Available online at www.sciencedirect.com

ScienceDirect

AASRI Procedia 5 (2013) 209 – 213

AASRI Procedia

www.elsevier.com/locate/procedia

2013 AASRI Conference on Parallel and Distributed Computing Systems

Implementation of DES Encryption Arithmetic based on FPGA

Cai-hong Liu[a]*, Jin-shui Ji[a], Zi-long Liu[a]

[a]*Northwest University for nationalities*
Lanzhou, Gansu, China

Abstract

It is very necessary for embedded applications to protect important data. A realization of the data Encryption Standard algorithm based on FPGA is presented in this paper. The implementations of the DES (data encryption standard) algorithm based on hardware is a low cost , flexible and efficient encryption solutions. This paper uses a method of iteration of the loop, with key size of 128 bits and realized by lookup table based on S-box. The simulation waveform showed that result in FPGA meet the requirements.

Keywords: FPGA, DES, Arithmetic, VHDL;

1. Introduction

Data encryption standard uses a key to custom conversion, so the decryption can be performed. They know the especially key used to encrypt. DES (data encryption standard) is A typical block cipher, it takes a plaintext bit fixed length string and changes it by much complicated operations into cipher text bit string. This string is same length. In the case of data encryption standard, the size of block is sixty-four bits. The key apparently composed of sixty-four bits; but, 8 bits are used uniquely for checking parity, and are then discarded, only fifty-six of those are effectively used by the algorithm. Therefore the effective key length is fifty-six bits.

* Corresponding author. Tel.: 1-399-318-9468;
E-mail address: cindyliu888@qq.com.

doi:10.1016/j.aasri.2013.10.080

As other block ciphers, Data encryption standard is not a safe way of encryption. It must be instead by a mode of operation. This key is usually transmitted or stored as eight bytes. 1 bit in each eight bit of the key may be used for error check in key distribution, generation, and storage. Bits eight, sixteen,..., sixty-four are used in ensuring that every bit is odd parity.

2. Features of FPGA

FPGA is a semiconductor device .It can be programmed after production. Rather than be limited to any concerted hardware function. A FPGA allows your program products alterable. So it is called "field-programmable". FPGA can achieve any logical function .It could be perform by ASIC. But it can update the functionality after shipping overmatch many applications. Today's FPGAs and previous generation FPGA compared different. Specifically, an FPGA contains programmable logic components called LEs . A hierarchy of reconfigurable interconnects that allow the LEs to be physically related as well. and can configure LEs to perform complicated combinational functions, or only simple logic gates such as AND OR. most FPGA, the logic blocks also contain memory elements, which may be simple flip flops or more complete blocks of memory. As FPGA continue to include, the device have changed more integrated. Hard IP blocks built into the FPGA fabric let the product have difference. Newer FPGA families are being produced with hard embedded processors, changing the devices into SOC.

3. Principle of the DES

The combination of substitutions and permutations is called a product cipher. The arithmetic includes implement substitutions , combinations and permutations between key and text to be encrypted, when ensure the operation can be implemented in all directions. The principal part of the arithmetic are as below: Part of the text into sixty-four bit blocks; permutation of blocks; divide the blocks into two parts: right and left; substitution and Permutation step will be repeated sixteen times; recombining of the right and left parts and then reverse permutation. as shown in Figure 1.

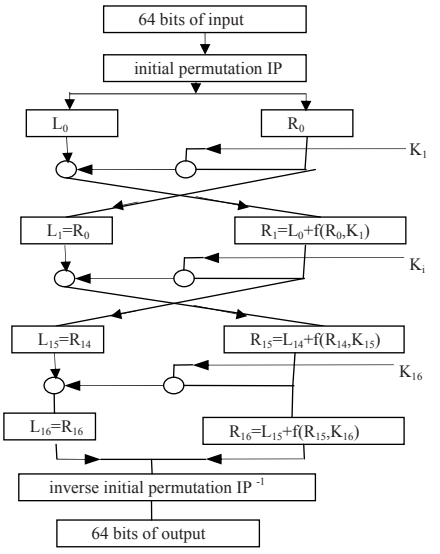

Fig. 1. DES encryption algorithm

4. Implementation of DES Algorithm Using VHDL

A flow of representative design includes an implementation which must be verified at many stages in the conversion to final hardware. The design stage includes selecting an appropriated section of the project between software and hardware, then partitioning of the software and hardware constituents based upon the suitability of realization in various tools and with different languages. The internal operation in each iteration of the DES algorithm can be realized by combinational logic. The system control part should be controlled by the iterative times. The overall diagram of the DES algorithm is shown in Figure 2.

