高速和资源节约型数据加密算法设计

贺刚　　赵红言

（空军工程大学　，陕西西安 710051）

来源：微计算机信息

摘要　介绍了 3DES 数据加密算法（DDA）的原理，针对利用 FPGA 硬件实现 3DES 算法，给出了一种可进化 IP 核的具体设计思想，采用可重构电路节省器件内部资源，并采用有限状态机设计技术从而实现数据高速安全传输。本设计是在 ALTERA 公司的 Quartus II 环境下实现的，并成功下载到支持电路部分重构的 Xilinx Virtex II 系列器件中的 XC2V1500 芯片中。

关键词　可进化 IP 核　3DES　FPGA　有限状态机

中图分类号：TP271+.5　　文献标识号：A

The design of DDA on adaptive IP core and FSM

HeGang　　zhao　hong-yan

（Airforce　Engineering University, xi’ an, Shaanxi　710051,China）

Abstract　This paper introduces the　theory of 3DES encrypt arithmetic, presents a detailed design idea of adaptive IP core Acording to using FPGA hardware to realize 3DES, adopt reconstituted circuit to save inner resource of chips, and adopt design method of finite-state machine(FSM),accordingly realize data transfer in a high speed and security way.This design　realized in Quartus II condition of ALTERA Corporation,and successfully download to XC2V1500 chip.

Keywords　adaptive IP core　3DES　FPGA　finite-state machine

一、引言

随着信息时代的到来，信息安全、数据传输快速在现代网络、军事通信等方面显得非常重要。因此对数据加密算法的改进很值得研究。传统的加密工作是通过加密软件实现的，此方法占用主机资源并且运算速度慢，安全性较差。采用硬件加密方式，是通过独立于主机系统外的硬件加密设备实现的，不占主机资源、速度快、安全性较高。DES（data encryption standard）算法是最为广泛使用的一种分组密码算法，已被证实是不安全的算法，在保持原有系统不做大的改动的前提下，研究 3DES 算法仍具有一定的实用价值。本文中利用 ALTERA 公司的 Quartus II 软件平台来开发，采用一种 FPGA 中可进化 IP 核设计思想和有限状态机设计方法，并成功下载到 Xilinx Virtex II 系列器件中的 XC2V1500 芯片中以实现 3DES 算法，以达到数据传输高效、安全、耗用资源少。

二、设计原理

1、3DES 数据加密算法原理

DES 算法中数据以 64 位分组进行加密，有效密钥长度为 56 位，在对明文进行初始置换 IP 后，执行 16 轮的迭代密码，最后经 IP 的逆变换得到密文。每一轮的运算包含扩展置换、S 盒代换、P 盒置换和两次异或运算，另外还有每一轮中还有一个子密钥。加密算法如图 1。3DES 以 DES 为基本模块，通过组合分组方法设计出分组加密算法。3DES 具体实现为：

加密过程为：C=EK3（DK2（EK1（P））

解密过程为：P=DK1（EK2（DK3（C））

其中 Ek()和 Dk()代表 DES 算法的加密和解密过程，K 代表 DES 算法的密钥，P 代表明文，C 代表密文。具体的加解密过程如图 2 所示。当三个密钥不同，本质上就相当于用一个长为 168 位的密钥进行加密。

2、 FPGA 中可进化 IP 核的一般结构及其实现

从进化硬件的经验可知，系统通常只有一部分是可进化的。同样，使用 IP 核构造的系统也是有些 IP 核是可进化的。可进化 IP 核在被下载并放在一个可重构器件中后，它们将自动地进化它们的内部电路。核由可重构电路构成（本文中可重构电路是指可进化 IP 核内的一个部分）。基因

单元不包含适应度计算，它只实现基因的操作、染色体存储和适应度存储。适应度的计算和环境由其它的核来提供。基因单元生成一些配置并上载到可重构电路中去，环境对这些配置进行评估,

