

doi: 10.3969/j.issn.1006-1576.2012.04.018

载波泄漏型硬件木马芯片设计

孙海涛¹, 刘洁²

(1. 军械工程学院火炮工程系, 石家庄 050003; 2. 军械工程学院装备指挥与管理系, 石家庄 050003)

摘要: 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, 设计一种泄密型硬件木马芯片, 使芯片能够在进行加密的同时将密钥传送出来。研究芯片硬件木马实现的基本方法, 在现有的商用 FPGA 平台上植入木马, 通过载波的方式泄露密钥。结果表明: 该设计能在使用者毫不知情的情况下, 利用硬件攻击获取秘密信息。对于进一步认识芯片硬件木马攻击实现机理, 警示集成电路芯片安全具有一定的作用。

关键词: 硬件木马; AM 载波; FPGA

中图分类号: TJ02 **文献标志码:** A

Design of Carrier Wave Leakage Hardware Trojan

Sun Haitao¹, Liu Jie²

(1. Dept. of Artillery Engineering, Ordnance Engineering College, Shijiazhuang 050003, China;

2. Dept. of Equipment Command & Management, Ordnance Engineering College, Shijiazhuang, 050003, China)

Abstract: Aiming at the safety danger of initial design and subsequent production of integrated circuit, design a secret leakage hardware Trojan chip, and chip encrypts and sends secret key at the same time. The thesis researches the basic method of the chip hardware Trojan realization. Implement Trojan in business FPGA platform, and leak secret key through carrier wave. The result shows that the design can use hardware attack to acquire secret information when users don't know anything about this. It is important to realize the implement mechanism and raise the attention to IC security.

Key words: hardware Trojan; AM carrier wave; FPGA

0 引言

当前, 伴随着半导体设计、制造与使用进一步全球化的发展趋势, 集成电路 (integrated circuit, IC) 已经在军事系统、金融基础设施等众多领域得到广泛应用, 其安全性问题也得到了极大的关注。

硬件木马 (hardware Trojan) 是通过在集成电路设计、制造或二次开发等过程中人为地制造一些非法电路, 从而留下“电子后门”, 为后续攻击打开方便之门。这种新型的硬件攻击方式可以轻易地绕过十分坚固的硬件密码等安全壁垒, 对现行硬件安全模型构成重大威胁^[1]。笔者以成品 FPGA 电路板为研究目标, 开发泄密型集成电路芯片硬件木马, 以了解硬件木马实现机理, 警示集成电路芯片安全。

1 硬件木马基本原理

硬件木马的 3 类功能^[2]包括:

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。

硬件木马是一种小型木马, 在百千万级的大规模和超大规模电路中只需几十个或几百个门电路就可以实现功能, 不容易被注意及发现, 犹如安装了一枚定时炸弹, 一旦经触发激活, 就有可能受控于敌方。目前还没有阻止硬件木马出现的有效办法, 这是由 IC 的设计与制造过程所决定的^[3]。IC 的生产过程包含 3 个主要阶段: ① 设计者利用 IP 核、模型与设计工具进行电路设计; ② 制造商对原始设计生成掩模, 加工并封装; ③ 对产品进行功能与性能测试。在每个步骤中均可能生成硬件木马^[4]。对一般设计者来说, 尽管没有植入硬件木马的恶意, 但是由于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, 从而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^[5]。

笔者主要研究芯片第 3 阶段中的硬件木马实现, 主要思路是在成品 FPGA 电路当中, 开发硬件木马, 实现在木马启动后能够通过 AM 载波发射信号, 完成向木马设计者传递秘密信息的功能。

收稿日期: 2011-10-16; 修回日期: 2011-11-09

作者简介: 孙海涛(1981—), 男, 吉林人, 博士, 讲师, 从事武器系统与运用工程研究。

2 载波泄露型硬件木马设计

笔者以运行 DES 密码算法的 FPGA 电路板为研究对象,目标是在该平台上插入硬件木马原型电路,通过 AM 载波将密钥等信息发射给无线电接收机,从而实现木马设计者的泄密接收及密码获取。

2.1 DES 密码平台设计

DES 密码算法实现于 FPGA 板,整个设计如图

1 所示,PC 机通过串口给 FPGA 密码芯片发送明文, FPGA 进行加密,将密文发送给 PC 机。

FPGA 选用 Spantan3 系列的 XC3S400 芯片,整个设计由 4 部分组成,时钟模块 clk40 用于转换所需时钟,串口接收模块 Serial 用于接收 PC 机送来的明文,des_complete 模块用于进行 DES 加密,Send 模块是串口发送模块,用于将加密后的密文发送给 PC 机进行显示。

