Design and Implementation of Reconfigurable Encryption and Decryption System Based on SOPC

Qingfang Zhou
School of Physics And Electronic Engineering
Qujing Normal University
Qujing, Yunnan, China
739837379@qq.com

Ying Yuan
School of Information Science and Engineering,
Yunnan University
Kunming, Yunnan, China
693666225@qq.com

Qian Huang
School of Information Science and Engineering,
Yunnan University
Kunming, Yunnan, China
501208684@qq.com

Jun Yang*
School of Information Science and Engineering,
Yunnan University
Kunming, Yunnan, China
junyang@ynu.edu.cn

***Abstract*—The system is based on DES/3DES，AES cipher algorithm as the research object.According to the characteristics of the algorithm, designs a configuration mode which can share resource in space and configurate algorithm in time. Then it uses hardware description language Verilog HDL to realize and optimize the design，and completes a custom reconfigurable DES/3DES/AES encryption/decryption IP core. By SOPC technology, the IP core, Nios II processor, network controller and other function. The design hardware structureis simple, flexibility, security, which can be widely used in the field of informationsecurity.**

Keywords- AES; DES; 3DES; SOPC

I. INTRODUCTION

At present, the most widely used crypto chip is implemented by the ASIC, although the arithmetic speed of the chip is fast,its core components is fixed and can only achieve one cryptographic algorithm. Once be breaken, the system will be faced a great threat, and it difficult to meet the multi-level security demand of different users at the same time, In recent years, with the advent of FPGA reconfigurable logic device and the development of reconfigurable computing technology, many research institutions dedicated to research reconfigurable cryptographic chip. The reconfigurable crypto chip use reconfigurable computing technology, adopt programmable hardware modules, use reusable hardware resources properly, and based on the requirement, it can flexible change the hardware configuration and structure for different cryptographic algorithms[1-3]. The reconfigurable cryptographic chip compromises software and hardware, Not ony it can ensure the performance of the system, also can enhance the flexibility of the system. And design the hardware system as a Software.

In this paper, on the basis of the structural characteristics of reconfigurable computing technology and several kinds of block cipher algorithm, we designed a reconfigurable encrypting and decrypting IP core which based on DES/3DES/AES cryptographic algorithm, and combined the characteristics of SOPC technology which based on the NiosII, to realized a reconfigurable SOPC encrypting and decrypting processing system.

II. THE ALGORITHM

A. The DES/3DES/AES Algorithm

It needs 16 Iterations to Complete a DES encryption and decryption, SO it needs 48 Iterations to Complete a 3DES encryption and decryption[4]. Because the every iterative input is the previous iterative output,it does not meet the condition that two adjacent statement S1, S2 should execute concurrently which put forward by Bernstein:

$$W(S1) \cap R(S2) = \phi \quad (2)$$

Therefore, The 3DES algorithm needs 48 Iterations at least. If each iteration need a clock cycle, the 3DES algorithm need 48 clock cycles. By the observation of DES algorithm, we remove the module which realize $f(R^{i-1},K^i)$ function, and design a concise hardware structure of 3 DES encryption and decryption system by Schedule this module. Set m ={ 1,2 ,3,…,48 },n = { 0, 16, 32 }, the mathematical formula is as follows:

$$L_i^{'} = IP(x),\ R_i^{'} = IP(x),\ i \in n \quad (3)$$

$$L_i = L_i^{'},\quad R_i = R_i^{'},\ i \in n \quad (4)$$

$$L_i = R_{i-1},\ i \in m \quad (5)$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_m),\ i \in m \quad (6)$$

$$x = IP^{-1}(L^i, R^i),\ i \in n \quad (7)$$

The new function IP (x), IP^{-1} (L_i, R_i) each complete initial displacement and inverse initial displacement function of DES algorithm, its equation priority from high to low, Namely the whole 3DES algorithm is an iterative process can be expressed as follows formula (3) to formula (7), and the whole 3 DES algorithm needs to poll 48 times.

