Introduction

This chapter provides an overview of the design security feature and its implementation on Stratix® III devices using advanced encryption standard (AES) as well as security modes available in Stratix III devices.

As Stratix III devices start to play a role in larger and more critical designs in competitive commercial and military environments, it is increasingly important to protect the designs from copying, reverse engineering, and tampering. Stratix III devices address these concerns and are the industry's only high-density, high-performance devices with both volatile and non-volatile security feature support. Stratix III devices have the ability to decrypt configuration bitstreams using the AES algorithm, an industry standard encryption algorithm that is FIPS-197 certified. They also have a design security feature that utilizes a 256-bit security key.

Altera® Stratix III devices store configuration data in static random access memory (SRAM) configuration cells during device operation. Because SRAM memory is volatile, SRAM cells must be loaded with configuration data each time the device powers-up. It is possible to intercept configuration data when it is being transmitted from the memory source (flash memory or a configuration device) to the device. The intercepted configuration data could then be used to configure another device.

When using the Stratix III design security feature, the security key is stored in the Stratix III device. Depending on the security mode, you can configure the Stratix III device using a configuration file that is encrypted with the same key, or for board testing, configured with a normal configuration file.

The design security feature is available when configuring Stratix III devices using the fast passive parallel (FPP) configuration mode with an external host (such as a MAX® II device or microprocessor), or when using fast active serial (AS) or passive serial (PS) configuration schemes. However, the design security feature is also available in remote update with fast AS configuration mode. The design security feature is not available when you are configuring your Stratix III device using Joint Test Action Group (JTAG)-based configuration. For more information, refer to "Supported Configuration Schemes" on page 14–5.

Stratix III Security Protection

Stratix III device designs are protected from copying, reverse engineering, and tampering using configuration bitstream encryption.

Security Against Copying

The security key is securely stored in the Stratix III device and cannot be read out through any interfaces. In addition, as configuration file read-back is not supported in Stratix III devices, the design information cannot be copied.

Security Against Reverse Engineering

Reverse engineering from an encrypted configuration file is very difficult and time consuming because the Stratix III configuration file formats are proprietary and the file contains million of bits which require specific decryption. Reverse engineering the Stratix III device is just as difficult because the device is manufactured on the most advanced 65-nm process technology.

Security Against Tampering

The non-volatile keys are one-time programmable. Once the tamper protection bit is set in the key programming file generated by the Quartus® II software, the Stratix III device can only be configured with configuration files encrypted with the same key.

For more information about why this feature is secured, refer to the *Design Security in Stratix III Devices white paper.*

AES Decryption Block

The main purpose of the AES decryption block is to decrypt the configuration bitstream prior to entering data decompression or configuration.

Prior to receiving encrypted data, you must enter and store the 256-bit security key in the device. You can choose between a non-volatile security key and a volatile security key with battery backup.

The security key is scrambled prior to storing it in key storage in order to make it more difficult for anyone to retrieve the stored key using de-capsulation of the device.

Flexible Security Key Storage

Stratix III devices support two types of security key programming: volatile and non-volatile. Table 14–1 shows the differences between volatile keys and non-volatile keys.

Table 14–1. Security Keys Options

Options	Volatile Key	Non-Volatile Key
Key programmability	Reprogrammable and erasable	One-time programmable
External battery	Required	Not required
Key programming method *(1)*	On-board	On and off board
Design protection	Secure against copying and reverse engineering	Secure against copying and reverse engineering. Tamper resistant if tamper protection bit is set.

Note to Table 14–1:

(1) Key programming is carried out using JTAG interface.

You can program the non-volatile key to the Stratix III device without an external battery. Also, there are no additional requirements to any of the Stratix III power supply inputs.

V_{CCBAT} is a dedicated power supply for volatile key storage and not shared with other on-chip power supplies, such as V_{CCIO} or V_{CC}. V_{CCBAT} continuously supplies power to the volatile register regardless of the on-chip supply condition.