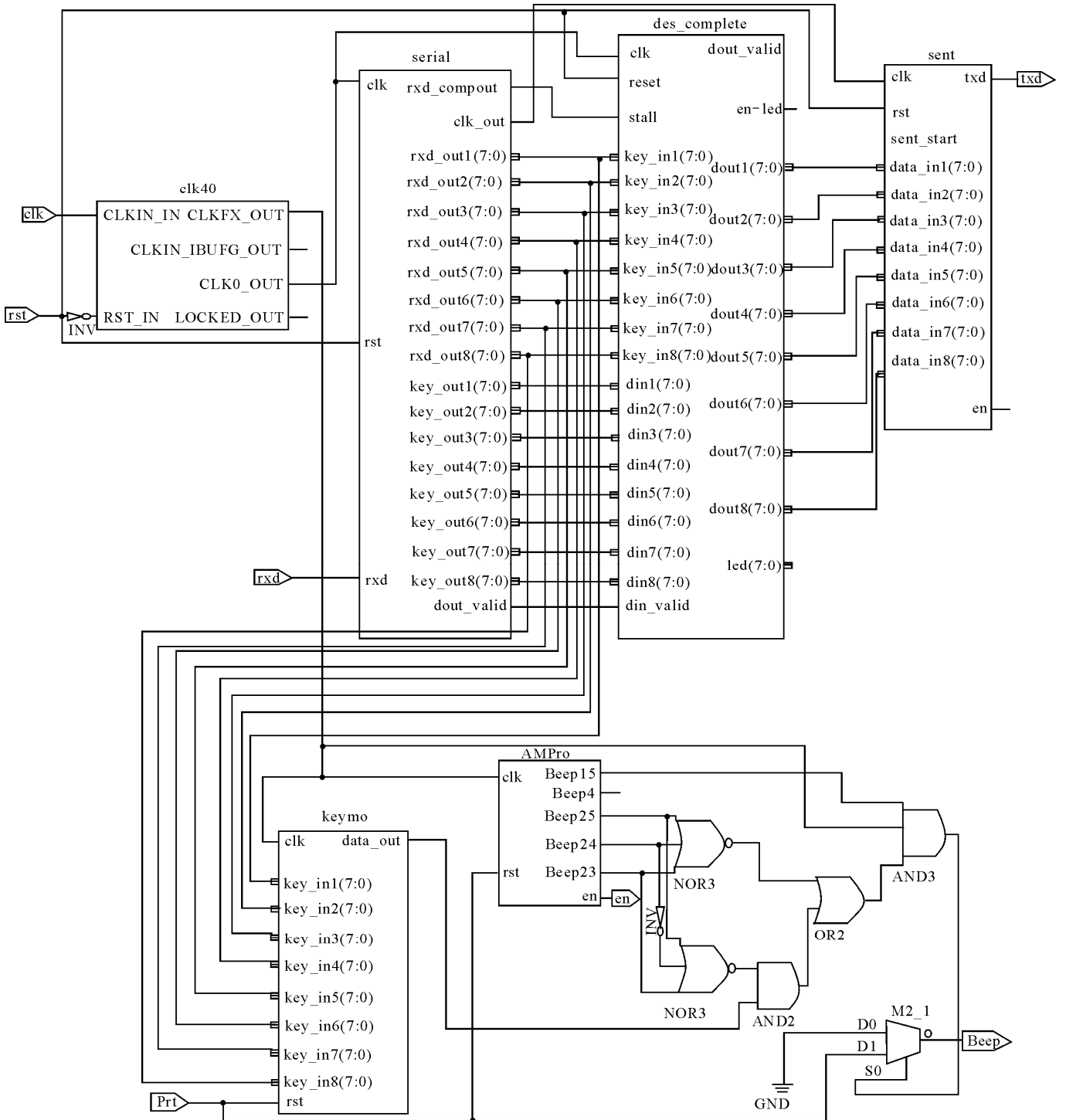


图 1 DES 密码平台设计

图 1 的下面部分是硬件木马模块。硬件木马在 FPGA 进行加密时, 每次加密将密钥由 keymo 模块获取, 经 AMPo 模块, 由 Beep 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。

2.2 硬件木马植入

在电路设计中, 使用电路板上的插座的一个插脚作为天线, 因为插脚正交于电路板的地, 因此它比一般的插头与插脚更好。笔者实现了 1 560 kHz 和 50 MHz 2 种载波发射频率, 都可以通过无线电接收机(收音机)进行远程接收。在实际的应用中也

可以实现更多的频率, 频率越高, 相对发射距离越远。

整个电路在木马未激活时, 芯片可以正常进行 DES 密钥加密。一旦木马激活后, DES 密码程序正常工作, 而与此同时, FPGA 芯片可以通过一个冗余的引脚将 DES 密码的加密密钥暗中发射出来。

