile key for configuration bitstream encryption.

How do I encrypt a configuration bitstream?

Simply load the security key into the FPGA during regular manufacturing flow, then encrypt the configuration file with the same key and store it in the external memory. At system power-up, the external memory sends the encrypted configuration file to the FPGA, which then uses the stored key to decrypt the configuration file in real time and configure itself (see Figure 1).

What are the benefits of non-volatile key storage over volatile key storage?

The non-volatile key storage in Stratix II and Stratix II GX FPGAs retains its information when power is off, offering a number of benefits:

- No need for an external backup battery when power is down. Batteries have limited life and are temperature-sensitive (causing a high maintenance cost), and are not suitable for harsh environments.
- Improves manufacturing flexibility because the security key can be programmed into the Stratix II or Stratix II GX device either on- or off-board.
- Offers tamper protection because the non-volatile key is also one-time programmable.
- Enables ASSP and royalty-based business models. ASSP and royalty-based IP vendors can securely deliver IP by shipping FPGAs with the key pre-programmed and an encrypted configuration file.

How does the design security feature protect my design?

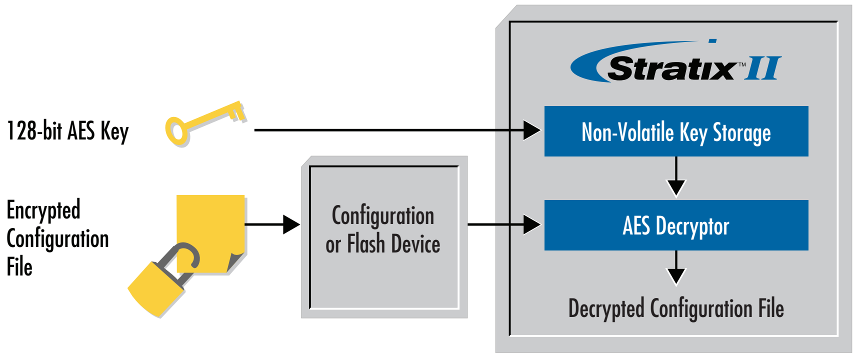
Altera's design security feature protects your IP from tampering, copying and reverse engineering:

- A secure Stratix II or Stratix II GX device can be programmed only if the configuration file is encrypted with the correct key. It cannot be configured if the configuration file is unencrypted or encrypted with the wrong key, preventing tampering.
- Even if your configuration file is captured, it cannot be decrypted, preventing design copying. Read-back of any configuration file, whether encrypted or unencrypted, is not permitted in Stratix II and Stratix II GX devices, adding another layer of security.
- Reverse engineering any high-density FPGA design through the configuration file is very difficult and time-consuming, even without encryption, as the configuration file contains millions of bits. In addition, Altera's configuration file formats are proprietary and confidential. With configuration bitstream encryption, it may be easier and quicker to build a competitive design from scratch than to use reverse engineering.

How does design security give me a competitive advantage?

Altera's design security feature allows you to deliver your products to customers safely and quickly, providing a risk-free path for testing your innovations with customers, differentiating your product from the competition, and bringing it to market.

Figure 1. Encrypting a Configuration Bitstream


128-bit AES Key
Encrypted Configuration File
Configuration or Flash Device
Stratix II
Non-Volatile Key Storage
AES Decryptor
Decrypted Configuration File