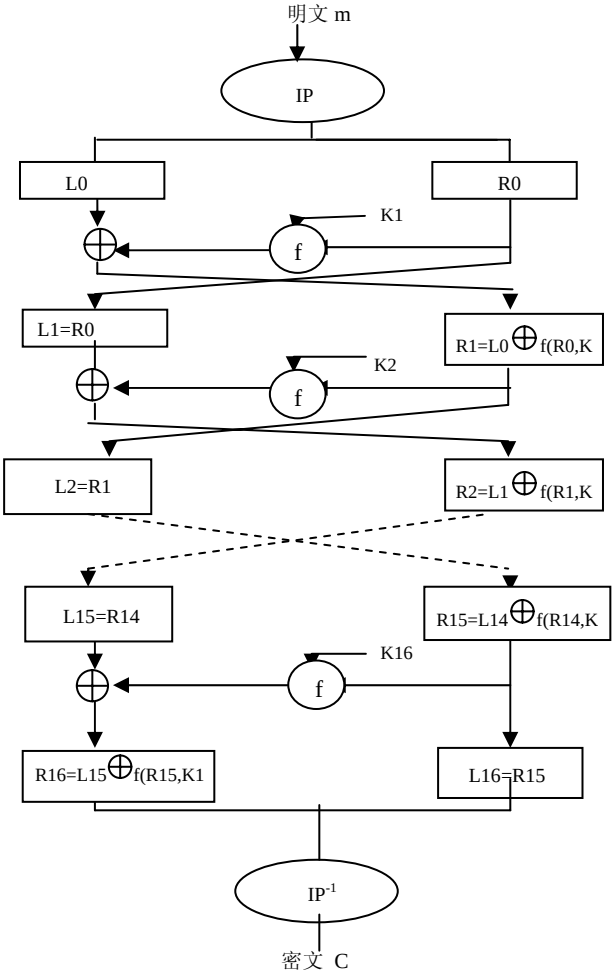

图 1 DES 加密算法

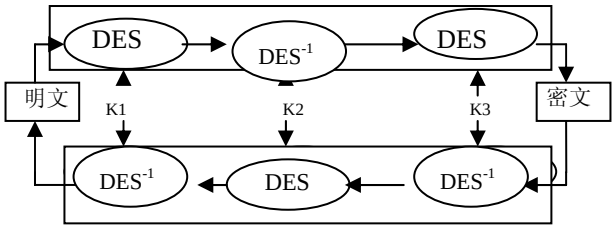

图 2　3DES 算法结构

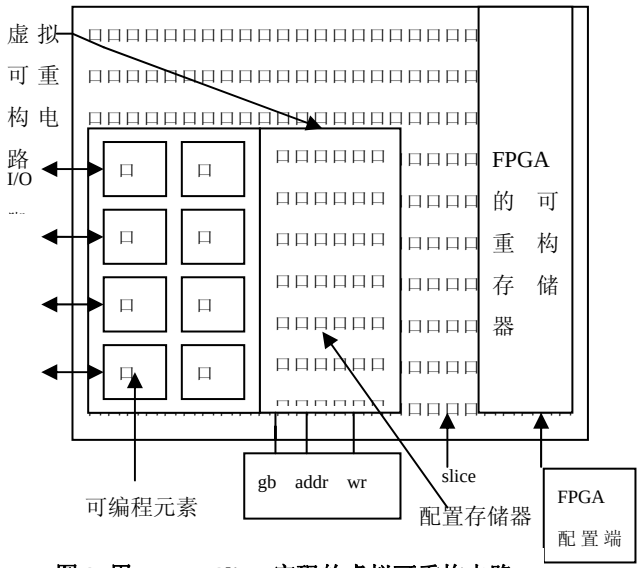

图 3 用 Vertex Slice 实现的虚拟可重构电路

并将适应度值发给 IP 核，可进化 IP 核实际上是一个由环境控制的电路生成器。

通常的 FPGA 只允许通过一个特殊的配置接口外部重构（如图 3）。为了在普通的 FPGA 器件实现可进化 IP 核，使之能在实际应用中发挥作用，所以采用硬件虚拟化这种设计技术。本设计中采用了虚拟可重构电路的技术来实现可进化硬件中的内部可重构电路。

3、有限状态机原理

状态机是组合逻辑和寄存器逻辑的特殊组合,其克服了纯硬件数字系统顺序方式控制不灵活的缺点，状态机的工作方式是根据控制信号按照预先设定的状态进行顺序运行的，状态机状态变换周期只有一个时钟周期，而且，由于在每一状态中，状态机可以完成许多并行的运算和控制操作，因此一般由状态机构成的硬件系统比 CPU 所能完成同样功能的软件系统的工作速度要高出 3~5 个数量级。

三、 3DES 算法的 FPGA 设计实现

1、 FPGA 器件选用

本文采用支持部分电路重构的 Xilinx Virtex II 系列器件中的 XC2V1500 以实现设计。所有的操作都通过 Virtex 重构端口和 Jbits 接口来完成。本设计中由八个可编程元素构成，由 Virtex 单元实现。Virtex 单元实现新的可编程元素阵列、新的布线电路和新的配置存储器。这些虚拟可编程元素称为可重配置功能块 CFB（Configurable Functional Blocks）。每个 CFB 对应一个配置位串，其中两个配置位决定了 CFB 的功能，其它四位定义了输入的连接信息。布线电路由多路器组成，它们由配置存储器中的位串控制。一个 Virtex 单元包含两个触发器，用于存储配置位串中的两位。配置存储器的所有位都连到多路器，多路器控制布线和 CFB 中功能的选择。