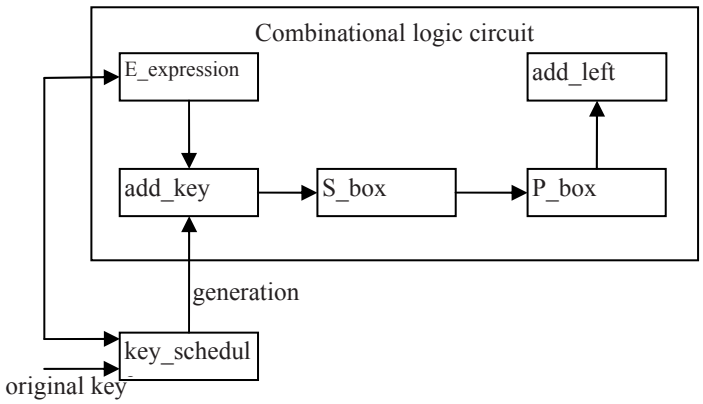

Fig.2. overall diagram of DES

The logic operation of iteration is accomplished in the combinational logic circuit. The combinational logic circuit consists of the following modules: Extended operation, The encryption algorithm, The compression arithmetic, Replacement operation and Exclusive-OR. The management and control of the iterative process is accomplished in the sequential logic circuit. The sequential circuits is described as state machine. It is shown in Figure 3.

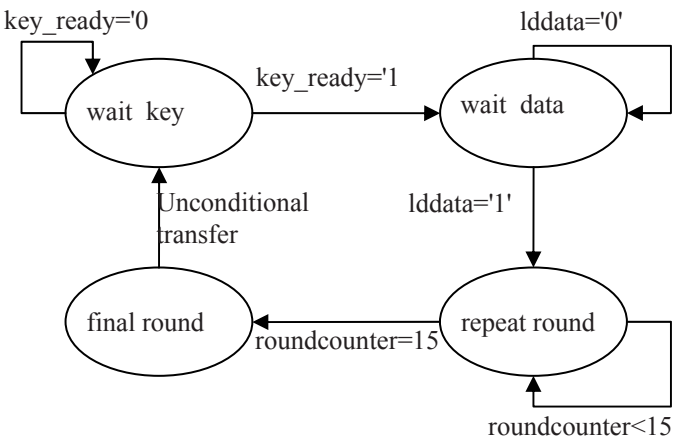

Fig.3. flow of state

It is very difficult for the designed circuit to use illustrative diagram for large design with hundreds of basic gates. Hardware description The language of hardware description supply standard text based expressions of the behavior and framework of circuit. So hardware description languages are preferred way to design logic in FPGA. VHDL is a language that was designed to explain the behavior of FPGA ,an application-specific circuits of systems in the design of electricity. The function of electronic component is described by VHDL in many areas. In order to increase the precise of electrical circuit, VHDL simulation model is created. the foundation for building larger circuits is consist of Combination with schematics, system level descriptions and the simulation model.

Some of design:

```
stim_proc:process
 reset <= '1';
 wait for 30 ns;
 reset <= '0';
 wait for 20 ns;
 ldkey <= '1';
 key_in <= x"FFFFFFFFFFFFFFFF";
 wait for 20 ns;
 lddata <= '1';
 data_in <= x"7359B2163E4EDC58";
 wait;
 end process;
```

5. Conclusion

When the completion of the design, in order to check the correctness of the design, the first thing is simulation,and then program the result in the FPGA chip on the board. it is very necessary to simulate it in order to ensure its correctness. The software named Quartus II can be used to simulate the behavior of design. The result of simulator is showed by the oscillogram .

This paper show that technique of one-round sub-key pre computation results in a faster design and generate sub-keys for encryption and decryption an no performance penalty. All designs are implemented on FPGA.

Acknowledgements

The work is supported by Key Program of Research Foundation For Young scholars under Grant No. zyz2012080. The work is supported by School Foundation of Research For Young scholars under Grant No.X2010-23 XBMU-2010-BD-140.

Corresponding Author

The contact of corresponding author must include: Cai-hong Liu, cindyliu888@qq.com, 13993189468

References

[1]McLoone, Máire. A FPGA high performance implementation of DES. 2000 IEEE ;374-383.
[2] Liu Cai-hong, Jin-shui Ji, and Xiu-ping Chen. Control Module for Stepper Motor Based on FPGA, 2010 International Conference on E-Product E-Service and E-Entertainment, 2010
[3] Xiu-ping Chen . Design of control module for ADC based on FPGA, 2011 IEEE International Conference on Computer Science and Automation Engineering, 2011.