FPGA 密码模块恶意木马后门设计

孙海涛[1]，刘 洁[2]，何循来[1]，俞文文[1]
(1. 军械工程学院 火炮工程系，河北 石家庄 050003；
2. 军械工程学院 装备指挥与管理系，河北 石家庄 050003)

摘 要：FPGA 器件安全性包括数据安全性和应用程序安全性两部分。FPGA 生命周期的各个阶段对其安全性都会产生至关重要的影响，由于 FPGA 电路在设计和生产中的脆弱性，使得恶意木马电路能够有机可乘。针对 FPGA 器件开发阶段，以 FPGA 密码模块为目标，设计能够泄露密钥的恶意木马后门电路，对于了解硬件木马实现机理、警示 FPGA 芯片安全具有重要作用。

关键词：恶意木马；FPGA 安全；硬件后门；密码模块
中图分类号：TP309 **文献标识码**：A **文章编号**：1674-7720(2013)22-0020-03

Design of vicious trojan backdoor for FPGA cryptographical module

Sun Haitao[1], Liu Jie[2], He Xunlai[1], Yu Wenwen[1]
(1. Department of Artillery Engineering, Ordnance Engineering College of PLA, Shijiazhuang 050003, China;
2. Department of Equipment Command & Management, Ordnance Engineering College of PLA, Shijiazhuang 050003, China)

Abstract: Security of FPGA contains two parts of data and program. Each phases in the life cycle of FPGA can bring significant influence for its security. The vulnerabilities in today's design and fabrication process have raised the possibility of malicious circuit modification as known as trojans in a design to impact the functionality or transmit key information to the adversary. This paper designs a hardware trojan of transmitting key information towards FPGA. It is importantation to realize the implement mechanism and raise the attention to IC security.

Key words: vicious trojan; FPGA security; hardware backdoor; cryptographical module

硬件恶意木马电路是恶意攻击者在量产集成电路(IC)的设计、制造或二次开发等过程中，出于某种特殊目的人为制造的非法电路[1-3]。这种硬件攻击方式通过预先设定“电子后门”，可以轻易地绕过硬件密码等安全壁垒，对现行的硬件安全模型构成重大威胁。目前还没有阻止硬件木马出现的有效办法，其根本原因是由于 IC 设计与制造的全球化过程并不能保证其使用安全性。此外，对于一般设计者来说，在设计过程中使用了非可信第三方开发的软件工具、IP 核或标准单元，也会不自觉形成硬件木马。但是对于军方和安全情报部门，为了获取情报或其他目的，植入硬件木马是非常理想的选择[4]。

本文研究了芯片硬件木马实现的基本方法，并且针对集成电路在初始设计和后续生产等环节中存在的安全隐患，在现有的商用 FPGA 平台上设计了一种无线载波泄密型硬件木马，使目标芯片能够在正常加解密工作的同时，以使用者不能察觉的方式通过载波将密钥传送出来。

1 FPGA 安全性与硬件木马

FPGA 器件作为一项成熟技术，已经被广泛应用到军事、空间、电子消费产品和汽车等各个领域，是现代密码协议、算法实现的优选平台。但与此同时，其安全性也受到人们的广泛关注。目前对 FPGA 安全性的研究主要有两个方面：(1)FPGA 的数据安全性，必须提供对 FPGA 上运行的应用程序的保护。芯片内部数据以及与外围电路之间的通信数据都需要被保护，主要方法是在 FPGA 内部集成数据加密方案。(2)FPGA 的设计安全性，即如何设计 FPGA 以抵御克隆及逆向工程方法的攻击，传统上也就是知识产权(IP)保护。

FPGA 器件的生命周期可分为 3 个阶段：(1)制造阶段中，主要依赖于第三方制造公司(通常位于亚洲)来制造物理器件；(2)设计开发阶段中，设计开发人员将 FPGA 组合成一个最终的系统，并对其编程以实现它的功能；(3)发行使用阶段中，FPGA 能够被广泛的使用。图 1 所示分别对这 3 个阶段的 FPGA 密码器件安全问题进行了

