DES算法的S盒的设计优化

焦冬莉
(中北大学分校，山西省太原市 030008)

【摘　要】 DES(数据加密标准)算法被广泛应用于软件加密和硬件加密。S盒是DES算法中的一个关键环节，它的设计好坏直接影响DES的加密性能。VHDL(甚高速集成电路硬件描述语言)是借助EDA(电子设计自动化)工具进行硬件设计的基本描述语言。文中结合VHDL的特点，对使用VHDL设计S盒进行了一些分析，综合速度、资源利用率等提出了最优方案。

关键词：DES，S盒，加密，VHDL，时间分析，优化设计
中图分类号：TP309

0 引　言

网络的普及与信息的公开化使得具有知识产权的信息保护越来越引起人们的关注，新兴的加密技术成为保护信息的基本手段，各种软件和硬件加密技术在信息流通领域发挥着重要的作用。

硬件加密从速度、可用性、成本等各方面考虑优越于软件加密，基于各种集成技术的加密算法实现成为加密技术的重要研究课题。DES(Data Encryption Standard，数据加密标准)算法是ANSI(美国国家标准学会)于1981年正式批准的加密标准。自公开以来受到过各种有针对性的攻击，经历了长期的考验，并在此基础上衍生了新的算法，如3DES等，具有很强的应用性。

在DES算法中起混乱作用的其他运算都是线性的，便于分析和破解，只有S盒是非线性的，所以S盒是DES算法中的一个关键步骤，它为DES的安全性提供了保障[1]。硬件实现时，S盒设计的好坏会直接影响算法整体的工作性能。

1 DES算法的S盒

S盒是DES算法的黑匣子，用于实现复杂的非线性运算，其输入为48位，输出为32位。在运算中，48位的输入被分成8个6位的分组，每一分组对应1个S盒作替代操作，输出结果为4位，8个4位分组合在一起形成32位的输出。每个S盒是一个4行、16列的表，S盒的6位输入的第1位和第6位组合构成一个2位的数，从0到3对应表中的各行，第2位到第5位组合构成一个4位的数，从0到15对应表中的各列，S盒的输出即为盒中的4位数的项，对应输入的6位数。例如：在第1个盒中，若输入110100，则对应盒中的行数为10，即第3行，对应的列为1010，即第10列，输出结果为1001。

2 S盒的VHDL设计

2.1 基本设计思路

S盒的VHDL(甚高速集成电路硬件描述语言)设计，通常有两种思路：一是调用开发工具中的库函数构造ROM；二是直接使用VHDL语句进行行为描述。

第1种方法要结合器件的内部结构，对于小容量的ROM，可以采用数组描述或者when-else语句来实现，但大容量的ROM应采用元件例化的方式来实现。而在VHDL设计中，库函数、子程序的调用以及例化时元件的调用，使用间接变量，均是影响速度的主要因素。因此，从系统处理速度的角度处出发，使用VHDL语句直接进行电路的行为描述更有利于加密速度的提高。

适合进行S盒设计的VHDL语句有两个：with-select语句和case语句。使用with-select语句设计，可以对照S盒直接进行替换的行为描述，不需要做任何整理；若使用双重case语句嵌套，则外层对应S盒的第1位和第6位，内层对应第2位到第5位，形成一个6输入、4输出的查找表，或者将S盒的4位输出事先进行手工卡诺图化简，以减少每次查找的输出变量。

2.2 设计结果与分析

以S盒中的第1个S盒为例，使用不同的方法时性能指标有很大的差异。

2.2.1 使用with-select语句

with-select语句[2]是并行赋值语句，由于S盒的行为比较单一，所以可用它来实现。

使用with-select语句实现的VHDL源程序主要结构如下：

收稿日期：2005-07-06；修回日期：2005-10-14。

```
...
WITH S1IN SELECT
  S1 OU < = "1110" WHEN "000000", "0000" WHEN
    "000001","0100" WHEN "000010"
  ...
    "0 000" WHEN "111110","1101" WHEN OTHERS;
```

