

基于 SRAM 的 FPGA 具有易失性，需要外部存储器来存储其配置文件，这带来了三种安全问题：复制、逆向剖析和篡改。本白皮书详细介绍 Stratix III 设计安全解决方案所提供的安全保护功能。

引言

随着越来越多的系统采用 FPGA 来实现核心功能，保护 FPGA 中的设计和知识产权 (IP) 变得更加重要了。Altera® Stratix® III 是第一款使用高级加密标准 (AES) 的高密度、高性能 FPGA，它采用非易失和易失密钥设置来保护设计不被复制、逆向剖析和篡改。为了使 Stratix III 设计安全解决方案更加安全，保护 AES 密钥，Altera 采用了多种安全特性。在设计阶段，外请安全顾问研究了这一解决方案，Altera 根据他们的反馈进行了改进。本白皮书详细介绍 Stratix III 设计安全解决方案所提供的安全保护功能。

基于 SRAM 的 FPGA 设计安全性

基于 SRAM 的 FPGA 是易失器件，需要外部存储器来存储其配置文件，这带来了三种安全问题：复制、逆向剖析和篡改。

复制

复制 FPGA 是获得设计的相同副本，不需要理解它是怎样工作的。可以通过从存储器件中读取设计，或者上电时，在存储器将配置文件发送到 FPGA 的过程中捕获配置文件来复制器件。被盗取的设计可以用于配置其他 FPGA。这种方法是 IP 盗窃的基本形式，会大大损害设计人员的利益。

逆向剖析

逆向剖析分析配置文件，在寄存器传送级 (RTL) 或者以原理图的形式重新得到最初设计。对得到的设计进行修改后就可以赢得竞争优势。这类 IP 盗窃要比复制更复杂，通常需要一定的专业技术，而且很耗时，占用大量的资源，有时候要比从头开始进行设计更费事。

篡改

篡改是对存储在器件中的设计进行修改或者以不同的设计进行替换。篡改后的器件会含有恶意设计代码，能够导致系统出现故障，或者窃取敏感数据。这类设计安全问题是军事、金融和游戏等领域特别关心的。目前的消费类市场也存在篡改问题，对设计进行修改后便可以使用未授权的服务或者高级服务。

Stratix III 设计安全解决方案

Stratix III 器件是基于 SRAM 的 FPGA。为实现设计安全性，Stratix III FPGA 使用一个 256 位安全密钥，对配置比特流进行加密。可以在 Quartus II 软件中综合、适配和时序分析后，进行这些安全配置。

按照以下三步来实现安全配置：

1. *将安全密钥设置到 Stratix III FPGA 中：* Quartus® II 软件需要用户输入 256 位用户定义的密钥，用于产生密钥设置文件。通过 JTAG 接口将含有密钥信息的密钥设置文件装入到 Stratix III FPGA 中。然后，将密钥存储到 256 位密钥存储器中，这些存储器可以是易失 (基于 SRAM) 或者非易失 (基于多状态熔丝) 器件。
2. *对配置文件进行加密，将其存储在外部存储器中：* Quartus II 软件需要步骤 1 中使用的同一 256 位用户定义的密钥来加密配置文件。然后，将加密后的配置文件装入到外部存储器中，例如配置或者闪存器件。

3. **配置 Stratix III FPGA:** 在系统上电时, 外部存储器向 Stratix III FPGA 发送加密配置文件。Stratix III 内置 AES 解密引擎使用密钥来解密配置文件, 对自己进行配置。

Stratix III 密钥设置解决方案

Altera 通过 JTAG 接口提供不同类型的设计安全密钥配置方案, 支持板上和板外密钥设置。

 **AN 512: 使用 Stratix III 器件的设计安全功能**介绍了设置易失和非易失密钥的步骤。

AES 加密算法

AES 是联邦信息处理标准 (FIPS-197), 经过认证, 美国政府组织利用这一技术保护敏感的、列入密级的信息。全球范围内商业系统也广泛采用了该标准。

AES 是一种对称分组密码, 以 128 位为一组进行数据加密解密。加密后的数据进行了一系列变换, 包括字节替换、数据混合、数据移位和置入密钥等。AES 有长度不同的三种密钥: 128 位、192 位和 256 位。

Stratix III FPGA 采用了 256 位 AES 密钥, 同时保证安全性和效率。据国家标准和技术研究所 (NIST) 的研究, 如果有人能够发明在几秒内解密数据加密标准 (DES) 密钥的机器, 那么这一机器需要花费 149 万亿年来解密一个 256 位 AES 密钥。Stratix III AES 实施方案经认证, 符合 FIPS-197 标准。

AES 解密模块

解密模块的主要功能是:

- 确定配置数据是否需要解密
- 确定安全模式
- 如果需要, 解密数据流, 解压缩数据, 否则, 对器件进行配置。

在接收到加密数据之前, 256 位安全密钥必须装入并存储在器件中。您可以选择使用非易失安全密钥或者带电池供电的易失安全密钥。非易失密钥和多状态熔丝密钥验证位 (用于指明有多状态熔丝密钥) 被存储在一次编程多状态熔丝中, 而 256 位易失密钥和易失密钥验证位 (用于指明有易失密钥) 存储在易失密钥寄存器中, 采用外部电池对其进行供电。

