WP266 (v1.0) 2007 年 7 月 24 日

利用 Spartan–3 系列 FPGA 实现安全解决方案

作者： *Maureen Smerdon*

在当今世界，安全是全球社会密切关注的问题。不论您是登机、关门，还是开始下一代电路设计，安全都是一个非常重要的问题。在家里，我们小心防范，以免家里的东西被盗。在电子行业，安全也在迅速成为不可忽视的关键要素。了解安全为什么会一跃而成电子设计领域密切关注的问题非常重要。其原因之一是由窃取设计导致的假冒产品的数量越来越庞大。国际反盗版联盟表示，这些假冒产品威胁经济的发展并且给全球的消费类市场带来了重大影响。本白皮书将确定设计所面临的主要安全威胁，探讨基本安全级别，并且介绍 Xilinx 的新型、低成本 Spartan™–3A、Spartan–3AN 和 Spartan–3A DSP FPGA 如何协助保护您的产品和利润。

假冒带来哪些财务影响?

假冒不仅会造成巨大的、不可挽回的经济损失，而且还会损坏公司的声誉，因为该领域的假冒产品而增加客户支持工作量，并且还会因为证实和处理 RMA 退货而影响公司财务底线。那些产品已经被盗的公司不得不找出假冒产品和潜在的不可靠产品，以便维护公司声誉和形象。公司未来的销售将存在危险，公司能否在行业中立足也存在问题。

2003 年，美国与假冒产品相关的交易额为 2870 亿美元，占全球全年 4560 亿美元总交易额的 63%。2004 年，据世界海关组织估计，假冒产品占全球商品贸易的 5%–7%。这一数字正在以每年 12%–15% 的速度递增，假冒产品造成了巨大的经济损失。各个行业都受到了影响，包括消费类电子、半导体器件、电池、汽车配件、货币、药品以及体育用品。在本白皮书中，您将了解到 Xilinx 提供的新型低成本 FPGA 如何帮助您免受设计领域的三大安全威胁。

主要的安全威胁有哪些?

当今设计领域所面临的主要安全威胁包括*反向工程*、*过度构建*和*克隆*。

当盗窃者出于重建或重造竞争性产品并在公开市场上销售之目的而利用您的设计时，这便是*反向工程*。反向工程的作用是窃取者可以更快地完成设计，并且可以将研发成本最小化。这是电子行业自问世以来遇到的最普遍的威胁。

当今，由于许多公司都转而外包制造，因此，他们面临着新的安全威胁：*过度构建*和*克隆*。让我们来看看这些都是什么：

*过度构建*是外包业务模型的一大隐患。在这种情况下，产品经过未授权过度构建，然后在未得到原始设备制造商许可的情况下通过其他渠道销售。最大的问题是，一旦这些产品进入市场，它将造成非常严重的后果。通常，“过度构建”的产品能够以更快的速度面市，并且其销售价格也更低。

当盗窃者以相同或不同的商标复制设计、IP 或产品，这就是*克隆*。克隆者获得的明显利益是，他们无需花费任何研发成本，并且极大地加快了克隆产品的上市。

怎样才算安全?

设计者应该做些什么? 首先，要认识到没有牢不可破的安全这一事实很重要。基本上，要完全阻止攻击者破解系统是不可能的。如果有人想要得到您的数据或设计，他们可采用蛮干来得到他们想要的东西。这不是一般的黑客，很可能是一个资金充裕的政府或者是一个资金充裕的竞争对手，因此，您不可能创建一个永远不会被破解的解决方案，而是创建能够充分保护您的设计免受克隆者、过度构建者以及反向工程者给您带来的常见威胁的解决方案。

当您想到安全时，您需要考虑满足您的需求的解决方案。如果您的产品值 10 美元，您只能在该价格范围内为该系统提供适当的安全性，而不是可能价值 10,000 美元的系统。这是您需要做的评估。完成评估后，您可以在该评估的基础上确定您希望实现的产品和安全级别。Xilinx 提供各种解决方案供您选择来解决您的安全问题，从简单解决方案到复杂解决方案。本白皮书将讨论在 Spartan–3 系列内实现的基本安全解决方案。

