

保护 FPGA 设计不受常见的入侵威胁

随着盗版和 IP 剽窃的增多，人们越来越关心设计和 IP 安全。对于 FPGA，这需要保护比特流和器件的配置。Cyclone III LS FPGA 在低功耗平台上实现了安全特性，帮助设计人员满足了约束要求，确信发售 IP 得到了保护的产品。

引言

2009 年，全球由于盗版带来的损失大约为 1.5 万亿美元。盗版影响了所有商业市场，从 Gucci 手包到计算机芯片，直至专用算法等。全球供应链越来越复杂，对企业知识产权 (IP) 的剽窃也日益增多。全球供应链的安全和保护问题是保持竞争优势的关键，需要认真对待。

盗版的第一步是篡改，采用各种强制手段来获得系统设计。以前，篡改是针对军用设备的；然而，由于电子行业的盗版，篡改成为所有生产商都必须面对的关键问题。防篡改的目的是探测到对技术的逆向剖析，通过剖析可以转移技术，改变系统功能，开发对策等。

政府和企业投入了大量的资金来开发关键网络基础设施、复杂的武器系统以及安全银行系统等。然而，很容易破坏易于篡改的系统，导致丧失竞争优势，利润下滑，品牌知名度下降。盗版丰厚的利润带来了电子产品的觊觎。因此，产品日益重要含有防篡改功能。

防篡改解决方案主要涉及到以下四个方面：

- 阻止篡改是指具有特殊功能，能够阻止篡改入侵。
- 篡改探测能够提醒系统或者用户出现篡改事件。
- 篡改响应是在探测到篡改后，系统必须采取一定的对策。
- 篡改证据必须是可查的，这样，监察系统的授权人员能够确定系统是否被篡改。

表 1 总结了防篡改的主要组成功能，简要介绍了 Altera® 解决方案。

表 1. 防篡改组成功能和 Altera 解决方案

防篡改组成	说明	Altera Cyclone III LS 解决方案
篡改阻止	特殊功能	加密密钥 JTAG 端口保护
篡改探测	觉察	可编程失败 循环冗余校验 (CRC)
篡改响应	对策	所有配置存储器归零
篡改证据	明显的证据	多次未成功编程

对 ASIC 的威胁

ASIC 市场通常采取一定的措施以应对篡改的威胁，例如，破坏性分析、过压或者欠压分析以及时序分析等。使用破坏性分析方法对 ASIC 逆向剖析时，采集器件的每一层来确定其功能。这一处理过程需要昂贵的设备和专业知识，ASIC 实际上有很少的保护措施来防止这类行为。时序分析和过压欠压分析不需要昂贵的设备，但是非常费力，容易出错，因此，不常用于对复杂的 ASIC 设计进行逆向剖析。而且，ASIC 时序分析是确定性的，因此，信号通过复用器的时间决定了输入到输出的时间。

一旦逆向剖析成功，ASIC 中的 IP 就能够不受限制的用在很多盗版系统中。倒卖设备会有很高的利润，全球盗版电子设备，特别是盗版网络设备越来越多。盗版是生产产品相对便宜的方法，利润很高。这些因素

吸引了很多人对电子设备进行 IP 盗取。然而，对于原始设备生产商 (OEM)，盗版系统却使得自身收益下降，利润降低，威胁到品牌形象。

对 FPGA 的威胁

FPGA 具有可编程和不会过时等优点，在工业市场上得到了越来越广泛的应用。军用市场采用比较特殊的商用 (COTS) 产品，使得 FPGA 成为同时实现 COTS 和定制产品的最好选择。网上银行系统需要多层安全防护措施，从闭锁门户到服务器锁定等，因此，银行要求底层有安全措施，使系统从根本上具备安全特性。所有市场关心的是盗取和黑市 / 盗版产品的泛滥。虽然 FPGA 不像 ASIC 那样容易被逆向剖析，但是，却易于遭受其他威胁。

FPGA 可编程体系结构是对设计逆向剖析、直接进行篡改的内在保护屏障。由于其易失特性，拆解和剖析管芯只能得到空白的 FPGA 体系结构。然而，一类不同的篡改活动会影响 FPGA，例如在配置过程中复制和克隆比特流，通过 JTAG 来控制设计，启动单事件干扰 (SEU) 来改变设计功能等。

配置威胁

可编程能力给设计人员带来了好处，但是由于需要采用外部器件进行配置，因此，这也带来了问题。整个设计必须存储在 FPGA 外部系统存储器中，上电时，从存储器传送至 FPGA。关心 IP 保护的设计人员可以将用于配置的走线嵌到 PCB 层中，但是在复杂 PCB 设计中，这产生了其他问题。因此，很少有解决方案能够保护 FPGA 设计在配置过程中不被复制。

加密解决方案

Altera 的 Cyclone[®] III LS FPGA 使用易失密钥，提供 256 位 AES 加密引擎，在配置期间保护比特流。因此，即使检测到比特流，也需要密钥才能逆向剖析设计。Cyclone III LS FPGA 中特殊的密钥方法不允许读回密钥，因此，编程完成后，密钥可以安全的存放在 FPGA 中。由于密钥是易失的，任何破坏性分析都会导致密钥的永久丢失。此外，Altera 还采取了多种措施来保护加密密钥的完整性。

