电子科技 2017 年第 30 卷第 6 期
Electronic Sci. & Tech. /Jun. 15,2017

doi:10.16180/j.cnki.issn1007-7820.2017.06.006

基于 FPGA 的加密算法验证平台设计

姚 霁

(西安邮电大学 自动化学院,陕西 西安 710121)

摘 要 为加快加密算法芯片的设计周期,提出了一种基于 FPGA 的设计验证平台,即将加密算法用 FPGA 加以实现,并利用数码显示直观观测结果,以验证设计的正确性。以 DES 算法为例,详细论述了该平台的系统结构,控制原理以及加密算法的设计验证过程。实验结果表明,该 FPGA 设计验证平台不仅缩短了加密算法的硬件开发开发周期,还为加密算法的开发提供了灵活性和实用性。

关键词 加密算法; FPGA; 验证平台

中图分类号 TN919.81; TP309.7 **文献标识码** A **文章编号** 1007-7820(2017)06-021-03

Design of Validation Platform of Encryption Algorithm Based on FPGA

YAO Ji

(School of Automation, Xi'an University of Posts and Telecommunication, Xi'an 710121, China)

Abstract A validation platform based on FPGA is put forward for shorter implementation cycle of encryption algorithm chip. The encryption algorithm is implemented in FPGA. The cipher texts can be observed with digital display circuits. The implementation example of DES Encryption algorithm is given. The system architecture, control principle of this validation platform and the implementation of DES algorithm are descripted. It is shown that the implementation cycle of encryption algorithm is shortened on this FPGA validation platform. The reliability, practicability and feasibility for encryption algorithm implementation are also guaranteed on this platform.

Keywords encryption algorithm; FPGA; verification platform

高密度、高复杂度、高安全性已成为加密芯片设计的主流趋势,但同时也提高了设计和验证的复杂度。它将系统概念设计、建模与架构设计、RTL 设计、物理实现等需求集中在一起,所有流程都必须经过严格缜密的仿真和验证。因此加密芯片设计约 70% 的工作量是在验证环节。而设计实现基于加密算法的 FPGA 验证平台不仅能够研究特定的加密芯片算法,而且利用该平台可扩展性好、可移植性强的特点,能够在该平台上实现多种加密算法[1]。

1 基于 FPGA 的验证平台系统框架

为了提高加密算法芯片设计的验证速度和质量,以 FPGA 为原型设计的验证平台无疑是好的选择。把加密算法用 FPGA 进行实现,在 FPGA 的验证平台平台中预留出加密算法的接口,即可在平台上直观验证加密算法的正确性[2]。同时在实验多种加密算法时,只需要把各种加密算法"插入"到 FPGA 中,即可直观快速的实现各种算法的验证。

1.1 验证平台的设计及系统框图

基于 FPGA 的加密算法硬件设计验证平台系统由平台控制电路和算法设计实现两大模块组成。加密算法设计模块完成算法的硬件实现,是算法设计的核心,也是该 FPGA 验证平台可移植扩展的部分,为尝试不同的加密算法实现提供了可行性。平台控制电路包括分频模块、扫描控制模块、编码显示控制模块,它是整个 FPGA 验证平台的核心,为算法模块提供时钟输入源,以及对算法的操纵和显示控制。当加密算法完成,并在 FPGA 平台上实现后,可以清楚地通过电子数码显示来验证加密算法的正确性。系统框图如图 1 所示[3]。

时钟控制部分采用片上 OSC 供入,利用 FPGA 的 DCM 专用时钟管理资源进行时钟管理,输入部分采用 4×4 矩阵键盘,键盘扫描采用延时确认按键的方法,将键值存储在缓存单元中,供加密算法使用。显示部分可采用数码管或液晶显示器,然后在其上显示按键值(即明文 M)和加密的结果(即密文 C),显示依次按

收稿日期:2016-06-02
作者简介:姚霁(1977-),女,硕士,讲师。研究方向:加密芯片、FPGA 设计。

下的键值,即当前按键值在最末位显示,之前的按键值依次左移显示。当加密算法(如 DES、AES、IDEA 等)实现后,将算法实现结果下载到 FPGA 中,就能够在密钥给定的情况下,对连续输入的字符不间断的进行加密,并将加密密文在平台上显示出来[4]。