如果您想了解更高级的技术，您可以参照 “利用 Spartan–3A 和 Spartan–3AN FPGA 实现的高级安全技术” 一文。除了 Spartan 产品以外，Xilinx 还提供利用 Virtex™ FPGA 产品实现的更为先进的解决方案。

Spartan FPGA 实现了灵活的低成本安全解决方案

Spartan–3AN FPGA 中的 Flash 存储器和隐藏比特流

Spartan–3AN 器件带有可以用于储存配置数据的片上 Flash 存储器。如果在您的设计中 Flash 存储器没有与外部相连，那么 Flash 存储器无法从 I/O 引脚读取数据。

由于 Flash 存储器在 FPGA 内部，因此配置过程中 Spartan–3AN 器件比特流处于隐藏状态。这一配置成了设计安全的起点，因为无法直接从 Flash 存储器拷贝设计。

配置安全

保护 Spartan–3 器件不加载未知配置的最简单的方法是硬连接模式引脚，只允许 Flash 存储器自动配置和连接数据引脚。此外，任何人想要从 BGA 或 CS 封装中直接接入引脚都极其困难，因为所有电路连接都在封装之下。如果引脚是硬连接，为了加载不同的配置则需要直接攻击 PCB。

比特流发生器的安全级别

在设计的测试和调试阶段，设计者可以决定将内部配置访问端口（ICAP）或 ChipScope™ Pro 分析器核留在设计中，来方便设计投产后可能进行的维护或随机检查。一些软件工具（如 ChipScope Pro 分析器）需要这些宏命令来读取内部逻辑的状态。虽然这为设计者带来了方便，但会留下安全漏洞。

比特流发生器基于名为 NCD 文件的物理实现文件的内容创建配置 **`.bit`** 文件。 **`.bit`** 文件规定已编程 FPGA 的行为。比特流发生器包括许多选项，其中一个选项是安全级别设置。比特流发生器有四个安全级别设置，第一个是默认值，其余三个选项则提供额外的安全保护。如下表所示，读回命令操作可以被完全禁用，或者仅限于有限访问。安全级别设置及其功能如表 1 所示。

表 1: **比特流发生器安全级别设置**

安全级别	描述
无	默认值。无限制访问所有配置和读回功能。
1 级	禁用两个 SelectMAP 或 JTAG 端口（外部引脚）的所有读回功能。允许通过 ICAP 读回。
2 级	禁用所有端口上的所有读回操作。
3 级	禁用所有配置和 JTAG 端口上的所有配置与读回功能。3 级中唯一可以发出并执行的命令（读回和配置）是 REBOOT。它会擦除器件的配置。这与启用器件上的 PROG_B 引脚具有相同的功能，除了它是在器件内进行的。

了解所有比特流发生器选项的详细信息，请参照 “Spartan–3 系列配置用户指南（UG332）”。

Device DNA 安全

Xilinx 在 Spartan–3A/3AN/3A DSP 平台上提供了 Device DNA 安全，用以保护您的设计、IP 和嵌入式代码等。Device DNA 是一个 57 位 ID，每个 Spartan–3A/3AN/3A DSP FPGA 的 Device DNA 都是独一无二的。这个 ID 可以用于将设计与特定 FPGA 关联起来。设计者的个性化算法也存储在 FPGA 上，这是一种算法方程式，定义了如何获得独一无二的 Device DNA 并生成结果。利用设计者的个性化算法将这个 ID 结合起来，然后将结果存储在设计者选择的外部存储器或内部 Flash 存储器（仅限于 Spartan–3AN FPGA 器件）之类的地方。该算法是机密的，因为只有设计者知道。

Device DNA 操作

在研究系列器件的安全性如何运行之前，了解解决方案的核心是什么很重要。Device DNA 是 Xilinx FPGA 器件所独有的，特别是 Spartan–3A/3AN/3A DSP FPGA 器件，用于实现设计安全。本节讲述 Device DNA 如何运行以及如何利用我们新的专利技术保护您今后的设计。

何为 Device DNA?