- 密钥存储在金属层下面，以防止物理攻击。
- 在将密钥存放到 FPGA 存储器之前，对其进行加扰处理。
- 密钥比特分布在其他逻辑之间。
- 如果探测到篡改事件，可以通过 JTAG 将密钥擦除。

要对具有设计安全性的 FPGA 设计进行逆向剖析，首先需要获得密钥，对配置文件解密。但是，密钥安全的存放在 FPGA 中，很难获得密钥。采用易失密钥，在探测到篡改时，用户可以清除密钥。即使通过别的手段获得了密钥，解密了配置文件，还是需要将配置文件映射到器件资源级，明确怎样使用逻辑单元 (LE)、互联、存储器模块和 I/O。Altera 使用加密配置比特流格式，因此，很难理解配置文件信息。

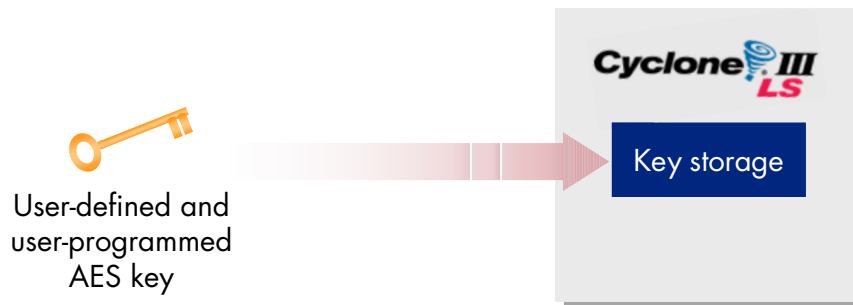
而且，包括 Cyclone III LS 器件在内的所有 Altera FPGA 都不允许以任何方式读回 FPGA 配置。因此，一旦将设计装入到 FPGA 中后，不可能再将数据输出。配置加密与不采用读回电路两种措施相结合，限制了对设计的直接复制，生产商可以充满信心的采用 Altera FPGA 进行设计，保证 IP 的安全。

实现设计安全的过程

Altera 建立设计安全的过程涉及到三个步骤。

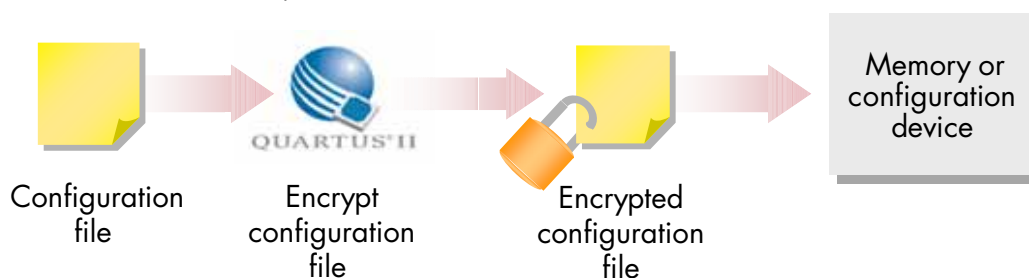
1. 用户必须先选择 256 位密钥，通过 Cyclone III LS JTAG 接口，将其设置到 FPGA 中 (图 1)。注意，由用户选择密钥并进行设置，Altera 并不参与这一过程。

图 1. 第 1 步——采用 256 位密钥设置 Cyclone III LS FPGA



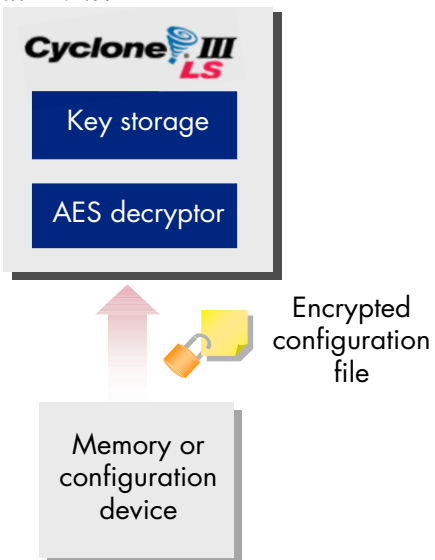
2. 下一步是处理配置比特流文件（也称为编程目标文件，即 .pof），通过 Altera Quartus® II 设计软件，采用与第 1 步中相同的密钥进行加密（图 2）。Quartus II 软件产生加密 .pof，用户将其存储在配置闪存（可以是 EPC 和 EPCS 器件，或者业界标准闪存）中。

图 2. 第 2 步——加密配置文件，存储到存储器中。



3. 最后，在配置过程中，加密 .pof 被下载到 Cyclone III LS FPGA（图 3）中。FPGA 中的 AES 解码器使用存储的密钥对 .pof 进行解密，配置 FPGA。即使竞争对手能够从闪存中复制加密后的 .pof，或者在文件传送到 FPGA 过程中获得该文件，由于不知道 AES 密钥，也无法使用 .pof 来设置另一 Cyclone III LS FPGA。

