WUJNS
Wuhan University Journal of Natural Sciences

Vol.11 No.6 2006 1569-1572

Article ID:1007-1202(2006)06-1569-04

Dynamically Reconfigurable Encryption System of the AES

WANG Youren, WANG Li, YAO Rui, ZHANG Zhai, CUI Jiang

College of Automation Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, Jiangsu, China

Abstract: Reconfigurable computing has grown to become an important and large field of research, it offers advantages over traditional hardware and software implementations of computational algorithms. The Advanced Encryption Standard (AES) algorithm is widely applied in government department and commerce. This paper analyzed the AES algorithms with different cipher keys, adopted a novel key scheduler that generated the round key real—time, proposed a dynamically reconfigurable encryption system which supported the AES algorithm with different cipher keys, and designed the architecture of the reconfigurable system. The dynamically reconfigurable AES system had been realized on FPGA. The result proves that the reconfigurable AES system is flexible, lower cost and high security level.

Key words: dynamically reconfigurable hardware; field programmable gate array (FPGA); advanced encryption standard (AES) algorithm; cipher key

CLC number: TP 391

Received date: 2006-05-28

Foundation item: Supported by the National Natural Science Foundation of China (60374008)

Biography: WANG Youren (1963-), male, Professor, Ph. D., research direction: bio-inspired hardware, intelligent testing and self-repairing of electronic equipments. E-mail: wangyrac@nuaa.edu.cn

0 Introduction

After three rounds of evaluation on the 15 candidate algorithms, the National Institute of Standards and Technology (NIST) selected the Rijndael as the Advanced Encryption Standard (AES) algorithm. The AES algorithm is a symmetric block cipher that processes data block of 128 bits using a cipher key of length 128, 192, or 256 b. The AES algorithm, which is safer than Data Encryption Standard (DES), is used in a wide range of application in Internet, electronic commerce, digital signature and wireless communication in order to protect sensitive data[1,2].

Nowadays, the implementations of the AES algorithm are hardware implementation and software implementation[3]. The software implementation is convenient, more flexible, and also easily upgraded. The hardware implementation is faster than software, and a special cryptographic chip is also safer than software. In the literature, there are some AES hardware implementations for both Application Specific Integrated Circuit (ASIC) and Field Programmable Gate Array (FPGA), but ASIC has less flexibility[4,5]. Configurable AES processor is complex, not easy to operate and holds more hardware resource[6]. Considering the speed, flexibility and security, a reconfigurable encryption system, which has the advantages of software and hardware, has been proposed. The reconfigurable encryption system is much easy and lower cost, while dynamical configuration saves the configuring time. Meanwhile the reconfigurable technology lays the foundation for realizing more flexible and safer cryptographic algorithm.

Based on reconfigurable technology, this paper designs an AES reconfigurable system which supports 128, 192, and 256 b keys. A novel key scheduler is also proposed to generate the

round key dynamically. The key generators generate the round keys concurrently during the encryption or decryption procedure without extra memory to store the sub-keys, which saves a lot of hardware resource. The dynamically reconfigurable AES system which supports AES-128, AES-192, AES-256 is realized on Xinlinx Virtex-E FPGA.

1 The AES Algorithm

The AES algorithm is a symmetric block cipher that processes data blocks of 128 b, using cipher key with three different lengths: 128, 192, or 256 b. Its operations are performed in the State. The State is a two-dimensional array of bytes, consisting of four rows and N_b column, where N_b is the block length divide by 32. At the start of the cipher operation the input block is copied to the State. After an initial Round Key addition, the State is transformed by a round function implemented N_r times. Number of rounds in an AES implementation depends on key length (see Table 1). There are four transformations in round function, as shown in Fig. 1[7,8].

Table 1 Number of rounds according to key length

Algorithm	Key Length (N_k words)	Block Size (N_b words)	Number of Rounds(N_r)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

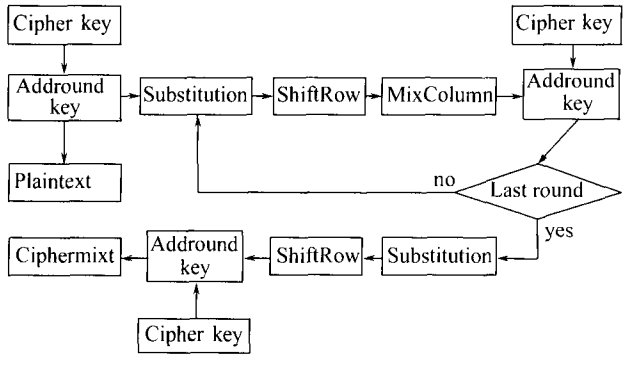

Fig. 1 Encryption structure of the AES algorithm

AddroundKey(): In this transformation a Round Key is added to the state by a simple bitwise XOR operation. The length of a Round Key equals the size of the State.

SubBytes(): This is a non-linear transformation that operates independently on each byte of the state using a substitution table (called S-box). The S-box is a one-to-one mapping table and consequently it is invertible. This operation provides the non-linearity in the cipher.