Device DNA 是一个独一无二的 57 位标识符，该标识符在 Xilinx 的制造流程中被置入 Spartan–3A/3AN/3A DSP FPGA 器件。每个 FPGA 都有一个独一无二的 ID，允许您将您的设计与特定 FPGA 器件关联起来。该安全或许可流程具有绝对的灵活性。您可以轻松地在不同模型之间更改安全或许可流程，从而增强您的设计安全性。可通过外部 JTAG 端口或内部 DNA 端口访问只读 Device DNA，从而轻松连接安全算法。

如果克隆者或过度构建者拷贝了比特流并将其放入另一个 FPGA 中，那么新 FPGA 的 Device DNA 就会不一样。在采用该算法检查 Device DNA 之后，设计将返回一个未授权或失败的结果，使得用户或设计者能够决定如何应对安全威胁。

Device DNA 安全基础

Device DNA 安全流程就像 ATM 交易。要从 ATM 上取钱，您需要插入您的 ATM 卡并在键盘上输入您的密码。如果您的卡和相关的密码与存储在银行的 ID 相匹配，就会批准您的交易，您就可以取钱。如果不匹配，就会拒绝您的交易，您也就取不到钱。安全流程如图 1 所示。

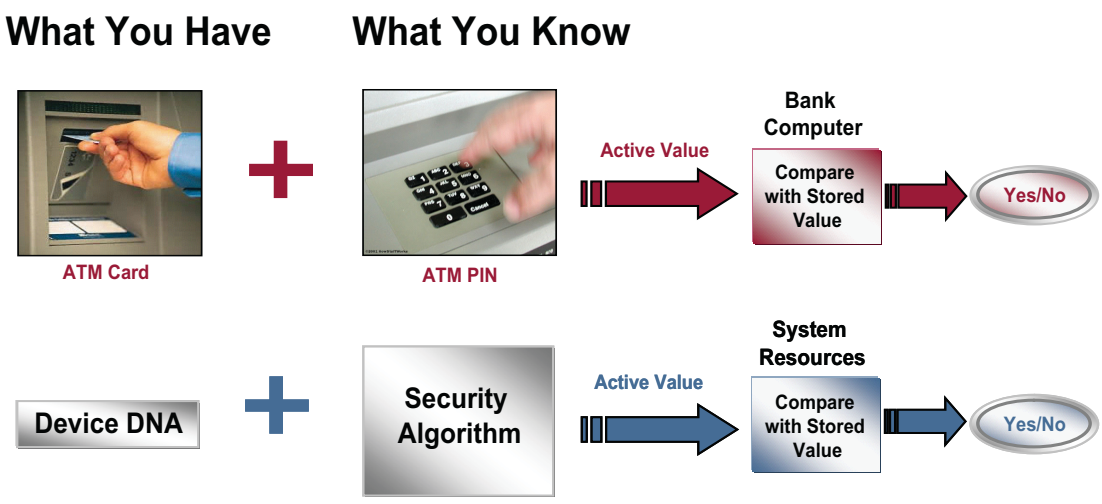

图 1: **安全流程**

安全算法和 Device DNA 都包含在 Spartan–3A/3AN/3A DSP 器件内。采用 Device DNA，安全算法就会生成校验值。虽然 Device DNA 默认的是 57 位，但是，您也可以采用更多的位来提高安全性。此外，Spartan–3AN 提供的 64 字节工厂 Flash ID 也可以在算法中使用，用以提高安全性。然后，校验值可以存储在系统资源（如配置存储器、外设存储器、系统存储器）的任何地方。如果是 Spartan–3AN FPGA，校验值也可以存储在安全寄存器的一次性可编程 64 字节用户定义字段中。该寄存器使得安全系统保持独立，而无需外部接口或存储器。