Table 14–2. Key Retention Time of Coin-Cell Type Batteries used for Volatile Key Storage

Battery	Typical	Worst-case (1)
35mAh	49 years	6 years
1000mAh	1429 years	190 years

Note to Table 14–2:

(1) Worst-case refers to worst-case process and 100°C junction temperature.

☞ After power-up, you need to wait 100 ms (PORSEL = 0) or 12 ms (PORSEL = 1) before beginning the key programming to ensure that V_{CCBAT} is at its full rail.

☞ As an example, here are some lithium coin-cell type batteries used for volatile key storage purposes: BR1220 (-30° to +80°C) and BR2477A (-40°C to +125°C).

✐ For more information about battery specifications, refer to the *DC and Switching Characteristics of Stratix III Devices* chapter in volume 2 of the *Stratix III Device Handbook*.

Stratix III Design Security Solution

Stratix III devices are SRAM-based devices. To provide design security, Stratix III devices require a 256-bit security key for configuration bitstream encryption.

To carry out secure configuration, complete the following steps. Figure 14–1 also describes secure configuration.

1. Program the security key into the Stratix III device.

   Program the user-defined 256-bit AES keys to the Stratix III device through the JTAG interface.

2. Encrypt the configuration file and store it in the external memory.

   Encrypt the configuration file with the same 256-bit keys used to program the Stratix III device. Encryption of the configuration file is done using the Quartus II software. The encrypted configuration file is then loaded into external memory, such as a configuration or flash device.

3. Configure the Stratix III device.

   At system power-up, the external memory device sends the encrypted configuration file to the Stratix III device.

Figure 14–1. Design Security   *(Note 1)*
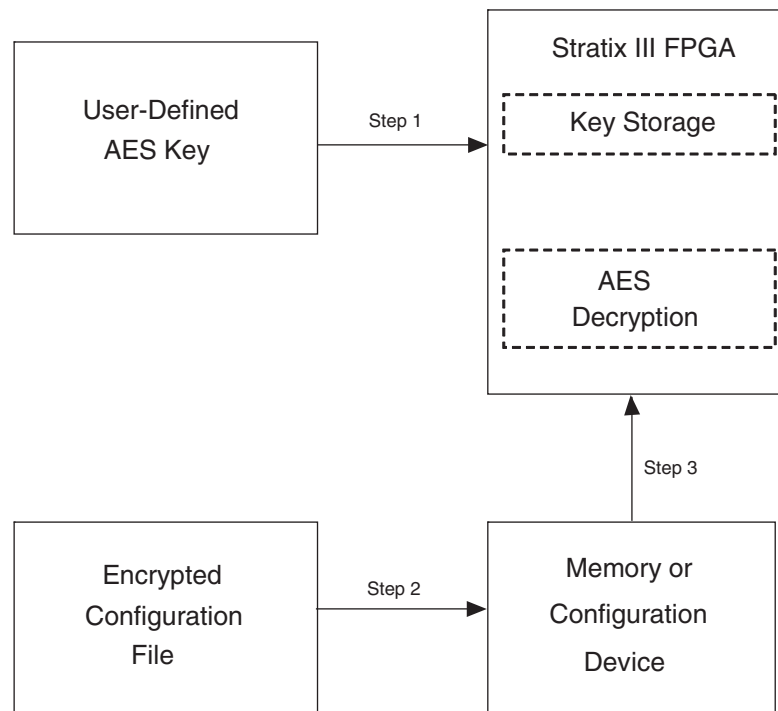
Note to Figure 14–1:

(1)   Step 1, Step 2, and Step 3 correspond to the procedure detailed in the "Stratix III Design Security Solution" section.

Security Modes Available

There are several security modes available on the Stratix III device, which are described as follows:

Volatile Key

Secure operation with volatile key programmed and required external battery—this mode accepts both encrypted and unencrypted configuration bitstreams. Use the unencrypted configuration bitstream support for board-level testing only.

Non-Volatile Key

Secure operation with one time programmable (OTP) security key programmed—this mode accepts both encrypted and unencrypted configuration bitstreams. Use the unencrypted configuration bitstream support for board-level testing only.

