

一种基于 AHB 总线的 DES IP 核设计

柳沐璇¹, 张树丹^{1,2}, 唐彩彬¹

(1 江南大学, 江苏 无锡 214122; 2 中国电子科技集团公司第 58 研究所, 江苏 无锡 214036)

摘 要: 设计了一款带有通用 AHB 总线从机接口的 DES IP 核, 能在 500 MHz 频率的总线下很好地工作, DES 模式下加、解密转换速率可达到 1.6 Gb/s, 3DES 模式下加、解密转换速率可达到 615 Mb/s. 用 VCS 软件仿真并用 DC 软件综合后结果均符合设计要求.

关键词: AHB 总线; DES 算法; IP 核

中图分类号: TN402

文献标识码: A

文章编号: 1000-7180(2014)10-0069-03

A Design of DES IP Core Based on AHB Bus

LIU Mu-xuan¹, ZHANG Shu-dan^{1,2}, TANG Cai-bin¹

(1 Jiangnan University, Wuxi 214122 China;

2 The 58th Research Institute of China Electronics Technology Group Corporation, Wuxi 214036 China)

Abstract: This paper presents a DES IP core equipped with a AHB Slave Interface. It works perfectly with a bus frequency of 500 MHz. The maximum sustained conversion rate for DES is around 1.6 Gb/s. And it is around 615 Mb/s for 3DES. After simulating by VCS and synthesizing by DC, results show that it fulfills the design require.

Key words: AHB bus; DES algorithm; IP core

1 引言

随着时代的信息化, 数据传送的安全性问题愈加得到人们的重视, 许多数据加密算法应运而生, 其中, DES(Data Encryption Standard)算法和加强型 3DES 算法目前应用特别广泛. 早在 1975 年, IBM 公司就已成功研究并公开 DES 算法, 随后被美国国家标准局和美国国家标准协会承认, 发展至今已成为工业界的标准密码算法^[1].

用软件实现 DES、3DES 算法效率很低^[2], 而现今 DES 算法的硬件实现多数采用纯粹算法的硬件直译, 不具备通用的总线接口, 无法良好地应用于 SOC 系统中. 现阶段使用较为广泛的 AHB(Advanced High-performance Bus)总线, 其接口已能与互连功能分离, 成为一种带有接口模块的互连体系^[3]. 所以, 本文选用 AHB 总线从机接口作为模块的接口, 使其能方便的运用到 SOC 系统中来完成

加、解密工作.

2 算法简介

DES 算法对 64 比特的数据进行加密和解密, 所用密钥也是 64 比特, 但由于其中包含了 8 个比特的奇偶校验位, 因而实际的密钥长度是 56 比特^[4].

以加密为例, DES 算法的流程如图 1 所示^[5]. 首先, 64 位明文经过初始序列 IP 变换后形成新的 64 位数据, 然后分成左边 32 位数据 L_0 和右边 32 位数据 R_0 , 然后将他们放入一个由 16 次反复运算组成的“螺旋梯子”中. 以第一次运算为例, 右边部分 R_0 通过一个函数 F_D , 和密钥选择函数 F_{K0} 选择出的子密钥 K_0 相作用后, 与左边部分 L_0 进行异或逻辑, 得到的结果成为新的右边部分 R_1 , 而原来的右边部分 R_0 成为新的左边部分 L_1 . 以此类推, 16 轮后形成新的 R_{16} 和 L_{16} . 最后由 R_{16} 和 L_{16} 组成的 64 位数据经过与初始序列完全相反的最终序列 IP^{-1} 变换后

收稿日期: 2013-11-26; 修回日期: 2014-01-12

基金项目: 江苏省“三三三”工程科研项目(BRA2011115)