未授权操作

在正常操作过程中，器件通电，然后加载比特流来配置 FPGA。安全算法读取 Device DNA 并生成一个有效值。然后，它会比较有效值和初始设置阶段存储的校验值。如果校验值等于有效值，就会进行正常操作。当这两个值不匹配时，您可以将您的产品设计为通过以下任何一种方式响应：

- 无功能

  设计完全停止运行。这可以通过采用全局控制信号（如 3 态、门控时钟、触发器时钟使能等）来轻松实现。

- 有限功能

  设计可进行部分或基本操作。这时主要功能被禁用或绕过。这一响应允许第三方测试或合约制造商在防止过度构建的同时进行构建和测试。它还允许系统在评估或演示模式下运行。

- 定时炸弹

  设计可在关闭之前预先设定的时间段内运行所有功能。这种响应方式允许第三方测试机构或合约制造商进行构建和测试。它还允许系统以演示模式运行或进行 IP 评估。

- 自毁（仅限于 Spartan–3AN 器件）

  采用 Flash 扇区擦除和锁定保护来擦除所有扇区并将 Flash 存储器永久锁定为零。这种响应方式可防止重复进行的未授权访问尝试。

采用 Device DNA 在 Spartan–3A FPGA 中实现安全

这仅仅是在您的设计中设置安全的一种 *可能*情形。我们说 *可能*，是因为这与决定您家里的安全系统相似。如果世界上只有一把 *可能*的锁和钥匙，那就没有安全可言。在最初的一次性设置流程中，可以通过 JTAG 端口或从 FPGA 的结构内部读取 Spartan–3A/3AN/3A DSP FPGA 的 Device DNA。然后就可以生成校验码。接着，该校验码（校验值）被存储到系统中的某个地方，比如配置或系统存储器中。这可以在图 2 的紫色区域中看到，它说明了这一可能实现过程。

接下来，我们看到 Device DNA 是蓝色的，“秘密的”安全算法和关键 / 种子代码（如果那是您的设计所采用的）是绿色的。最后，会有一个比较器或几个选项给出授权的和未授权的结果。

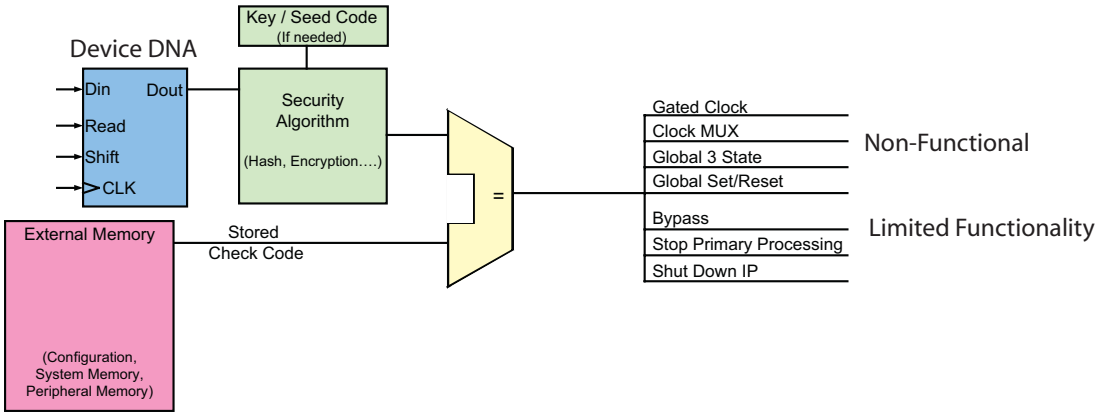

图 2: **Device DNA 安全实例**

在这种设置情形下，将会出现以下操作顺序：

1. 器件通电，加载比特流，进行配置。安全算法和 Device DNA 都包含在 Spartan–3A 器件中
2. 读取 Device DNA，并将其发送至安全算法
3. 安全算法生成有效代码（结果）
4. 比较结果（有效代码）和存储的校验码
5. 如果存储的校验码等于计算出的有效代码，设计就被授权
6. 如果两个代码不匹配，设计就不会被授权并且会按设计者设置的方式响应。可以为未授权设计设置多种响应方式，比如，无功能、有限功能以及定时炸弹。