2、密钥生成器设计

密钥生成器的设计是独立于 DES 轮函数运算实现的，采用 3 级流水线来与轮函数中的流水线相平衡，单轮的实现如图 4。其中，3 级流水线由移位寄存器（SR）和 1 个触发器(FF)构成，在 SR 中完成两级流水线，在 FF 中实现第三级。XC2V1500 的 LUT 中的每个查找表 LUT 可以用来生成 1～16 个移位寄存器，而且在一个单独的可配置逻辑功能块 CFB 中连接 8 个移位寄存器来构成一个 128 位的移位寄存器。

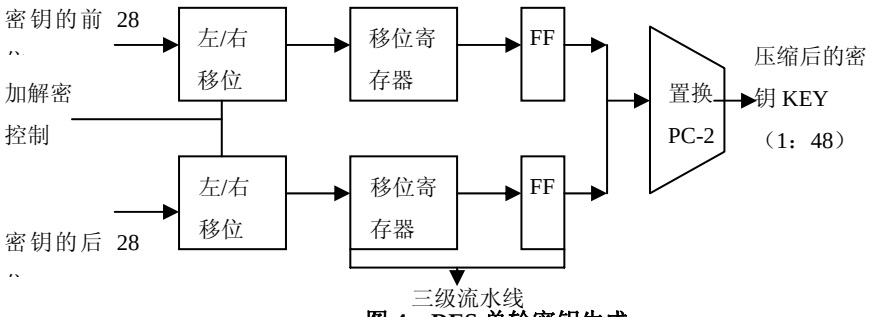

图 4 DES 单轮密钥生成

3、DES 模块设计

面积和速度两个指标是 FPGA 设计所追求的目标。在本设计中采用状态机和流水线相结合的技术，同时采用并行复制多个操作模块,利用器件 XC2V1500 的 IP 核的可进化特性使得在减少芯片资源消耗的情况下同时提高设计频率。

分析 DES 的算法结构可知中轮运算是相同的，只是输入子密钥不同，同时各轮的子密钥都可以通过密钥移位再经过一个压缩置换操作直接得到，所以将轮运算作为一个共享模块，重复进行该操作，其输入参数由状态机控制部分提供。只在空闲状态下将轮运算结果输出。

因数据端是 16 位，故每个状态机模块中进行四轮运算。流水线处理是高速设计中一个常用设计手段。它是在很长组合路径的中间点引入寄存器。DES 的 16 轮运算结构是相同的，即将前面的状态机模块作为流水线的一个单元，这样 DES 共有四个单元，串联起来形成四级流水线。将 DES 模块复制三份，就形成了 16 级流水线，如图 5，所不同的是流水线内部是状态机结构，所以每四

个时钟周期才会得到一组加解密结果。（其中加密每轮直接左移位数(1~16 轮):1、2、3、4、6、10、12、14、15、17、19、21、23、27、0）

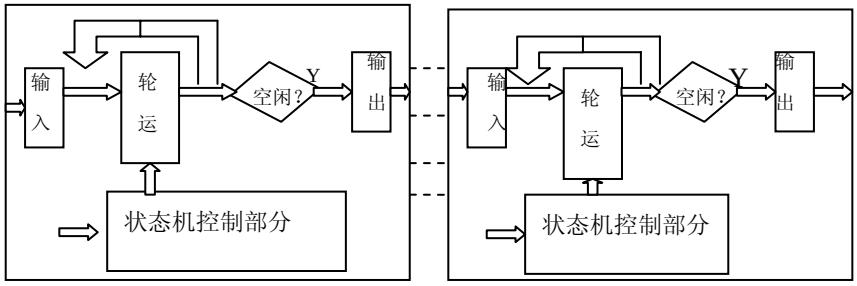

图 5 状态机及流水线结构

4、S 盒的设计和接口设计

在此算法中，S 盒代替是算法的关键所在。其它的运算都是线性的，易于分析和实现，而 S 盒是非线性的，因此 S 盒的设计和优化将直接影响整个系统的性能。DES 的 8 个 S 盒都是 6 输入、4 输出的结构，适合于用 ROM 来实现，用 VHDL 定义如下结构设计的 ROM：

```
Input : in std_logic_vector(5 downto 0);
Output : out std_logic_vector(3 downto 0);
Subtype s_word is std_logic_vector(3 downto 0);
Subtype sl_rangeij is integer range 0 to 63;
type s_type is array(sl_rangeij) of s_word;
constant s:s_type : =((“1110”),(“0100”),(“1101”),(“0001”)……);
function logic2int(din:std_logic_vector(5 downto 0)) return sl_rangeij
  output<=s(logic2int(input));
```