B. The AES algorithm

The AES algorithm include encryption/solution algorithm and the key expansion algorithm [3]. Encryption process includes Subbyte, ShiftRow[5], MixColumn and AddRoundKey, after Nr iteration, of which final round not do MixColumn. Decryption process is similar to the encryption process, all aspects of use the inverse transformation. Encryption and decryption algorithms used in the same sub-key, each round require the participation of an extended key which is the same length as input packets[6-8], but the order is opposite. AES encryption / decryption process is shown in Fig.1

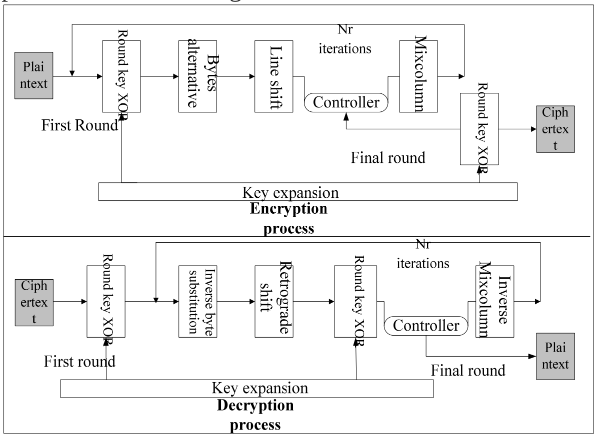

Fig.1 AES encryption / decryption process

III. System Design

The system structure diagram as shown in Fig.2.

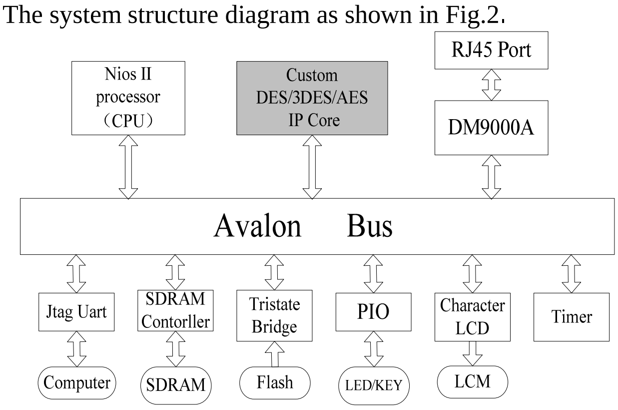

Fig.2 System Structure Diagram

A. The design of DES/3DES/AES IP core

IP-core is composed of data input module, control module,keys generation module and reconfigurable operation module. It is shown in Fig.3. First, initializing the system, then inputting the operational data which is included plaintext data, keys and control signal, the control module changes the relevant inner sturcture circuit for conforming process unit of the selected algorithm[9], and the keys generation module generates the subkey for a series of operations, then transferring the plaintext needed to process to the data process unit to implement the relevant encryption/decryption operation, last, outputing the ciphertext to implement the operation.

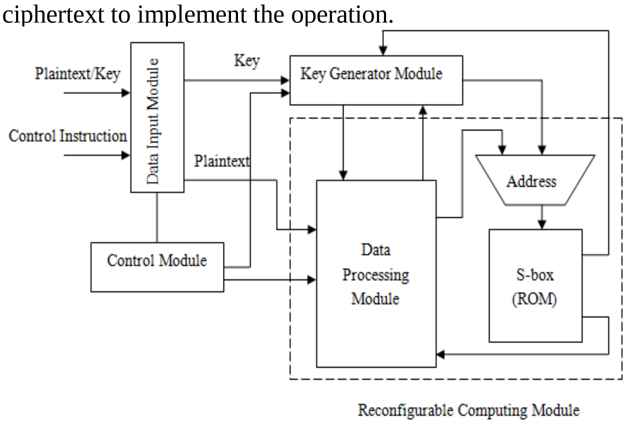

Fig.3 IP Core hardware structure

B. Reconfigurable Computing Module

Reconfigurable arithmetic module is the key module of the IP core. The data processing unit is the core unit of the system structure. The module includes a non-reconstructed unit ALU and the reconfigurable unit RPU, as shown in Figure 4. Reconfigurable arithmetic module complete the data processing of encryption/decryption process, e.g. DES/3DE XOR and alternative operation[10], the row shift transform of AES, column mixing transform, byte replaces the transform and so on.