这也只是一种简单的可能情形。还可以轻松实现更复杂的安全性。

凭借 Spartan–3AN Device DNA 和工厂 Flash 存储器 ID 保证安全

在我们的非易失性 FPGA – Spartan–3AN 平台中，采用了与 Spartan–3A 器件几乎相同的工艺，只是进行了一些增强。第一种安全增强是比特流隐藏在 FPGA 内。这使监控变得更加困难。

Spartan–3AN FPGA 的第二种安全增强是两个独一无二的序列号：Device DNA 和 Flash 存储器内的工厂 Flash ID。这两个独一无二的 ID 序列号超过 70 字节，从而实现了更多的算法可能性，因此，大大增加了破解安全算法所需的时间。该设计现在专门融合了 FPGA 和 Flash ID。

拥有两个独一无二的 ID 就像需要两张不同的 ATM 卡才能取钱一样。如果您想提取现金，您必须持有两张卡。如果其中一张卡丢失了，您的钱不会被取走并且仍然是安全的。

第三种改进在于存储的校验码。在 Spartan–3AN 平台上，安全代码可以存储在安全寄存器的特殊一次性可编程 64 字节用户定义字段中。该寄存器使得安全系统保持独立，而无需外部接口或存储器。该特性增强了总体安全性并且使产品的反向工程变得更加困难。

安全算法是用户定义的，允许设计者以适当的系统成本实现合适的安全级别。安全算法也是安全系统的首要机密。安全流程中的东西必须是机密，这样才能保证系统不被破解。由于算法是未知的，因此它是设计级安全的关键所在。算法是在 FPGA 架构内实现的，因此它只是 FPGA 内数百万个配置位中的少数几位。除非您知道比特位是怎样连在一起的，或者算法是怎样操作的，否则对于旁观者或克隆者来说，它只是一堆数字。