密钥存储

安全密钥被存储在 Stratix III FPGA 中的易失密钥寄存器和多状态熔丝中。多状态熔丝为非易失, 一次可编程。需要外部后备电池来存储易失密钥, 在器件关机时对其进行供电。在普通生产流程中, FPGA 在板上 (易失和非易失密钥) 或者不在板上 (仅非易失密钥) 时, 都可以将安全密钥设置到 Stratix III FPGA 中。

Stratix III FPGA 提供的安全保护

采用配置比特流加密, 可以保护 Stratix III FPGA 设计不被复制、逆向剖析和篡改。

防止被复制的安全特性

通过任何接口都不能读出 Stratix III FPGA 中的安全密钥。存储了安全密钥的多状态熔丝和易失密钥寄存器隐藏在数百个其他多状态熔丝金属层下面。简单的视觉检查很难确定某一熔丝或者寄存器的功能。对密钥位进行了加扰, 分布在 FPGA 的其他逻辑中间。此外, 其他功能的密钥存储设置状态随器件各不相同。随机性使得更难发现哪一熔丝或者寄存器存储了安全密钥。

Stratix III FPGA 不支持配置文件读回, 防止了在 FPGA 中解密配置文件后的读回攻击。

防止被逆向剖析的安全特性

即使不加密，从配置文件中对任何 Stratix III 设计进行逆向剖析都非常困难，而且很耗时。Stratix III 配置文件含有数百万个比特，配置文件格式是专有的，没有公开。要对 Stratix III 设计进行逆向剖析，首先要对 FPGA 进行逆向剖析，或者使用 Quartus II 设计软件来揭示从配置文件到器件资源的映射。

对 Stratix III FPGA 本身进行逆向剖析也非常困难。Stratix III FPGA 采用最先进的 65nm 工艺技术在 TSMC 进行制造。与 ASIC 不同，仅有标准工具和知识还不能逆向剖析这些前沿的 FPGA。逆向剖析 Stratix III FPGA 中的一个逻辑模块、找到 FPGA 中的密钥位置就需要花费大量的时间和资源。


对比特流加密后，更难进行逆向剖析。找到安全密钥来解密配置文件和对其进行复制一样困难。从头开始一个竞争设计，可能要比逆向剖析一个安全 Stratix III 设计容易得多。

防止被篡改的安全特性

非易失密钥为一次可编程。一旦设置了篡改保护位，FPGA 只能接收采用相同密钥加密的配置文件。而且，不允许进一步设置密钥。试图采用未加密配置文件或者以错误密钥加密的配置文件来配置 Stratix III FPGA 都会导致配置失败。不论是在外部存储器中，在外部存储器和 FPGA 之间进行传送或者远程连接系统更新期间，出现配置失败都表明有可能出现了设计篡改。

所支持的配置方案

当外部主机（例如，MAX[®] II 或者微处理器）采用快速被动并行（FPP）配置模式，或者使用主动串行（AS）和被动串行（PS）配置方案来配置 Stratix III FPGA 时，都可以应用设计安全特性。如果您使用增强配置器件 FPP 或者基于 JTAG 的配置来配置您的 Stratix III FPGA，则不支持设计安全特性。根据加密 Stratix III 器件时所选择的安全模式，器件将只支持所选择的配置方案。

 关于 Stratix III 器件所支持的安全模式以及每一安全模式相应配置方案的详细信息，请参考 *Stratix III 器件手册* 的 *Stratix III 器件设计安全性* 一章。

结论

Stratix III FPGA 利用多种安全特性，提供可靠的设计安全解决方案来保护设计人员的知识产权，防止被篡改，使这类器件非常适合保密通信和一般军事应用。设计人员利用这些安全特性，能够迅速安全地向客户交付采用 Altera 设计和验证工具设计的产品，无风险向客户推出创新产品，在竞争中突出自己的产品优势。

详细信息

- AN 512: 使用 Stratix III 器件的设计安全功能:
www.altera.com/literature/an/an512.pdf
- Stratix III 器件手册的 Stratix III 器件设计安全性一章:
www.altera.com/literature/hb/stx3/stx3_siii51014.pdf
- 联邦信息处理标准 (FIPS-197):
<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- 高级加密标准算法批准清单:
<http://csrc.nist.gov/cryptval/aes/aesval.html>



101 Innovation Drive
San Jose, CA 95134
(408) 544-7000
<http://www.altera.com>

版权 © 2009 Altera 公司。保留所有版权。Altera，可编程解决方案公司、程式化 Altera 标识、专用器件名称和所有其他专有商标或者服务标记，除非特别声明，均为 Altera 公司在美国和其他国家的商标和服务标记。所有其他产品或者服务名称的所有权属于其各自持有人。Altera 产品受美国和其他国家多种专利、未决应用、掩模著作权和版权的保护。Altera 保证当前规范下的半导体产品性能与 Altera 标准质保一致，但是保留对产品和服务在没有事先通知时的变更权利。除非与 Altera 公司的书面条款完全一致，否则 Altera 不承担由使用或者应用此处所述信息、产品或者服务导致的责任。Altera 建议客户在决定购买产品或者服务，以及确信任何公开信息之前，阅读 Altera 最新版的器件规范说明。