Non-Volatile Key with Tamper Protection Bit Set

Secure operation in tamper resistant mode with OTP security key programmed—only encrypted configuration bitstreams are allowed to configure the device. Tamper protection disables JTAG configuration with unencrypted configuration bitstream.

☞ Setting the tamper protection bit disables test mode in Stratix III devices. This process is irreversible and prevents Altera from carrying-out failure analysis if test mode is disabled. Contact Altera Technical Support to set the tamper protection bit.

☞ You can perform Boundary Scan testing or use the SignalTap II logic analyzer to analyze functional data with the tamper-protection bit set programmed into the Stratix III FPGA.

No Key Operation

Only unencrypted configuration bitstreams are allowed to configure the device.

Table 14–3 summarizes the different security modes and the configuration bitstream supported for each mode.

Table 14–3. Security Modes Supported

Mode *(1)*	Function	Configuration File
Volatile key	Secure	Encrypted
	Board-level testing	Unencrypted
Non-volatile key	Secure	Encrypted
	Board-level testing	Unencrypted
Non-volatile key with tamper protection bit set	Secure (tamper resistant) *(2)*	Encrypted

Notes to Table 14–3:

(1) In No key operation, only unencrypted configuration file is supported.

(2) The tamper protection bit setting does not prevent the device from being reconfigured.

Supported Configuration Schemes

The Stratix III device supports only selected configuration schemes, depending on the security mode you select when you encrypt the Stratix III device.

Figure 14–2 shows the restrictions of each security mode when encrypting Stratix III devices.
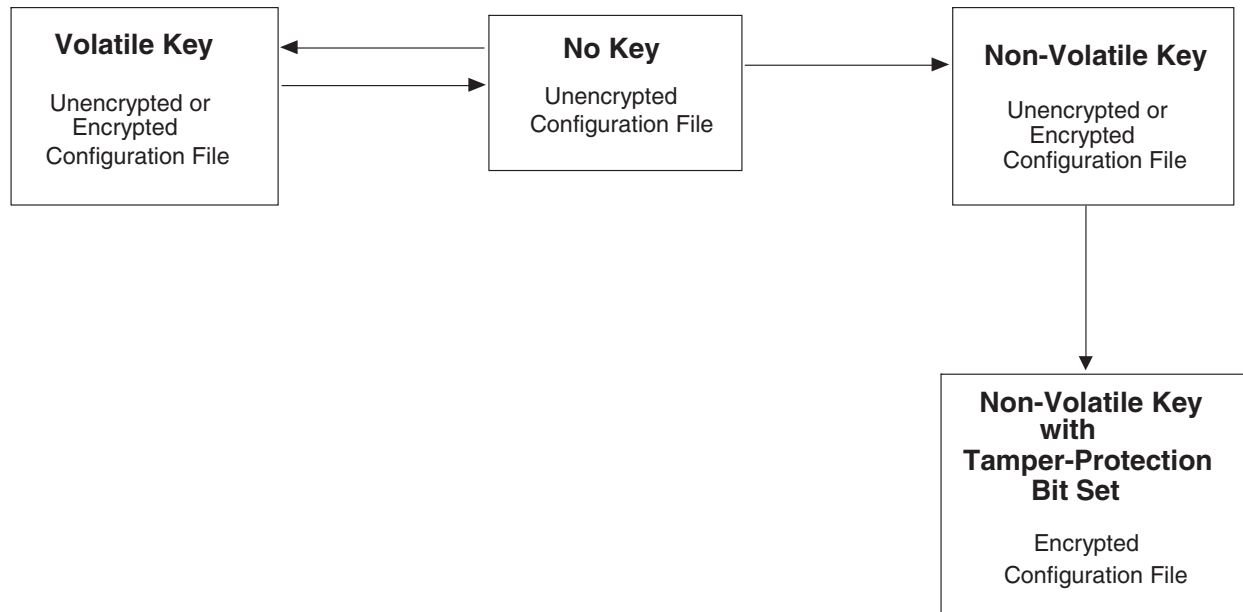
Figure 14–2. Stratix III Security Modes - Sequence and Restrictions

Table 14–4 shows the configuration modes allowed in each of the security modes.