选定器件 EPF10K30ETC144-1 编译仿真后,得到时间分析结果如表1所示。仿真波形如图1所示。

表1　使用 with-select 语句的时间分析结果　　ns

	S10U0	S10U1	S10U2	S10U3
S1IN0	10.8/27.3	10.3/23.1	10.5/24.9	10.7/25.3
S1IN1	11.0/27.5	10.5/23.3	10.7/25.1	10.9/25.5
S1IN2	10.6/28.2	10.0/23.8	10.6/25.7	10.4/25.4
S1IN3	10.8/28.4	10.2/24.0	10.8/25.9	10.6/25.6
S1IN4	10.9/28.4	10.3/24.1	10.9/25.9	10.7/25.6
S1IN5	10.8/28.5	10.2/24.0	10.8/26.0	10.6/25.7

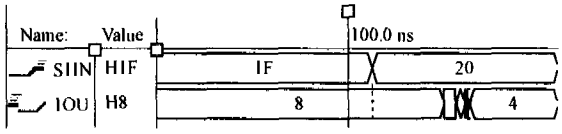

图1　使用 with-select 语句的仿真波形

2.2.2　使用双重 case 语句

case 语句属于顺序执行语句,一般用于进程中,结合S盒的特殊结构,使用 case 语句可以非常清晰地进行行为描述。

使用双重 case 语句实现的 VHDL 源程序结构如下:

```
...
S21 < = S2IN(0) & S2IN(5);S22 < = S2IN(1 TO 4);
process(s2in)
begin
CASE S21 IS
WHEN "00" = > CASE S22 IS
  when "0000" = > s2ou < = "1110"; when "0001" = > s2ou <
    = "0100";
  ...
  when others = > s2ou < = "0111";
  end case;
WHEN "01" = > CASE S22 IS
  ...
WHEN others = > CASE S22 IS
  ...
```

同样,选定器件 EPF10K30ETC144-1 编译仿真后,得到仿真波形同图1,时间分析结果如表2所示。

表2　使用双 case 语句设计的时间分析结果　　ns

	S20U0	S20U1	S20U2	S20U3
S2IN0	8.3/12.8	8.3/11.1	7.3/13.3	7.4/11.2
S2IN1	11.0/15.7	9.4/14.3	8.3/15.8	8.4/15.4
S2IN2	11.2/15.9	9.6/15.4	8.5/16.0	8.6/15.6
S2IN3	11.2/16.0	9.6/14.5	8.5/16.0	8.6/15.6
S2IN4	11.3/15.9	9.7/14.6	8.6/16.1	8.7/15.7
S2IN5	8.3/13.0	8.1/11.3	7.3/13.5	7.4/11.2

2.2.3　事先将输出用卡诺图化简后再使用双 case 语句设计

从传统的设计理念出发,可以先化简再进行描述。若先用卡诺图化简,再使用双 case 语句设计,则 VHDL 源程序结构基本不变,选用相同器件编译后得到的时间分析结果如表3所示。仿真波形如图2所示。

表3　使用卡诺图化简后的双 case 语句的时间分析结果　　ns

	S30U0	S30U1	S30U2	S30U3
S3IN0	7.5/16.3	9.9/10.7	8.9/11.1	10.1/10.9
S3IN1	10.3/19.6	11.2/20.5	11.4/19.7	10.4/19.7
S3IN2	10.4/19.5	11.3/20.3	11.4/19.8	10.5/19.6
S3IN3	10.3/19.6	11.2/20.5	11.4/19.7	10.4/19.7
S3IN4	10.1/19.7	11.0/20.6	11.2/19.5	10.2/19.8
S3IN5	7.6/16.5	10.0/10.9	9.0/11.3	10.3/11.1