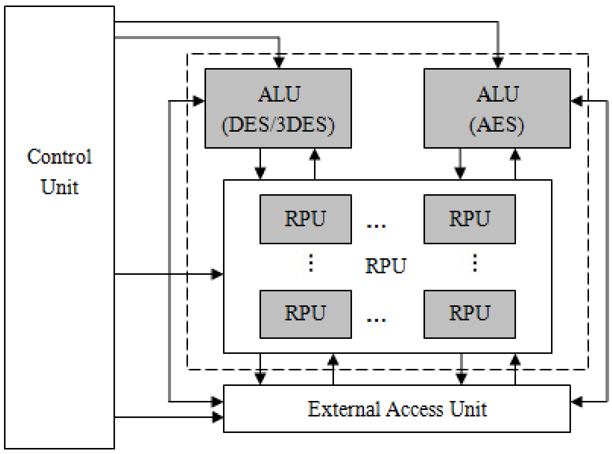

Fig.4 Reconfigurable Data Processing Unit Structure

IV. System Test

This design in Quartus II 8.0 platform for synthesis, placement and routing. Use ModelSim SE 6.0 for the Nios II integrated simulation. Then download to the DE2 board for experimental verification on the Nios IDE software environment.Finally manipulate data in the Console winow of Nios II 8.0 IDE, Observate and verify the data processing results. This paper mainly to simulate the core components of the reconfigurable encryption and decryption system, and on the basis of the simulation, analyse the performance of the system to verify the correctness and high efficiency of the system.

A. DES/3DE Simulation

The Simulation clock set as 100MHZ, in order to ensure the accuracy of the system simulation and test, randomly input 2 groups of test data, among which the test data key of first group K1=K2=K2, realizing DES encryption operation. the input three keys of the second group test data are mutually different, realize 3DES encryption operation, respectively realizing simulation test to them and comparing simulation test results and theoretical results. The waveform of function simulation and sequential simulation respectively as shown in figure 6.1 and figure 6.2, It could be known from the simulation figures that the test results is consistent with the theory add/decryption results of DES/3DES, meet the theoretical value and requirements of timing sequence, explain the component fully realized plus/decryption function of DES/3DES algorithm.

The DES simulation：

The Input key：

4839564C0302519B_4839564C0302519B_4839564C0302519B

Test Data：66453B582DCf440A

The encryption results：C6ED0F1A2F4FAEEF

The 3DES simulation：

The Input key：

04B915BA43FEB5B6_8602876659082198_64056ABDFEA93457

Test Data：7371756967676C65

The encryption results：B8F3189174090598

The simulation as shown in Fig.5 and Fig.6.

Fig.5 DES/3DES Functional Simulation

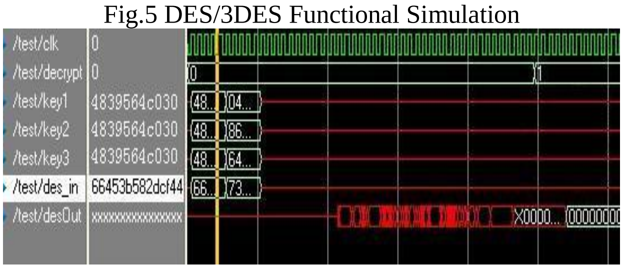

Fig.6 DES/3DES Timing simulation

B. AES Simulation

The Simulation clock set as 100MHZ, in order to ensure the accuracy of the system simulation and test, randomly input 2 groups of test data. The input keys' length is 256, and compare the simulation test results and theoretical results. Function simulation and sequential simulation waveform out respectively as shown in figure 6.3 and figure 6.4,From the simulation waveform ,that test results meet the theoretical value, and meet the timing requirements,

The AES simulation：

The Input key：

49C12E59_5B727361_24472915_43162051_40162224_14816C51_

292315D3—4A317423

In the simulation waveform, input 256-bit key: 49C12E59_5B727361_24472915_43162051_40162224_14816C51_292315D3_4A317423,

Test Data:9A852465_5359C257_23B13338_2811A356,

The encryption results : CDD32741_8370D117_279C0876_83A1F975.

The simulation as shown in Fig.7 and Fig.8.