形成加密后的密文。

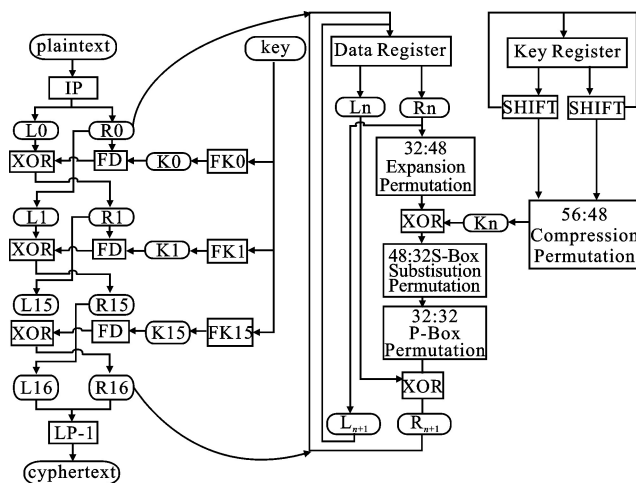


图 1 DES 加密算法流程图

忽略初始序列和最终序列的变换,中间阶段的每一轮运算都采用流水线形式,在一个时钟周期内完成,所以 DES 加密转换过程总共需要 16 个时钟周期。每一轮运算的具体步骤如图 1 右边部分所示。从图上可以看出,由数据寄存器分出来的右边 32 位数据 R_n 先要经过一个扩展序列,由 32 位变成 48 位,同时,由密钥寄存器经过左移一位或两位选择出的 56 位子密钥,要经过一个压缩序列变成 48 位的密钥 K_n ,然后与扩展后的 R_n 进行异或逻辑。异或逻辑后得到的 48 位数据通过 S-Box 替换序列由 48 位变成 32 位,再通过 P-Box 序列后与 L_n 异或,最后的结果成为新的 R_{n+1} ,而此时,原始的 R_n 成为新的 L_{n+1} 。

解密过程与图 1 所示的完全一样,唯一需要替换的是,子密钥选择时,循环左移的部分换成循环右移,这样做的结果能得到 16 个相反顺序的子密钥,即第一个右边部分 R_0 被扩展后是与最后一个子密钥 K_{15} 相异或的。

由于考虑到模块面积的优化,使可读性和可移植性更强,加强型 3DES 采用 3 次调用 DES 运算模块来实现,所以整个运算过程需要 48 个时钟周期。图 2 所示为 3DES 算法的加、解密过程。以 3DES 加

密运算为例,明文先用密钥 K_1 进行加密,然后用密钥 K_2 进行解密,再用密钥 K_3 进行加密后得到密文。需注意,若三个密钥均不相同,那么经过 3DES 运算后,密文的安全性得到了更大的保障,但是,若两个密钥完全相同(如 $K_1 = K_2$),那么两个 DES 运算将相互抵消,得到的结果与普通的 DES 加密相同。3DES 解密算法与加密算法相反。

3 模块设计

DES IP 核总体框图如图 3 所示,总共分为四个功能块。其中,AHB_BIU 是 AHB 总线从机接口电路,可以将从 AHB 总线主机发出的信号转化为 DES 模块所需的信号,实现该模块与 AHB 总线间的良好兼容性;REG 是寄存器电路,用来存放数据寄存器和密钥寄存器的值等;DES_ALU 是加、解密算法电路,包括 DES 算法的各个具体步骤的实现;CTRL 是整个模块的控制中心,负责控制整个模块的运行,并存放控制寄存器的值。由于只支持 32 位字长的数据传输,所以 HSIZE、HBURST 和 HPROT 信号都没有出现在 AHB 总线接口。输出端口 DOEI、DECI 和 DDCI 分别为弱密钥检测中断、加密完成中断和解密完成中断,将在后面 DCCSR 寄存器功能介绍中详细说明。

DES 模块寄存器地址映射如表 1 所示,总共有 4 个 64 位的存放转换数据的寄存器(其中包括一个数据寄存器和三个密钥寄存器),和 1 个 32 位的控制状态寄存器。剩下的寄存器地址是保留的,无法对其进行写操作,若是进行读操作则返回 0x00。

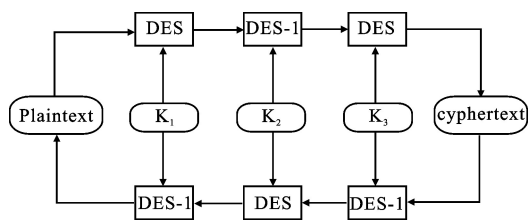


图 2 3DES 算法流程

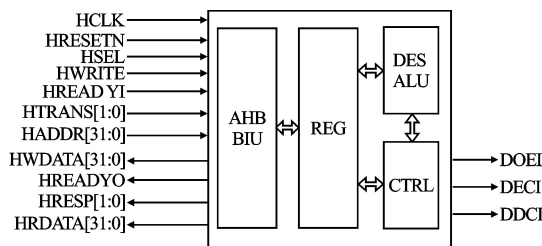


图3 总体框图

表1 DES模块寄存器地址映射

地址	寄存器	描述
0x00	DCDLR	数据寄存器低位(DCDR[31:0])
0x04	DCDUR	数据寄存器高位(DCDR[63:32])
0x08	DCK1LR	密钥寄存器1低位(DCK1R[31:0])
0x0C	DCK1UR	密钥寄存器1高位(DCK1R[63:32])
0x10	DCK2LR	密钥寄存器2低位(DCK2R[31:0])
0x14	DCK2UR	密钥寄存器2高位(DCK2R[63:32])
0x18	DCK3LR	密钥寄存器3低位(DCK3R[31:0])
0x1C	DCK3UR	密钥寄存器3高位(DCK3R[63:32])
0x20	DCCSR	控制状态寄存器
0x24-0xFF	—	保留