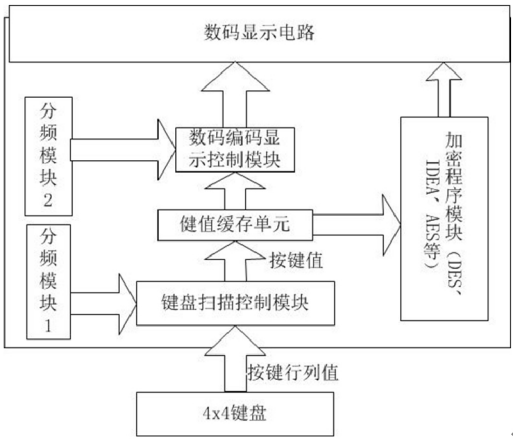

图1　加密算法 FPGA 验证平台系统框图

1.2　验证平台各控制模块的实现

本验证控制平台电路的设计采用 3 个子模块来实现键盘扫描和数码显示功能,分别为分频模块、扫描控制模块、显示编码控制模块,数字电路设计模块结构如图 2 所示。

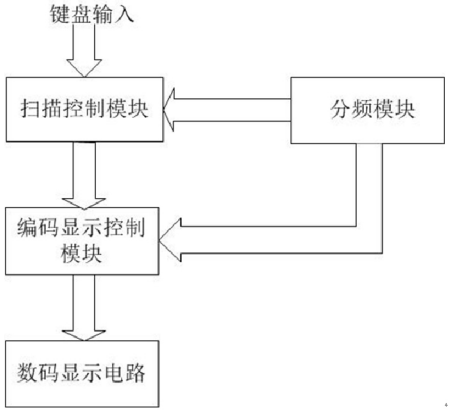

图2　数字电路设计模块框图

1.2.1　时钟分频模块

时钟分频模块的功能是对输入时钟 CLK 进行管理,为键盘扫描控制、数码显示控制以及算法实现模块提供时钟信号。该分频模块支持可配置模式,可根据不同的加密算法,提供不同的控制时钟,同时也为低功耗设计提供了可能[5]。当算法中某个模块不工作时,关闭其时钟,既能简化电路,减少控制信号,减少门的翻转次数,降低芯片集成度,进而达到降低功耗的目的。

1.2.2　键盘扫描控制模块

键盘扫描模块主要完成键盘去抖动以及键盘扫描控制。键盘扫描控制是将按键连接成矩阵,每个按键位于某行、某列的交点上,先通过扫描方式确定按下键的行值和列值,即位置码。再查表将位置码转换为按键码值。此类键盘的按键识别方法主要是行扫描法[6]。由于执行扫描的过程由硬件逻辑实现,故在执行键盘扫描时应注意两个问题:

(1)将按键在闭合过程中往往会有一些难以避免的机械性抖动,使输出信号也发生抖动,通常达 10 ~ 20 ms。若不避开抖动区,则可能误认为多次按键;

(2)当前一个键值还未送出又有按键按下时,后边的键值将覆盖前边的键值,从而造成数据丢失。

根据以上键盘扫描原理及执行键盘扫描时应注意的问题,在程序设计时设置了硬件延时电路,延迟数十 ms 后才读取键值在此设置一个控制信号 OE,使前一键值送出后才允许产生后一键值,或者设置一组寄存器保存前面若干个键值,等待系统逐个按序处理[7]。

当连续几次扫描到同一个按键时,则认为此键被按下。然后 OE 置高电平,禁止扫描并同时开始延时,此时对 ROW、COLUMN 输入信号进行检测,以判断哪个键被按下,并送出相应的即时键值 GOUT (BCD 码)存入寄存器。当 CNT 达到某一数值时,OE 重置为低电平允许重新扫描并再次延时,直到检测到其他键值[8]。这样就可以达到良好的防抖效果,提高按键的正确识别率。

1.2.3　编码显示控制模块

编码显示模块对键值进行编码,控制显示前后 8 次按的键值,当有按键按下时,键盘值串行移入寄存器,利用一个模 8 计数器,使当前按键值在最末位显示,之前的按键值依次左移显示[9]。最终保证显示正确键值,在验证平台上观测到加密算法的码流,以此来验证加密算法的正确性。

2　应用实例

2.1　DES 算法实现

以传统的 DES 算法为例[10],验证该 FPGA 平台的实用性。DES 算法主要有以下接口:明文 datain [63:0] 及密钥 keyin [63:0];密文 dataout [63:0] 以及有效信号 dataout_en。其核心算法是以多轮的密钥变换轮函数和密钥加数据运算轮函数为特征,本实验采用了资源优先的硬件实现策略:即仅用硬件实现一套密钥变换和密钥加数据运算轮函数,通过多次调用这一硬件单元来完成一次 DES 加密运算。这虽然牺牲了芯片的部分性能,但却大幅减少了硬件资源的消耗。于是实验中又采用数据加密钥轮函数和密钥变换函数的同步流水线架构,减少相邻流