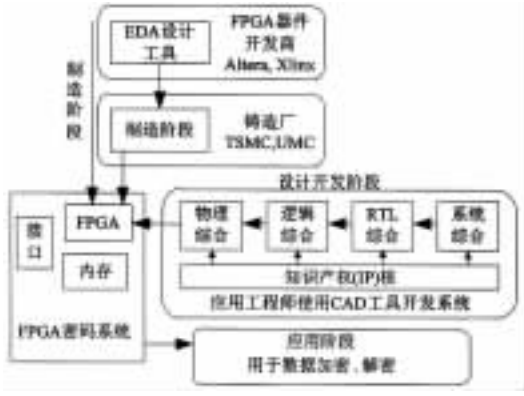

图 1 FPGA 密码器件生命周期

描述[5]。

在 FPGA 生命周期的各个阶段，其自身的安全性都可能受到来自硬件木马电路的威胁。攻击者将针对 FPGA 整个生命周期中最薄弱的环节和最易发现的弱点进行攻击。由于芯片的设计、制造、测试在不同的公司，甚至是不同的国家，保持整个生产环节的安全是很困难的，使得 FPGA 芯片内的安全状态可以被恶意程序非法读取或破坏，恶意实体能够通过程序和数据更新机制更改硬件的可信度。总之，在 FPGA 生命周期的每个步骤中均可能生成硬件木马。

硬件恶意木马可以实现三类功能：(1)篡改硬件功能，通过增加、删减或绕过已有电路逻辑的方式来改变电路功能；(2)篡改硬件规格，通过修改线路和晶体管几何形状等方式改变电路的参数特征，使得电路芯片可靠性降低并在特定的激励效应下失效；(3)泄漏秘密信息，通过设计特殊的电路传递密钥等秘密信息，或植入具有定位功能的芯片完成相关工作[6]。

本文针对 FPGA 器件设计开发阶段，以商用 FPGA 器件加解密模块为研究目标，设计并开发了嵌入加密模块内部的泄密型硬件木马电路，对于研究 FPGA 硬件攻击技术原理、提高芯片安全等级、加强敏感数据保护、警示集成电路芯片安全具有重要作用。

2 FPGA 密码模块恶意木马后门设计

本文以运行 RSA 密码算法的 FPGA 器件加解密模块为研究对象，在该平台内嵌入载波型硬件木马原型电路，实现通过 AM 载波将平台加解密密钥信息对外广播，从而实现木马设计者利用无线接收机接收加解密密钥。

FPGA 器件主平台上运行 RSA 密码算法加解密模块，为方便监控，利用 PC 串口发送程序向 FPGA 密码模块发送明文（待加密信息），在密码模块进行加密操作后，FPGA 平台将密文（已加密信息）反馈给 PC。这是 FPGA 平台工作的主要流程。FPGA 器件选用 Xlinx 公司 Spantan3 系列的 XC3S400 芯片，整个 FPGA 平台有 4 大组成部分：(1)时钟模块，用于转换所需时钟；(2)串口接收模块，用于接收 PC 送来的明文；(3)加密模块，用于运行 DES 算法；(4)串口发送模块，用于将加密后的密文发送给 PC 进行显示。

FPGA 平台的整体设计如图 2 所示，木马电路的工作是在平台运行加密操作的同时获取加密密钥，并将密钥信息进行调制后经 AM 载波向外部传递。木马电路具体设计如图 3 所示，硬件木马电路在 FPGA 平台进行加