64 位数据寄存器用来存放等待加、解密的数据,3 个 64 位密钥寄存器用来存放密钥。DES 模式中,只需将密钥写入密钥寄存器 1 中;3DES 模式中,需要依次向密钥寄存器 1、2、3 中写入相应密钥。32 位的控制状态寄存器比较特殊,表 2 中详细列出了 DCCSR 每位对应的功能。

表2 DCCSR 控制状态寄存器

位数	名称	读/写	功能描述
31:28	—	只读	默认读出为 0000
27	WE	只读	弱密钥错误(1 检测到弱密钥错误 0 未检测到)
26	PE	只读	奇偶校验错误(1 检测到奇偶校验错误 0 未检测到)
25	DC	只读	解密完成(1 检测到解密完成 0 未检测到)
24	EC	只读	加密完成(1 检测到加密完成 0 未检测到)
23:16	CS	只读	高四位为状态(DES 或 3DES 加密或解密) 低四位为转换步骤计数
15:12	—	只读	默认读出为 0000
11	WI	读写	弱密钥错误中断使能(1 使能产生中断 0 不使能)
10	PI	读写	奇偶校验错误中断使能(1 使能产生中断 0 不使能)
9	DI	读写	解密完成中断使能(1 使能产生中断 0 不使能)
8	EI	读写	加密完成中断使能(1 使能产生中断 0 不使能)
7	TC	可写	中断转换,默认读出为 0(1 立刻取消 DES 转换 0 无影响)
6:5	RR	读写	读取忙回应(11 保留 10 冻结总线 01 产生总线错误 00 返回垃圾数据)
4	WR	读写	写入忙回应(1 写入正忙时产生总线错误 0 忽略写入操作)
3	CD	读写	转换方向(1 数据解密 0 数据加密)
2	CT	读写	转换类型(1 选择 3DES 算法 0 选择 DES 算法)
1	FC	可写	强制转换,默认读出为 0(1 立刻开始 DES 转换 0 无影响)
0	AC	读写	自动开始转换(1 等待 FC 位 0 新的转换数据写入后立刻开始转换)

4 功能验证和综合

本文设计的基于 AHB 总线的 DES IP 核,可以选用普通 DES 模式或加强型 3DES 模式对 64 位数据进行加、解密,转换开始方式可以是自动开始或者强制开始,检测到弱密钥时,系统会产生错误中断,避免错误加密过程。

综合工具为 Synopsys 公司的 DC 软件,时钟为 500 MHz,并选用 TSMC 公司 65 nm 的典型库,电压为 0.95 V,温度为 85℃,综合结果如表 3 所示。

从表 3 可知,时间冗余均为正数,符合要求,设计的 IP 核能在 500 MHz 频率下正常运行,所以 DES 模式下加、解密转换速率可达到 1.6 Gb/s,3DES 模式下加、解密转换速率可达到 615 Mb/s。

表3 综合结果

名称	综合结果
时间冗余/ns	Set up time 0.28
	Hold time 0.09
面积/ μm^2	Combinational area 6 639
	Noncombinational area 4 650
	Total cell area 11 289
功率/ μW	Leak power 131
	Total power 183

5 结束语

本文设计的 DES IP 核,带有 AHB 总线从机接口,与 AHB 总线兼容性良好,并且 DES 模式下加、解密转换速率可达到 1.6 Gb/s,3DES 模式下加、解密转换速率可达到 615 Mb/s。

参考文献:

- [1] 汪翼,沈海斌,何乐年,等. DES 算法的高速流水线实现[J]. 微电子学与计算机,2003,20(8):158-160.
- [2] 邵金祥,何志敏. 基于 FPGA 的 3DES 加密算法高速实现[J]. 现代电子技术,2004,27(21):55-57.
- [3] ARM Company. AMBA™ specification rev 2.0 [EB/OL]. [2014-04-12]. <http://www.arm.com>.
- [4] 孙凌宇,冷明. VHDL 语言在描述 DES 加密机中的应用[J]. 微电子学与计算机,2002,19(12):43-45.
- [5] 张丽娜,陈建华,张家宏,等. 基于 ASIC 的有效 DES/3DES 流水线设计[J]. 计算机工程,2007,33(2):225-22.

作者简介:

柳沐璇 女,(1990—),硕士研究生.研究方向为集成电路设计。
 张树丹 男,(1956—),教授级高工.研究方向为集成电路设计。
 唐彩彬 男,(1990—),硕士研究生.研究方向为集成电路设计。