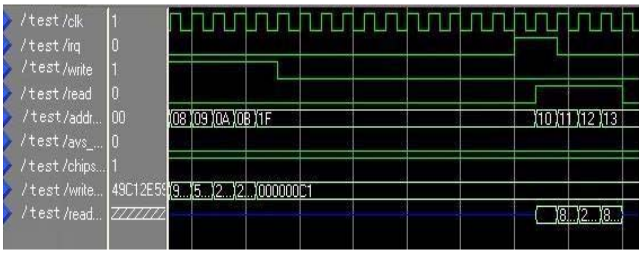

Fig.7 AES Functional Simulation

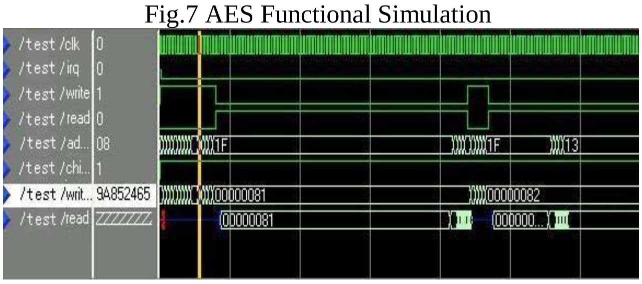

Fig.8 AES Timing simulation

V. CONCLUSION

This paper researched the algorithms DES/3DES/AES, deep analysed the characteristic of arithnmetic and structral properties ot the algorithms, discussed the design and implementation of reconfigurable encryption/decryption system based on SOPC according to the introduction of the SOPC and NiosII system design procedures and process. In this paper, a reconfigurable encryption/decryption IP-core which conforms the the Avalon bus standard, this IP-core can provides two kinds of application choices of the algorithm DES/3DES or AES according to the uese requirements. Then based on SOPC technology we implemented intergration of the system, and coded the relevant driving function and application program, and accomplish the design of reconfigurable process unit, the relevant peripheral function model and the circuit. The system has good versatility and certain practical value, and it can be flexible used in a variety of encryption/decryption occasions. This design layouted and wired on QuartusII 8.0, simulated and verified on ModelSim SE 6.0, and downloaded to DE2 development platform, implemented the system encryption/decryption operation and the acquirement of the operation result by the Console debug window of Nios II 8.0IDE.

REFERENCES

[1] WANG Jian-yu,ZHANG Lu-guo. Reconfigurable Design and Efficient Implementation for AES and SMS4 Algorithm. Computer Engineering,2008,34(15):159-161.

[2] LIU Ze-wen, TANG Liu-chun. Design and Implementation of Security Network Adapter Based on SOPC. Computer Engineering ,2008,34(1):150-152.

[3] ZHANG Wei-ping, ZHAO Ga, SHU Ping-ping, YANG Jun. The design and implementation of a configurable security network adapter on chip，2012,34(14）：246-250.

[4] PANG Zheng-yuan, JIANG Jing-fei. Research and Design of Symmetric Cipher Processing Architecture. cipher processing subword parallism operation linking,2007,(5):796-800.

[5] Yang Xiaohui, Dai Zibin. Research and Design of Reconfigurable Computing Targeted at Block Cipher Processing. Journal o f Computer Resear ch and Dev elo pment, Journal o f Computer Resear ch and Dev elo pment , 2009,46(6):962-967.

[6] QIU Wei-xing, XIAO Ke-zhi, NI Fang, HUANG Hua. DES Key Extension Method. Computer Engineering , 2011, 37 (5):167-171.

[7] [7]Lianqing ZHAO,Miaoying ZHAO.The Application of DES Algorithm in Experimental Teaching of Intelligent Management System[C]. Proceedings of 2011 National Teaching Seminar on Cryptography and Information Security,2011:153-155.

[8] LI Ai-Ning, TANG Yong. Optimization of 3DES Cryptography Algorithm Based on Python.Computer Systems & Applications,2011,20(8):184-187.

[9] Fips-197, advanced encryption standard, National Institute of Standards and Technology(NIST).2001.

[10] Chen Yicheng,Zou Xuecheng,et al.Energy-efficient and security-optimized AES hardware design for ubiquitous computing[J].Journal of Systems Engineering and Electronics,2008,19(4):652-658.