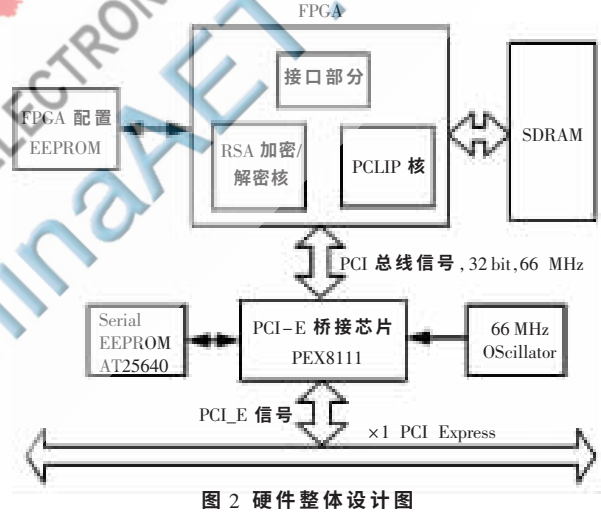

图 2 硬件整体设计图

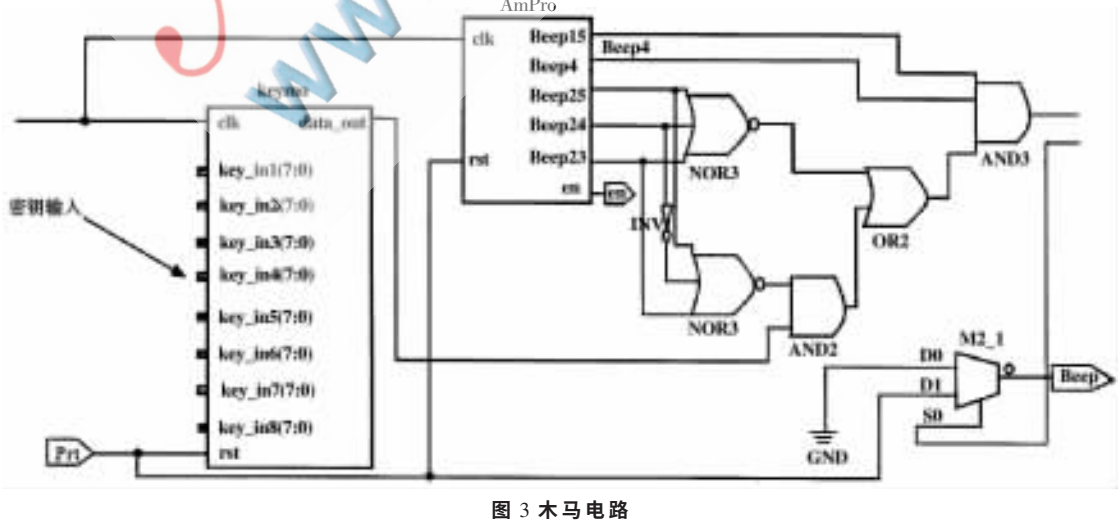

图 3 木马电路

密操作时，由 keymo 模块获取加密密钥，经 AMPro 模块，由 Beep4 引脚接到电路板的插座上，将密钥通过 AM 调制方式发射出来，并可用无线接收机进行接收。

电路存在两种工作状态：(1)在木马电路未激活时，芯片以正常方式工作，接收 PC 传来的明文，并对明文进行 RSA 加密操作；(2)激活硬件木马电路。通过向电路发送“lucky”字符的方式激活木马电路，之后，RSA 密码程序正常工作，而与此同时，FPGA 芯片可以通过将电路板上 AMPro 模块插座的 Beep4 引脚作为天线的方式实现将 RSA 密码算法进行加密的密钥通过载波的方式暗中发射出来。

本文实现了通过 1 560 kHz 和 50 MHz 两种载波频率完成无线信号发送任务的模式。在实际的应用中也可以实现更多的频率，相对发射距离与所选择的信号频率成正比关系。以 1 560 kHz 发射为例，Beep4 用于产生方波，在进行 RSA 密码加密时，配合一个 26 位时钟的 AMPro 计数器模块，密钥寄存器 keymo 模块就可以将输入密钥以串行模式进行输出。

本文以商用 FPGA 密码模块为研究目标，设计并实现了载波泄漏型恶意木马后门电路，验证了在 FPGA 器件生命周期的设计开发阶段植入安全威胁的可行性，对于集成电路设计、加工、使用过程中的安全问题起到了一定的警示作用。

参考文献

[1] TEHRANIPOOR M, KOUSHANFAR F. A survey of hardware trojan taxonomy and detection[J]. IEEE Design and Test of Computers, 2010, 27(1): 10-25.

[2] BHAMIDIPATI H. Single trojan injection model generation and detection[D]. Cleveland: Case Western Reserve University, 2009.

[3] POTKONJAK M, KARRI R. Special issue on integrated circuit and system security[J]. IEEE Transactions on Signal Processing, 2010, 58(11): 5968.

[4] FELLER T, DEMIREZEN A. Hardware trojans: data leakage using general purpose LEDs[Z]. Technical Report-TUD-CS-2010-2384, 2010.

[5] 张鹏，邹程，邓高明，等.基于电磁泄漏相关性分析的硬件木马设计[J].华中科技大学学报(自然科学版)，2010，38(10)：22-25.

[6] 胡桂廷，陈向东.基于 LabVIEW RT 的自动测试系统的研究与实现[J].微型机与应用，2012，31(18)：5-7.

(收稿日期：2013-08-27)

作者简介：

孙海涛，男，1981 年生，讲师，博士，主要研究方向：武器系统与运用工程。

刘洁，女，1981 年出生，讲师，博士，主要研究方向：作战模拟与仿真。

何循来，男，1969 年出生，副教授，博士，主要研究方向：兵器科学与技术。