下图 3 给出了采用 Spartan–3AN 器件的一个可能流程。

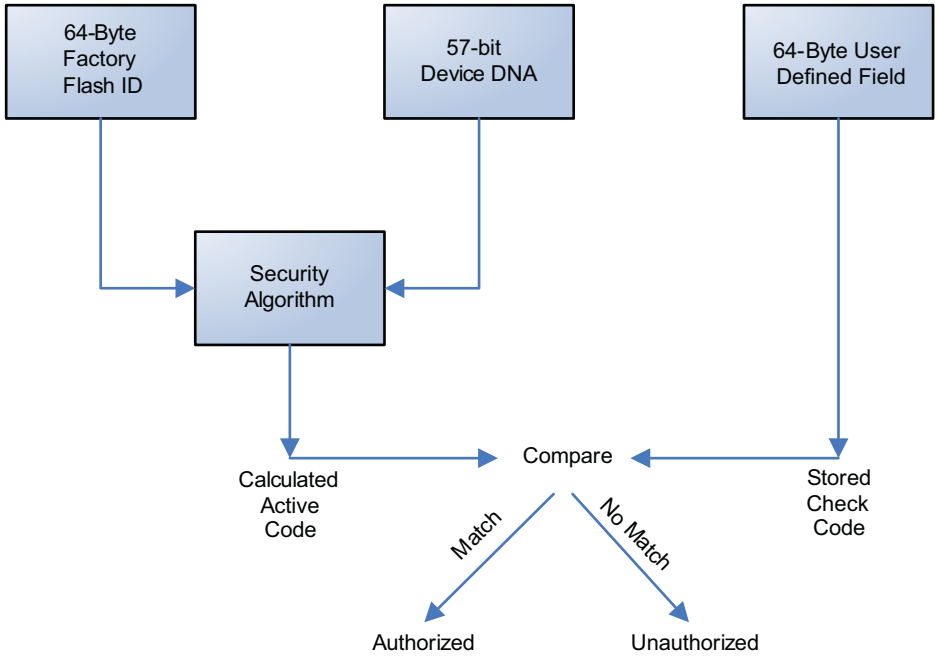

图 3: **Spartan–3AN 安全**

下图 4 中的 Spartan–3AN 设计级安全是一种完全独立的安全解决方案。Flash 既包含 FPGA 配置比特流，又包含以前生成的校验码。该校验码由可信赖的 / 安全的制造商或者注册流程存储在一次性可编程 Flash 存储器用户字段中。

在通电时，FPGA 正常配置。配置完成后，FPGA 应用包括验证是否批准设计在相关的 Spartan–3AN FPGA 上操作的电路。安全算法读取 Device DNA 和工厂 Flash ID，反过来，安全算法又会生成有效代码，并将该有效代码与以前生成的存储在 Flash 用户定义字段中的校验码进行比较。如果这两个代码相同，器件就被授权。否则，该器件就是非法的并且不会被授权。

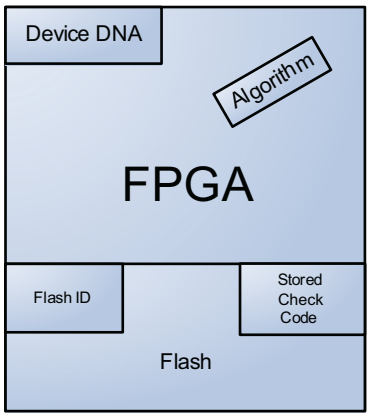

图 4: **Spartan–3AN 安全**

处理授权失败是 Device DNA 设计级安全的另一个优势。设计级安全的其他优势是，它可以被完全整合到设计中。未授权设计可以有多种响应模式，这跟 Spartan–3A 平台一样。

Spartan–3AN 平台中的设计级安全提供了多种保护设计不被过度构建、克隆和反向工程的方法。除本文以外，您还可以了解更多关于如何保护您的低成本 FPGA 设计的知识。了解利用我们的 3 个系列的产品实现设计安全方面的更多信息，请参照我们的“Spartan–3 系列配置用户指南”（ http://www.xilinx.com/cn/bvdocs/userguides/ug332.pdf ），来了解保护您的设计安全方面的更多信息。了解高级技术方面的信息，请参照 白皮书 267。

Xilinx 的其他安全解决方案

Virtex–4 和 Virtex–5 FPGA 采用 AES 加密算法实现安全性。两个产品系列都将关键位存储在易失性存储器中，该存储器通过电池供电，具有很长的使用寿命。有趣的是，FIPS 140 标准要求 “密钥归零”，而采用该技术在断电时这种情况就会自动发生。因此，如果电源被中断，在比特流加密的情况下，部件就无法使用了。

Virtex–5 系列器件支持 256 位 AES 加密 / 解密技术，从而可以获得很高的设计安全级别。由于具有 1.1 X 10^{77} 种可能的密钥组合，所以如果不知道正确的加密密钥，几乎不可能克隆外部截获的比特流。

CoolRunner™–II CPLD 是非易失性的，并且提供一些对保护设计有用的额外变量。由于具有多位读 / 写保护功能，并采用非易失性 EPROM 技术，原来的 CoolRunner–II CPLD 已经可以提供很高的安全性。它不会直接曝露比特流，并且还具有读保护功能可以防止从内部读取数据。其它客户反馈显示，可以对其进行改进，进行一些合理的“向上兼容”改进。在第 1 步 CoolRunner–II CPLD 的介绍中提到，已经增加了新的安全特性，包括 **`Read Protect + Boundary Scan Disabled`** 和 **`One Time Programmable`**。了解 CoolRunner–II 安全方面的更多信息，请参照白皮书 265。