经综合，每个 S 盒只用了 24 个逻辑单元。

3DES 是 64 位分组大小的加密算法，数据线一般是 8 位、16 位或 32 位，为此增加了输入、输出接口，这部分接口完成的功能就是串并联转换和并串联转换。以 16 位输出接口为例，将加解密出来的数据在 valid 信号有效的情况下同时存入四个 16 位寄存器，再通过一个选择器依次将数据送出。输入接口只需一个 64 位可移位的寄存器，在第四个 16 位数据到来后才将这一组 64 位数据送给加密模块。这种结构非常容易用硬件描述语言实现。

5、总体结构

通过一个密钥控制模块为 3DES 提供三个 56 位的密钥以及加解密控制信号。密钥的输入是 28 位的，所产生的三个 56 位密钥并不是同一时间提供给 3DES 的，相互之间有 16 个时钟的延时，这样可以保证修改密钥后并不影响先前流水线的工作。再加上输入输出接口就构成了此设计的总体结构，如图 6 所示。加解密的流程是先输入六组 28 位的密钥，然后就可以发送需要加解密的数

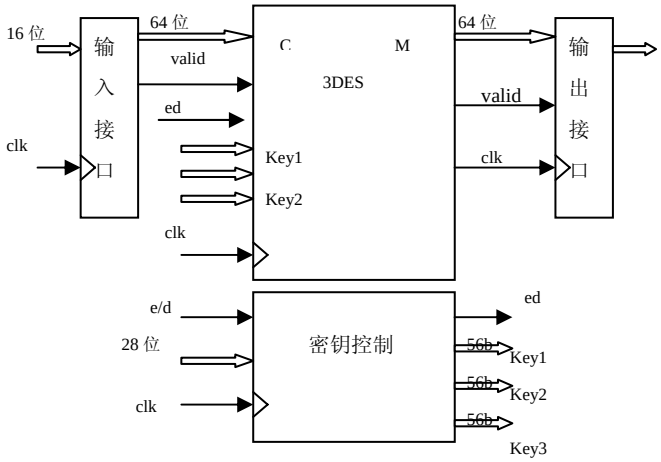

图 6 FPGA 实现的 3DES 总体结构图

据了，中间可以有间断，如果要更改密钥，也是先输入改后的密钥，再输入数据，可实时更改.

四、 结论

针对用硬件对数据加密具有安全性高的特点，本文所采用的在硬件设计中应用 FPGA 中 IP 核复用技术和状态机设计方法具有增加系统可靠性、提高数据传输速度、增加数据传输安全性及节约硬件资源等优点。采用此设计对现有的大量加密系统不需做大的改动，从而更有效地实现数据信息安全，同时能大量节约资金和时间。设计中共消耗逻辑单元 16350 个，在试验板上晶振为 25MHz 的情况下，大致评测出加密速度为 520Mb/s。

本论文的创新点：1、提出了一种可进化 IP 核的思想及其实现；2、首次利用这种可进化 IP 核思想和有限状态机设机相结合进行数据加密算法设计，更能有效地提高设计频率，节约系统资源；3、这样的设计思想为复杂系统的设计提供了借鉴。

参考文献:

[1] 马涛,陈娟,单洪. 单芯片可重构数字接收机的研究 微计算机信息，2006,8-2:151-153.

[2] 孙淑玲. 应用密码学.北京:清华大学出版社 2004.

[3] 潘松 黄继业 IDA 技术与 VHDL 北京: 清华大学出版社 2005

[4] EDA 先锋工作室 吴继华 王诚 ALTERA FPGA/CPLD 设计(高级篇) 北京:人民邮电出版社 2005

[5] Xilinx Corporation chip Scope Pro Software and Cores UserManual

作者简介：

贺刚（1979-），男（汉族），江西永新人，空军工程大学微电子学与固体电子学硕士研究生，主要研究方向为 EDA 环境与集成电路设计。

赵红言（1964-），男（汉族），陕西人，空军工程大学教授，主要研究方向为 EDA 环境与集成电路设计。

Biography:

HE Gang(1979-),male(the Han nationlity),from Yongxin,Jiangxi province,major in microelectronics and solide electronics,master,engaged in EDA condition and IC design.

ZHAO Hong-yan(1964-),male(the Han nationality),from shaanxi province, professor of Air Force Engineering University ,engaged in EDA contion and IC design.

附言： 联系人姓名：贺刚

通讯地址： 西安市空军工程大学理学院研究生大队一队

邮政编码： 710051

E-mail: hegang_1979@163.com