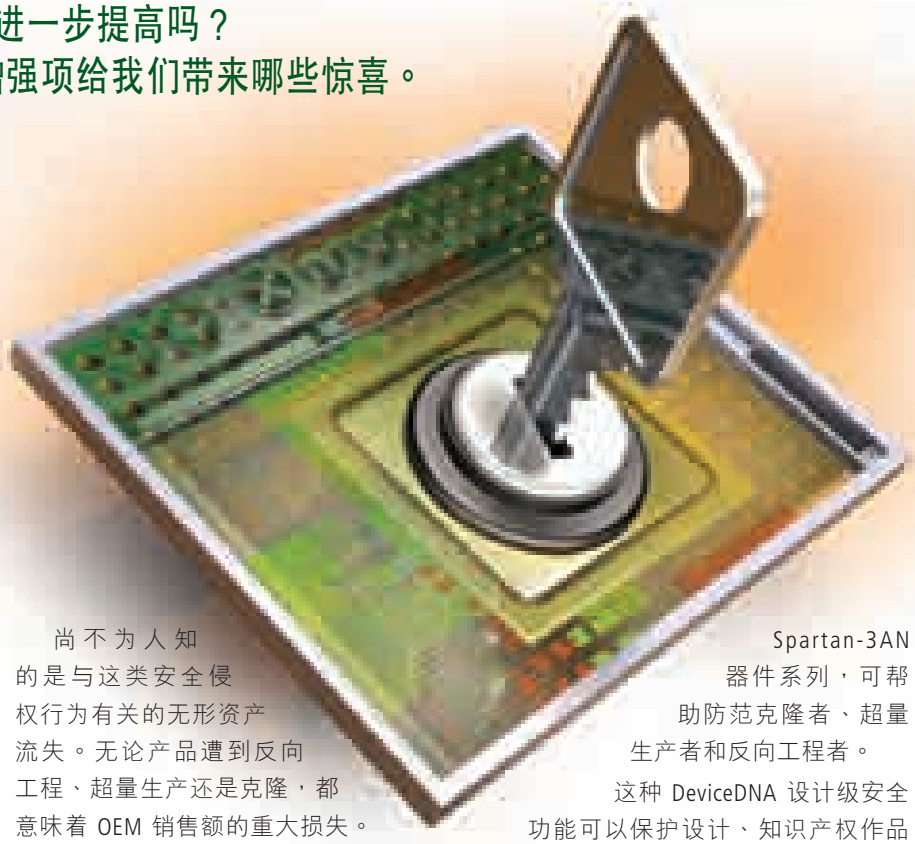
用Spartan-3A和Spartan-3AN平台实现低成本安全解决方案

低成本 FPGA 设计的安全性能进一步提高吗？请看 Xilinx 的 Spartan-3 最新增强项给我们带来哪些惊喜。

作者：Maureen Smerdon
Xilinx 公司
战略营销经理
maureen.smerdon@xilinx.com



安全已成为当今的热门话题：无论是乘坐飞机、关好前门还是开始下一代电路设计，安全都是一个重大问题。对于设计人员来说，最大的威胁莫过于市场上由设计盗版带来的数量惊人的假冒产品。根据反假冒联盟（Anti-Counterfeiting Coalition）估计，2003 年，美国全国涉及假冒的交易达 2870 亿美元，占全世界假冒产品年销售总量（4560 亿美元）的 63%。

本文描述能保护低成本 FPGA 设计的 Xilinx® 安全措施。

三大安全威胁

电子设计中最常见的安全侵权行为就是反向工程。当盗版者以在公开市场低价销售为目的企图重新设计或制作某产品时，就会发生这种行为。通过反向工程，盗版者能够非常迅速地完成设计，不必花费研发经费，成本很可能更低。

今天，许多公司采取外包生产方式，因而面临著两种新侵权行为的威胁，即超量生产和克隆。在超量生产中，承包制造商只需生产出多于 OEM（原始设备制造商）订货量的产品就行了。这些超量产品在未经 OEM 授权的情况下售出。