ShiftRows(): The ShiftRows block operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For the algorithm, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifts by offsets of two and three respectively. In this way, each column of the output state of the ShiftRows block is composed of bytes from each column of the input state.

MixColumns(): In the MixColumns block, the four bytes of each column of the state are combined using an invertible linear transformation. The MixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes. Each column is treated as a polynomial over GF (2^8) and is then multiplied modulo x^4+1 with a fixed polynomial $c(x)=3x^3+x^2+x+2$. The MixColumns block can also be viewed as a matrix multiply in Rijndael's finite field. This transformation operates on the state column-by-column[9-11].

2 Implementation of the Dynamically Reconfigurable AES System

This paper combines software with hardware to realize the reconfigurable system which suits to AES-128, AES-192, AES-256. At first, according to the control data, the key length of the AES has been chosen, and then the hardware realizes the AES algorithm. The architecture of the system is shown in Fig. 2. Program compiled by Visual C++ is used to read the control data, choose the bit file, and then download the plaintext and the key to the SRAM. The software flowchart of the reconfigurable system is shown in Fig. 3. The input data includes plaintext, key, and control data. The Visual

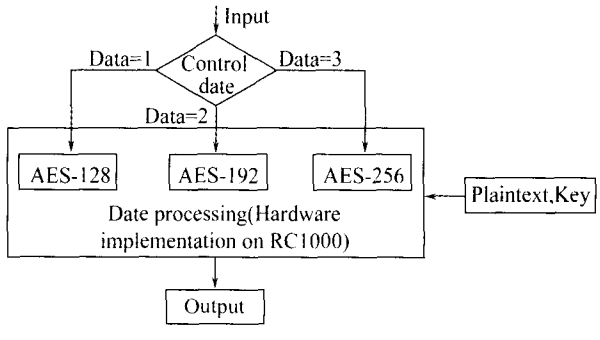

Fig. 2 The architecture of the reconfigurable AES system

C++ program configures the bit file, reads the data from the card, and shows the results.

The hardware resource of the reconfigurable AES system is RC1000 from the Celoxica Company, and the core circuits in RC1000 are the Xinlix Virtex-E FPGA, several SRAMs and interface control circuit. The Virtex-E FPGA is based on the SRAM, and needs to download the bit file to internal memory to realize the customization. The Handle-C language is used to perform hardware design of the AES algorithm, whose hardware structure is shown in Fig. 4. The structure includes: data input unit, key generator, and data processing unit. The data input unit stores the control data, key and plaintext. The key generator generates the round keys real-time. The data processing unit completes the operations of AddroundKey, SubBytes, ShiftRows, MixColumns.

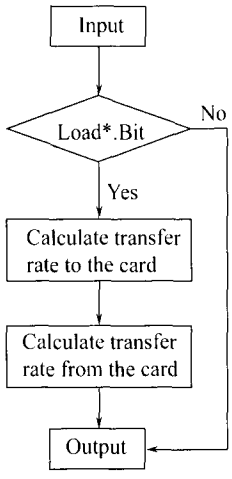

Fig. 3 Software flowchart of reconfigurable AES system

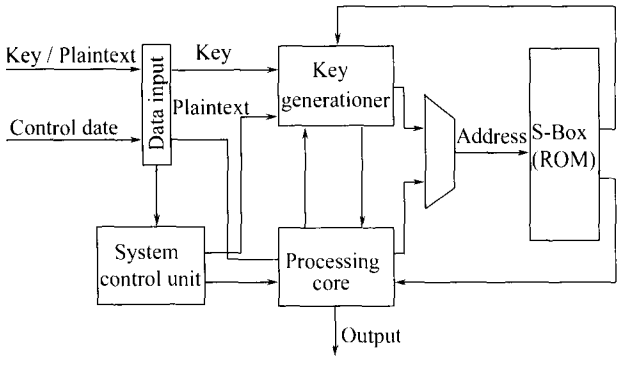

Fig. 4 Hardware structure of reconfigurable AES hardware implementation

The AES algorithm requires different round key used in every round, so it is important to generate a new round key real-time. This paper adopts a novel key scheduler that generates round keys dynamically. The key generator generates the round keys concurrently during the encryption or decryption procedure. The method, adopted in this paper, is safer and more convenient, and also saves the encryption time which improves the implementing speed.

The design criteria of S-box in key expansion and SubByte transformation are inspired by the use of algebraic manipulation. But the algebraic manipulation needs more hardware resource and more time. S-box in this paper is in form of Look-up Table (LUT), which saves the time to generate the S-box.

The MixColumns transformation of the AES cipher algorithm mixes the bytes in each column by the multiplication of the state with a fixed polynomial modulo with its coefficient in GF(2^8). The method of multiplication holds a lot of resource, so shift and XOR operation are used to realize the MixColumns transformation which reduces logic resource, simplifies the circuit and improves the computing speed.

3 Results

The dynamically reconfigurable system which supports the AES-128, AES-192, AES-256 has been realized on RC1000. According to the control data, the key length and bit file are chosen. The key length is different, the encryption round and the security are also different. The longer the key length is, the higher security level the AES algorithm has. The transmission rates of the dynamically reconfigurable AES system are shown in Table 2.