Table 14–4. Allowed Configuration Modes for Various Security Modes *(Note 1)* (Part 1 of 2)

Security Mode	Configuration File	Allowed Configuration Modes
No key	Unencrypted	All configuration modes that do not engage the design security feature.
Secure with volatile key	Encrypted	■ Passive serial with AES (and/or with decompression) ■ Fast passive parallel with AES (and/or with decompression) ■ Remote update fast AS with AES (and/or with decompression) ■ Fast AS (and/or with decompression)
Board-level testing with volatile key	Unencrypted	All configuration modes that do not engage the design security feature.
Secure with non-volatile key	Encrypted	■ Passive serial with AES (and/or with decompression) ■ Fast passive parallel with AES (and/or with decompression) ■ Remote update fast AS with AES (and/or with decompression) ■ Fast AS (and/or with decompression)
Board-level testing with non-volatile key	Unencrypted	All configuration modes that do not engage the design security feature.

Table 14–4. Allowed Configuration Modes for Various Security Modes *(Note 1)* (Part 2 of 2)

Security Mode	Configuration File	Allowed Configuration Modes
Secure in tamper resistant mode using non-volatile key with tamper protection set	Encrypted	■ Passive serial with AES (and/or with decompression) ■ Fast passive parallel with AES (and/or with decompression) ■ Remote update fast AS with AES (and/or with decompression) ■ Fast AS (and/or with decompression)

Note to Table 14–4:

(1) There is no impact to the configuration time required compared to unencrypted configuration modes except fast passive parallel with AES (and/or decompression) which requires DCLK of 4× the data rate.

☞ The design security feature with encrypted configuration file is available in all configuration methods, except JTAG. Therefore, use the design security feature in FPP mode (when using external controller, such as a MAX II device or a microprocessor and a flash memory), or in fast AS and PS configuration schemes.

Table 14–5 summarizes the configuration schemes that support the design security feature both for volatile and non-volatile key programming.

Table 14–5. Design Security Configuration Schemes Availability

Configuration Scheme	Configuration Method	Design Security
FPP	MAX II device or microprocessor and flash memory	✓ *(1)*
Fast AS	Serial configuration device	✓
PS	MAX II device or microprocessor and flash memory	✓
	Download cable	✓
JTAG *(2)*	MAX II device or microprocessor and flash memory	
	Download cable	—

Notes to Table 14–5:

(1) In this mode, the host system must send a DCLK that is 4× the data rate.

(2) JTAG configuration supports only unencrypted configuration file.

Use the design security feature with other configuration features, such as compression and remote system upgrade features. When you use compression with the design security feature, the configuration file is first compressed and then encrypted using the Quartus II software. During configuration, the Stratix III device first decrypts and then decompresses the configuration file.

Conclusion

The need for design security is increasing as devices move from glue logic to implementing critical system functions. Stratix III devices address this concern by providing built-in design security. These devices not only offer high density, fast performance, and cutting-edge features to meet your design needs, but also protect your designs against IP theft and tampering of your configuration files.

Chapter Revision History

Table 14–6 shows the revision history for this document.

Table 14–6. Chapter Revision History

Date and Revision	Changes Made	Summary of Changes
May 2009, version 1.5	Updated "Flexible Security Key Storage" and "Non-Volatile Key with Tamper Protection Bit Set" sections.	—
February 2009, version 1.4	■ Updated "Flexible Security Key Storage" section. ■ Removed "Referenced Documents" section.	—
October 2008, version 1.3	■ Updated "Non-Volatile Key with Tamper Protection Bit Set" section. ■ Added Table 14–2. ■ Updated New Document Format.	—
May 2008 , version 1.2	■ Updated "Introduction" section. ■ Updated "Flexible Security Key Storage" section. ■ Updated Table 14–1 and Table 14–4. ■ Updated "Security Modes Available" section.	—
October 2007, version 1.1	■ Added new section "Referenced Documents". ■ Added live links for references.	Minor update
November 2006, version 1.0	Initial Release.	—