克隆是指盗版者以相同（或不同）品牌复制设计、知识产权作品或产品。同样，克隆者不必花费任何研发成本。超量生产和克隆的产品都大大缩短了上市时间。

尚不为人知的是与这类安全侵权行为有关的无形资产流失。无论产品遭到反向工程、超量生产还是克隆，都意味着 OEM 销售额的重大损失。除了损失销售额，还会发生以退货量形式表现的质量成本。这可能影响品牌形象，并且，由于 RMA（退货授权书）数量增多，或者由于为确定症结所在以及如何解决最终客户的问题提供技术支持，OEM 的财政负担也加重了。最终，产品可能变得真伪难辨。这些是无法补偿的永久性损失。

使用 Device DNA 实现安全功能

在传统上，FPGA 使用某种比特流加密技术来防范反向工程和克隆。在以往的版本中，这样做效果不错。然而在当今时代，比特流加密已无法保护您免遭超量生产侵权。

作为设计人员，如何才能保护您的设计免遭以上三种安全盗版行为呢？Xilinx 提供几种解决方案，并在最近推出了带有 DeviceDNA 的 Spartan™-3A 和 Spartan-3AN 器件系列，可帮助防范克隆者、超量生产者和反向工程者。

这种 DeviceDNA 设计级安全功能可以保护设计、知识产权作品和嵌入式代码。DeviceDNA 是一种特殊的 57 位 ID，对于每个器件都是独一无二的。这种 57 位 ID 置于 FPGA 的某个部位，是在 Xilinx 工厂中固化或设定的，因而不能更改。Spartan-3A 和 Spartan-3AN 两种 FPGA 在每个出厂的器件中都包含独一无二的 ID。

然后，这个 ID 与设计人员的个性化算法结合起来储存在 FPGA 上。该算法基本上是一个算术方程式，它规定如何提取 DeviceDNA 并创建一个结果。然后，该结果可以存储在任何地方，例如外部存储器或 Flash 中。该算法是安全性的秘密所在，因为只有设计人员才知道它。尽管它存储在 FPGA 上，但在旁观者看来，这只是一部分比特流。

Spartan-3A 的安全性

对于 Spartan-3A 器件，该算法将使用

DeviceDNA 的结果与器件配置后存储在 Flash 中的结果相比较。如果二者匹配，则认可该设计。如果二者不匹配，该设计会被设置成多种行为方式，从轻微故障到严重功能障碍。

我们举一个日常生活中的认证例子。比方说，您到本地一家快餐厅吃快餐。现金花光了，不得不使用 ATM 卡 (DeviceDNA)，而只有您才有权使用该卡。您订餐，然后刷卡。这时，机器要求您输入 PIN 号码（个性化算法）。然后，系统会将您输入的 PIN 号码与银行存储的号码进行比较。如果相符，您将得到快餐。如果不符，您可要挨饿了。

其潜在弱点是，可能出现某人同时得到您的 ATM 卡和 PIN 号码的情况。这种 PIN 授权算法密码，一旦为人知晓便很容易被克隆。这正是设计本身集成授权算法的原因。该算法置于可编程逻辑内部最隐秘的位置，可以选择数百万种配置方案。

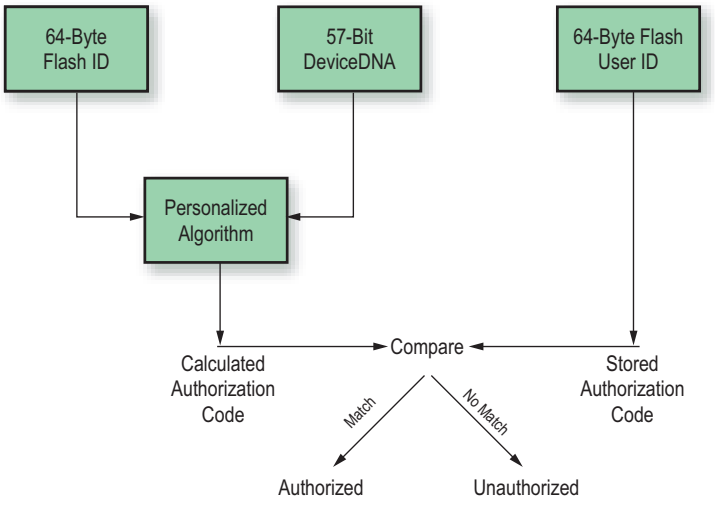


图 1 – 可用 Spartan-3AN FAGA 实现的安全设置

Spartan-3AN 的安全性

对于 Spartan-3AN 平台（即新型非易失性 FPGA 平台），此过程大同小异，只是有几个增强项。第一个安全增强项是，比特流隐藏在 FPGA 内部。这样更难于被人窥见。