Table 2 Transmission rates of the dynamically reconfigurable AES system Mb/s

Algorithm	Writing speed to the card	Reading speed from the card
AES-128	111.30	116.40
AES-192	110.31	108.46
AES-256	111.30	114.29

From the Table 2, It is concluded that the key length do not influence the data throughput of the AES algorithm. The difference of AES-128, AES-192, AES-256 is the round number of the encryption which do not influence the speed much. The hardware implementation ensures that the three algorithms are same on realizing speed.

The key generators generate the round keys concurrently during the encryption or decryption procedure without extra memory to store the sub-keys. The methods of this paper and using extra memory to store sub-

key are both emulated on FPGA. The hardware resources of the two methods are shown in Table 3.

Table 3 Hardware resource with memory and without memory (NANDs)

Algorithm	The method adopted in this paper	Adopting extra memory to store the sub-keys
AES-128	49 404	87 356
AES-192	96 580	115 924
AES-256	126 693	150 043

Comparing to the method that uses extra memory to store the sub-keys, the method adopted in this paper is safer, lower cost, and not easily attacked. From Table 3, it is concluded that if increasing the key length, the cost is increased too. The reconfigurable system reduces a huge amount of resources that only needs 126 693 NANDs (Not AND gate), while the conventional AES system needs much more than 126 693 NANDs. 126 693 NANDs are used to realize AES-256 which is the biggest cost in the three algorithms, and these hardware resources are enough to realize the AES-128, AES-192. The dynamically reconfigurable AES system is optimized for achieving lower cost.

4 Conclusion

A dynamically reconfigurable system is designed to implement the AES-128, AES-192, AES-256. According to the control data, the algorithm is chosen to encrypt the data. Meanwhile, a novel key scheduler is proposed to generate the round keys concurrently during the encryption or decryption procedure, and the security of cipher key is improved. This dynamically reconfigurable system is suited to the AES algorithm with different cipher key lengths and different surroundings. The dynamically reconfigurable AES system is realized on Virtex-E FPGA, and achieves higher speed, lower cost and higher security level.

References

[1] Xiao Guozhen, Bai Enjian, Liu Xiaojuan. Some New Developments on the Cryptanalysis of AES[J]. *Acta Electronica Sinica*, 2003, **31**(10): 1549-1554(Ch).

[2] Su Chihpin, Horng Chialung, Huang Chihtsun, *et al*. A Configurable AES Processor for Enhanced Security [C]// *Asia and South Pacific Design Automation Conference*. Shanghai: IEEE Press, 2005: 361-366.

[3] Huang Xiaoyuan, Dai Zibin. Design on FPGA Implementation of AES Algorithm Chip [J]. *Microelectronics and Computer*, 2005, **28**: 62-68(Ch).

[4] Zhang Xinmiao, Psrhi K K. High-Speed VLSI Architectures for the AES Algorithm[J]. *IEEE Transaction on very Large Scale Integration (VLSI) Systems*. 2005, **12**: 957-967.

[5] Wang S S, Ni W S. An Efficient FPGA Implementation of Advanced Encryption Standard Algorithm[C] //*Proceedings of the* 2004 *International Symposium on Circuits and Systems*. Chengdu: IEEE Press, 2004: 597-600.

[6] Fu Yongzhi, Hao Lin, Zhang Xuejie, *et al*. Design of An Extremely High Performance Counter Mode AES Reconfigurable Processor [C] //*Second International Conference on Embedded Software and Systems*. Scottsdale, USA: IEEE Press, 2005: 262-268.

[7] Brokalakis A, Kakarountas A P, Goutis C. A High-Throughput Area Efficient FPGA Implementation of AES-128 Encryption[C] //*IEEE Workshop on Signal Processing System Design and Implementation*. Athens, Greece: IEEE Press, 2005: 116-121.

[8] Wang Jingfa, Chang Sunwei, Lin Pochuan. A Novel Round Function Architecture for AES Encryption/Decryption Utilizing Look-up Table[C] //*IEEE 37th Annual* 2003 *International Carnahan Conference on Security Technology*. Taipei: IEEE Press, 2003: 132-136.

[9] Hsiao S F, Chen M C. Two Efficient Area Reduction Methods for Implementations of the Rijndael Advanced Encryption Standard[C] //*The* 2004 *IEEE Asia-Pacific Conference on Circuits and System*. Fukuoka, Japan: IEEE Press, 2004, 1: 353-356.

[10] Lai Y K, Chang L C, Chen L F, *et al*. A Novel Memoryless AES Cipher Architecture for Networking Applications[C] // *Proceedings of the* 2004 *International Symposium on Circuit and System*. Vancouver, Canada: IEEE Press, 2004: 23-26.

[11] Kotturi D, Yoo S M, Blizzard J. AES Crypto Chip Utilizing High-Speed Parallel Pipelined Architecture[C] //*IEEE* 2005 *International Symposium on Circuits and Systems*. Tokyo, Japan: IEEE Press, 2005: 4653- 4656.

□