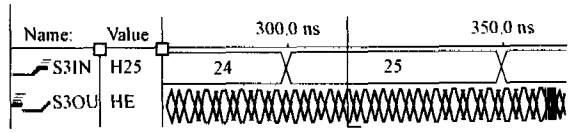

图2　使用卡诺图化简后的仿真波形

2.2.4　结果分析

由仿真结果来看,前两种语句方法均可以正确实现S盒的功能,双 case 语句的结构比 with-select 语句的结构复杂,但从时间分析的结果来看,使用双 case 语句的延时较其他两种方法要短,所以实现起来速度更快。先化简后描述的方法最不可取,仿真结果很不理想,且延时较长。比较结果也体现了硬件描述语言的特点。3种方法对资源的占用情况如表4所示。

表4　资源占用情况对比

使用的语句	LC/个	LC 利用率/(%)
with-select 语句	142	8
双 case 语句	63	3
先化简的双 case 语句	132	7

从表4所示数据可以看出:直接使用双 case 语句进行行为描述占用的资源最少,因此,从速度和资源利

用两方面综合考虑,直接使用双 case 语句进行行为描述的方法最可取。

3 S盒的设计优化

S盒毕竟只是 DES 算法的一部分,要实现整个 DES 算法,S 盒应采用顺序语句描述,即采用 case 语句。具体到 VHDL 语言中,中间使用变量和信号对硬件资源的应用是完全不同的,由于变量在器件中无连线,可以大大节约器件资源,为 DES 算法的改进提供可以扩展的空间。同样,下载到 EPF10K30ETC144-1,S 盒的仿真结果如图 3 所示。

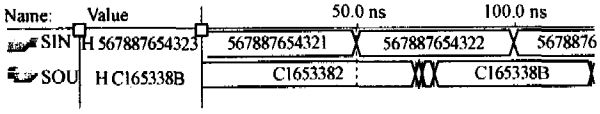

图3 S盒的仿真波形

最终,占用 LC 为 429 个,利用率为 24%。

4 总束语

当前,加密技术的发展速度很快,硬件加密更是加密工作者的研究目标,集成芯片的更新换代以及加密算法的不断更新和完善为加密技术的发展提供了保证。在保证安全性的同时,应尽量提高系统的处理速度及成品的高集成度。S 盒作为 DES 算法中起混乱作用的重要环节,其设计优劣直接影响整个加密系统的性能,所以,有必要对 S 盒的设计进行分析。

参 考 文 献

[1] Schneier B. 应用密码学:协议、算法与 C 源程序. 吴世忠,祝世雄,张文政,等译. 北京:机械工业出版社,2000

[2] 卢 毅,赖 杰,VHDL 与数字电路设计. 北京:科学出版社,2001

Optimum Design of S-box of DES Algorithm

Jiao Dongli

(The branch of Mid-north Univeristy, Taiyuan 030008, China)

【**Abstract**】 DES algorithm has been applied to the software and hardware encryption extensively. S-box is a key part of DES algorithm and the design of S-box directly influences the DES's function. VHDL is the basic description language that use EDA to carry out the hardware design. In this paper, a design using VHDL of S-box is analyzed in association of the characteristics of VHDL, and an optimum design was suggested in terms of speed, utilization rate etc.

Keywords: DES, S-box, encryption, VHDL, time analysis, optimum design

(上接第 49 页)

Design and Application of Multi-bit LED Serial Display Circuit

Ma Biao

(Liaoning Information Vocational and Technical College, Liaoyang 111000, China)

【**Abstract**】 The chip of 74HC595A has functions of serial input and parallel output, so we could design a circuit for multi-bit LED display by making use of this integrated circuit. This paper introduces 12 bit LED serial display circuit designed by making use of the chips. Then it illustrates the operation principle of the circuit in detail and presents the referenced program. Using 3 pins of the MCU only, the circuit saves the system resource compared with parallel display method. It has been applied to practical systems.

Keywords: serial display, 74HC595A, LED display