整个系统的工作流程为: 系统通过上层软件经 PCI-E 总线将明文送给 PCI 加密卡进行加密, PCI 加密卡加密完成后, 通知上层软件进行接收显示密文。要触发木马, 只需要在发送的明文包含“Lucky”, 即可激活木马, 从而泄露密钥。

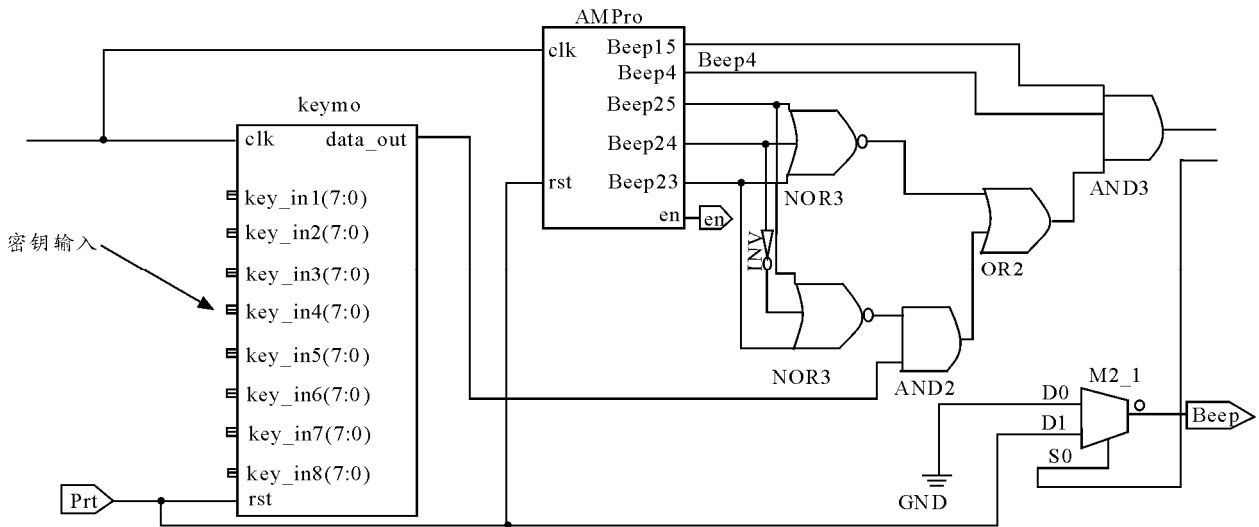


图 2 木马电路设计图

木马电路具体设计为: 以 1 560 kHz 发射为例, 在 DES 密码进行工作时, 将密钥寄存器引入 keymo 模块, keymo 模块用于将并行输入密钥变为串行输出。其中 AMPro 是一个 26 位时钟计数器模块, Beep4 用于产生一个载波频率 1 560 kHz 的方波, Beep15 用于产生音调频率为 762 Hz。Beep25、Beep24 及 Beep23 用于产生声音间的停顿。通过调制, 用普通收音机可以接收到当密钥输入为“1”时, 产生“哔, 哔”2 声音调, 而当密钥输入为“0”时, 产生“哔”的一声音调, 从而达到泄露私密信息的目的。如图 2。

整个木马电路占用 3 个 Slice, 相对整个 FPGA 资源来说占用资源非常少, 并且只在触发条件下工作, 因此具有很强隐蔽性。该硬件木马能够通过载波调制的方式将密钥发射出去, 通过普通收音机能够在一定距离进行接收。实物平台如图 3。

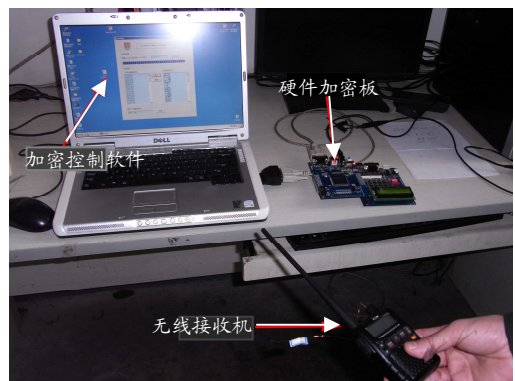


图 3 FPGA 硬件加密板木马泄漏演示平台

3 结论

笔者设计并完成了安插在运行 DES 密码算法的 FPGA 电路板中的硬件木马, 实现了密码电路在硬件攻击下通过无线载波泄露秘密信息的功能, 为了解泄密型木马实现机理奠定了基础。同时, 对于