Spartan-3AN FPGA 的第二个安全增强项是两个特有的序列号，即 DeviceDNA 和工厂预设 Flash ID，存储在 Flash 中。这两个特有的 ID 提供长达 70 多个字节的序列号，可产生大量可能的算法，从而延长了破解认证算法所需的时间。于是，设计既要受 FPGA 约束，又要受 Flash ID 的约束。

延用前述类比，拥有两个特有的 ID 就像需要用两张不同的 ATM 卡买快餐。

第三项改进是在存储的授权代码中。在 Spartan-3AN 平台上，可以将授权代码存储在片上一个叫做 Flash 用户字段的专用一次性可编程 64 位寄存器中。这样可使整个安全系统自成一体。由于不需要外部接口或存储器，整体安全性得以提高，使反向工程更加困难。

该认证算法由用户定义，这使您能在设计预算内实现恰当的安全等级。该认证算法也是安全系统中的主要秘密。认证过程中必须有不为人知的秘密，才能保护安全系统不被破解。因为算法是未知的，所以它是设计级安全性的关键。算法是在 FPGA 架构中实现的，因此便成为 FPGA 中数百万配置位当中的区区几个。除非您知道这些位如何组合在一起，或者知道是哪种算法，否则这看起来仅仅是一堆数字。图 1 所示为应用 Spartan-3AN 器件的一种可能的流程。

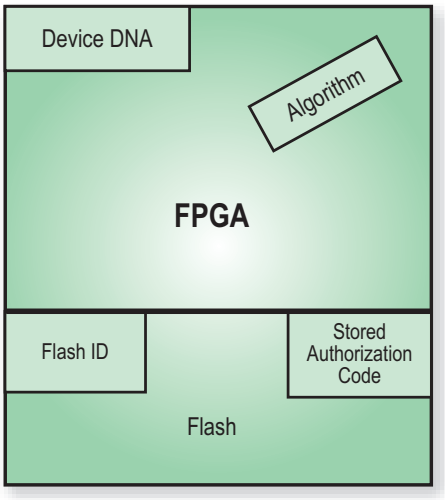


图 2 - 安全的 Spartan-3AN 器件

图 2 所示 Spartan-3AN 设计级安全功能是完全自成一体的安全解决方案。Flash 中既包含 FPGA 配置比特流，也包含预生成的授权代码。此代码由可信/安全制造商或注册流程存储在一次性可编程 Flash 用户字段中。

通电后，FPGA 进行正常配置。一旦配置完成，FPGA 应用程序便包括了批准已授权设计在相关 Spartan-3AN FPGA 上运行的电路。认证算法将读取 DeviceDNA 和工厂预设 Flash ID，然后生成一个主动授权代码，并将此授权代码与 Flash 用户字段中存储的预生成授权代码进行对较。如果两代码相等，则器件通过认证。否则，器件属非法而无法获得授权。

拒绝访问

失败认证的处理是 DeviceDNA 设计级方案的又一强项。认证可以完全集成到设计中。这样，未经授权的设计可以引起多种反应，例如：

- 无功能 – 该设计完全停止工作。
- 有限功能 – 主电路或关键电路被禁用或旁路。
- 定时炸弹 – 仅在限期内提供全部功能。
- 主动防御 – 系统监测各项活动并抵御攻击。
- 永久性自毁 – 删除所有 Flash 内容，并且将 Flash 永远锁定在全零状态。

本文所述设计级安全功能是 Spartan-3A 和 Spartan-3AN 平台中可实现的基本安全级别。

结 论

Spartan-3A 和 Spartan-3AN 平台中的安全措施为防范反向工程、超量生产和克隆提供了多种方法。欲了解有关如何确保低成本 FPGA 设计安全的详情，请参阅《Spartan 系列配置用户指南》，网址是：

www.xilinx.com/cn/bvdocs/userguides/ug333.pdf。