水线级间的逻辑复杂度,通过设置轮计数器对所进行的轮运算计数,控制数据选择器,从而实现轮函数复用,以补偿部分的性能损失,其硬件结构如图 3 所示。

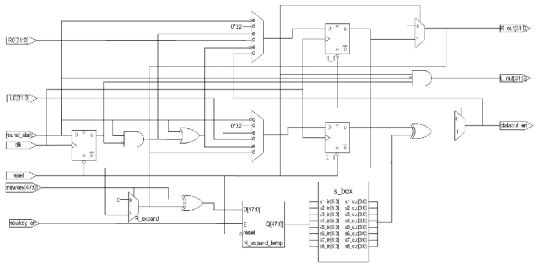

图 3　轮函数硬件结构逻辑电路图

2.2　仿真验证

本文算法采用 Verilog HDL 实现,并编写了测试激励,在 Modelsim 仿真环境中进行了 RTL 级功能仿真,当密钥流选择混沌加密,算法采用 DES 算法[12],输入明文为 636F6D7075746572 时,输出的密钥数据为 7365637572697479,与理论计算值完全吻合,具体波形如图 4 所示。

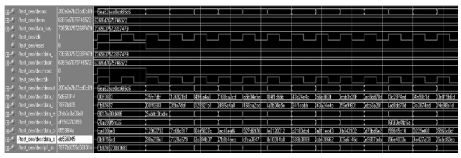

图 4　DES 算法仿真波形

仿真完成后,又采用 FPGA 专用综合工具 Synplify 对算法进行综合,最高工作频率可达 50 MHz。由于设计采用 16 级流水总线设计,所以最高数据编解码速率可达 3 Gbit·s^{-1}[13]。实验选取 Xilinx 公司的 Virtex7FPGA 芯片,采用 ISE 软件完成布局布线,并提取了网表和延时文件,进行了后仿真,实验结果完全符合时序要求[14]。最终,将本设计下载到 FPGA 平台,并将加密密文在平台上用 LED 显示出来,直观地验证加密算法的正确性。

3　结束语

提出了基于 FPGA 的加密芯片设计验证平台的快速原型的建立,将大幅提高设计验证的效率和质量,同时还可以提供用户早期的软件开发平台,加速复杂测试用例的仿真。FPGA 的加密原型验证流程是,快速将待验证加密算法映射到实际硬件上加以验证,提高加密算法验证的效率和可信度,使加密模块的开发可以领先于系统集成,从而缩短周期。实现这一思想的关键是在一定范围内建立普适的 FPGA 平台,使得验证人员容易地将一个新加密算法嵌到这个平台。这一平台的建立也将进一步促进新型加密算法的研究,促进加密芯片在通信、军事、网络、大数据、云计算等新兴领域的应用[15]。

参考文献

[1] 于海,樊晓桠,张盛兵. 32 位 RISC 微处理器 FPGA 验证平台设计与实现[J]. 计算机工程与应用,2007(5):110 – 112.

[2] 徐慧,王金海,王巍. 基于 FPGA 的 8051IP 核的设计与实现[J]. 计算机技术与发展,2009(4):42 – 45.

[3] 詹文法,陶芳泽,张溯,等. 系统芯片验证平台设计[J]. 微机发展,2005(11):74 – 76.

[4] 于治楼,姜凯,李峰. 基于 FPGA 的 SoC 验证平台的设计[J]. 信息技术与信息化,2008(5):96 – 98.

[5] 韩雪,郭文成. FPGA 的功耗概念与低功耗设计研究[J]. 单片机与嵌入式系统应用,2010(3):9 – 11.

[6] 帅仁俊,张齐. 基于 FPGA 的 LED 显示控制系统的设计和实现[J]. 微计算机信息,2009,26(3):133 – 135.

[7] 朱副成,陈跃. LED 矩阵连接控制技术[J]. 兵工自动化,2012(7):85 – 87.

[8] 于娟,唐瑞. 基于 89C52 单片机的 LED 显示器设计[J]. 科技与创新,2016(1):8 – 10.

[9] 周庆芳. 基于 FPGA 基础设计扫描数码显示器[J]. 科技展望,2016(8):183 – 185.

[10] 戈勇,李华,宁永成. 基于 FPGA 的 DES 加密算法实现[J]. 电子科技,2013,26(7):172 – 176.

[11] 谭会生. 基于 FPGA 的 DES 加密算法的高性能实现[J]. 电子工程与设计,2009(2):87 – 89.

[12] 蒋存波,孙朝华,杜婷婷,等. 基于 FPGA 的 DES 加密芯片的设计[J]. 计算机工程与应用,2008,44(16):83 – 86.

[13] 姚霁,刘建华,范九伦. 一种密钥可配置的 DES 加密算法的 FPGA 实现[J]. 电子技术应用,2009(7):145 – 148.

[14] 蒋昊,李哲英. 基于多种 EDA 工具的 FPGA 设计流程[J]. 微计算机信息,2007(32):201 – 203.

[15] 虞致国,魏敬和. 基于 FPGA 的 ARM SoC 原型验证平台设计[J]. 电子与封装,2007(5):25 – 28.