图 3. 第 3 步——接收并解密加密配置文件



JTAG 威胁

另一类威胁利用了 JTAG 端口。端口虽然是用于链接电路板，实现基本系统功能测试，但是可以不正当的使用灵活的 JTAG 来确定 FPGA 的配置。在大部分 FPGA 中，使能了 JTAG，使用专用引脚，使其优先级高于任何其他配置机制，它可以用于分析设计，有组织的对功能进行逆向剖析，从而盗取设计。然而，与 FPGA 时序分析相似，这虽然不需要专门的设备，但费力、耗时，是非常机械的过程。

JTAG 端口保护解决方案

认识到 JTAG 的弱点，Cyclone III LS FPGA 采取了额外的措施来限制对 JTAG 端口的访问。传统上，FPGA 总是使能 JTAG 端口，可以立即执行 JTAG I/O 引脚上接收到的任何指令。在 Cyclone III LS FPGA 中，将 JTAG 的自然状态限制为只能执行符合 IEEE 规范要求的指令。可以复位 JTAG 端口来接收所有指令集。但是，在允许完全访问 JTAG 引脚之前，复位 JTAG 端口会导致 Cyclone III LS FPGA 自动擦除自己的所有配置（包括易失 AES 密钥）。因此，用户不能以任何方式使用 JTAG 端口来测试或者修改设计。

不受未来威胁的影响

Cyclone III LS FPGA 的安全特性已经超越了当今市场对配置期间保护比特流的要求，以及保护设计不受 JTAG 端口威胁的要求。除了这些特性，Cyclone III LS FPGA 还提供篡改探测功能，使用循环冗余校验 (CRC) 电路发现对设计进行有意或者无意的位操作。CRC 电路不断检查 FPGA 配置，判断是否出现由于大气中子导致软错误（或者 SEU）引起一个或者多个比特变化。在出现错误时，系统立即提醒进行校正。对系统行为进行控制，支持错误记录或者缓慢关断等各种操作。CRC 特性增加了另一层防篡改保护措施，如果 FPGA 在最后一次配置之后，存储器内容出现了变化，该特性会提醒用户。

Cyclone III LS FPGA 超越了阻止篡改的特殊要求，还提供主动篡改响应功能。最安全的响应方法是清除系统中的所有敏感数据，防止数据被损坏。归零处理涉及到对所有数据的清除和验证，大部分应用适合采用归零处理，清除 FPGA 的所有存储器单元。Cyclone III LS 归零解决方案不仅具有清除和验证功能，而且大大提高了用户在设计上的灵活性。默认情况下，清除功能清除含有设计的配置 RAM 和含有特殊设计数据的嵌入式 RAM。此外，可以独立于器件的其他部分单独清除 AES 密钥。

这种归零功能使设计人员能够在探测到篡改事件时，启动校正措施。任何设计输入都可以启动归零操作，用户能够非常灵活的控制系统的篡改响应，完成归零操作之前，很难禁用该功能。为完成归零操作，验证过程重新装入设计，开始重新配置，随后进行 CRC 处理，确保成功的进行重新配置。可以设置设计，完成很多功能，包括标记篡改证据，继续对外部系统组件进行归零操作等。

而且，Cyclone III LS FPGA 通过内部振荡器提供不中断时钟源。如果系统时钟或者 FPGA 输入时钟受到控制，这可以保证系统仍能完成健康检查，通过 CRC 监视 FPGA 配置，如果意外事件损害到设计安全，开始进行校正。提供内部时钟源使设计人员可以在现场完全控制系统，确保出现威胁事件时，设计能够得到保护。

结论

随着盗版和 IP 剽窃的增多，人们越来越关心设计和 IP 安全。对于 FPGA，这需要保护比特流和器件的配置。安全带来了体积、功耗以及产品及时面市等经济性问题。而 Cyclone III LS FPGA 很好的解决了这些问题。Cyclone III LS FPGA 在低功耗平台上实现了安全特性，提供全面的防篡改解决方案，帮助设计人员满足约束要求，确信发售 IP 得到了保护的产品。

详细信息

- Cyclone III FPGA——安全：
www.altera.com/products/devices/cyclone3/overview/security/cy3-security.html
- 资料：Cyclone III 器件：
www.altera.com/products/devices/cyclone3/literature/cy3-literature.jsp
- 在高可靠性和信息安全保障系统中实现设计分离：
www.altera.com/literature/wp/wp-01110-design-separation.pdf
- Quartus II 订购版软件：
www.altera.com/products/software/quartus-ii/subscription-edition/qts-se-index.html

致谢

- Juwayriyah Hussain，产品营销高级工程师，低成本产品，Altera 公司。
- Paul Quintana，高级技术经理，军事业务部，Altera 公司。



101 Innovation Drive
San Jose, CA 95134
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、模板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升级变更权利。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。