结论

通过反向工程、过度构建或克隆进行的安全攻击会使公司由于未实现销售额、投资回报和技术支持而遭受巨大的经济损失。这些成本和损失是永久的，不可挽回的。Spartan–3A/3AN/3A DSP 平台可协助保护您的设计免受这些威胁。Device DNA 安全允许您将您的设计与特定器件关联起来，从而大大降低了安全威胁。Spartan–3AN 平台的其他设计级安全特性包括片上 Flash 和隐藏比特流配置，提供了更多防止安全威胁的保护功能。

参考文献

Xilinx 技术文档

Xilinx 的下述技术文档提供了低成本 FPGA 和 / 或安全性的补充信息：

Spartan 安全应用技术文档

1. UG332，*Spartan–3 系列配置用户指南*（包含更多如何保护您的设计方面的信息）
2. WP267，*高级安全技术（利用 Spartan–3A 和 Spartan–3AN FPGA 实现高级安全技术）*
3. DS529，*Spartan–3A FPGA 系列数据手册*
4. DS557，*Spartan–3AN FPGA 系列数据手册*
5. DS610，*Spartan–3A DSP FPGA 系列数据手册*
6. WP261，*FPGA 内的 IP 安全*
7. XAPP780，*采用 Dallas Semiconductor/Maxim DS2432 安全 EEPROM 实现 FPGA IFF 拷贝保护*

Virtex 系列安全白皮书

1. WP155，*在选定的 Virtex–II 器件中采用三重 DES 加密技术*
2. WP261，*FPGA 内的 IP 安全*

CoolRunner–II 安全应用指南和白皮书

1. XAPP371，*CoolRunner–II Galois Field GF (2^M) 乘法器*
2. XAPP374，*CryptoBlaze，8 位安全微控制器*
3. WP170，*安全应用中的 CoolRunner–II CPLD*
4. WP265，*CoolRunner–II 的增强型安全特性*

入门套件 / 设计板

http://www.xilinx.com/cn/products/devboards/index.htm

相关参考文献

下述技术文档和链接提供对了解安全问题有用的辅助材料：

1. Anderson, Ross。*安全工程：构建可靠的分布式系统的指南：*

   http://www.cl.cam.ac.uk/~rja14/book.html
2. Anderson, Ross, Mike Bond, Jolyon Clulow, and Sergei Skorobogatov。*密码处理器——概况*

   http://www.cl.cam.ac.uk/~mkb23/research/Survey.pdf
3. Schneier, Bruce。*应用密码学*，John Wiley Sons, 1996
4. Dolan, D. G. Abraham, G. Double 及 J. Stevens。*交易安全系统*，IBM 系统杂志第 30 期 2 号（1991），第 206–229 页
5. 医疗信息保密：

   http://www.hhs.gov/ocr/hipaa/
6. 其他政府机构：

http://www.nist.gov/

http://csrc.nist.gov/CryptoToolkit/aes/ (AES)

http://www.itl.nist.gov/fipspubs/fip180-1.htm (SHA)

http://csrc.nist.gov/cryptval/ (FIPS 140-1, FIPS 140-2)

7. Certicom

   http://www.certicom.com

8. RSA

   http://www.rsa.com/

9. Menezes, A.J., P.C. van Oorschot 及 S.A。Vanstone，*应用密码学手册*，1996 年，CRC 出版社。还可以在以下网站上找到：
   http://www.cacr.math.uwaterloo.ca/hac/

10. Kerchoffs, Auguste。*La cryptographie militaire*, Journal des sciences militaires，第九卷，第 5-83 页，1883 年 1 月，第 161-191 页，1883 年 2 月。

修订历史

本技术文档的修订历史如下表所示。

日期	版本	修订
2007 年 7 月 24 日	1.0	Xilinx 最初版本。