Hardware Implementation of AES Encryption and Decryption System Based on FPGA

Shihai Zhu*

College of Information Engineering and Art Design, Zhejiang University of Water Resources and Electric Power, Hangzhou, 310018, China

Abstract: AES algorithm has played an important role in information security field for a long time since Rijndael algorithm was announced as advanced encryption standard. Hardware implementation based on FPGA of AES algorithm has the advantages of fast, flexible, short development cycle, etc. Hardware implementation based on FPGA of AES encryption and decryption system was studied in detail in this paper. First, implementation scheme and key technology to adopt internal and external mixing pipeline structure were determined, and the overall design flow chart was given. Next, this design supports three modes of encryption and decryption process of AES algorithm under the condition of data group of 128 bits, key length of 128, 192 and 256 bits respectively. In the following, system optimization design of AES encryption and decryption algorithm was completed on the same piece of FPGA chip; Finally, coding work and comprehensive compilation were finished by QUARTUS II development tool, and the simulation results by MODELSIM software were also given. In a word, this design realized the balance of resources and speed to a bigger extent.

Keywords: AES, FPGA, encryption & decryption algorithm, pipeline.

1. INTRODUCTION

Advanced encryption standard (AES) has undergone the development process from software to hardware implementation since it was taken into effect from May, 2002. Along with network transmission speed is promoted to gigabits orders of magnitude, the requirement of algorithm execution speed is becoming more and more high, password algorithm based on software implementation appears insufficient in performance, therefore it is necessary for people to adopt hardware encryption algorithm, which uses some special optimization techniques (such as pipeline and lookup table, etc.), thus data flow is greatly improved and the generation time of key is reduced [1, 2]. In addition, encryption algorithm and corresponding key generation implemented by hardware can be encapsulated into a chip which is not easy to be read or changed by outside attacker, thus will have a higher physical security [3-5]. Therefore, cryptographic algorithms based on hardware implementation have caught widespread attention of the industry. Reconfigurable hardware represented by FPGA has its own inherent characteristics of higher security and speed of hardware and flexibility and maintainability of software, which has become a hot research direction of block cipher algorithm for hardware implementation [6, 7]. We introduced FPGA realization method of AES encryption and decryption system in this paper, and the optimization of its speed and resource-intensive processing techniques was discussed.

2. PRINCIPLE OF AES ENCRYPTION AND DECRYPTION SYSTEM

AES algorithm is a kind of iterated block cipher, which deals with encryption and decryption operations of 128-bit data blocks. As advanced encryption standard, both of data group length and initial key length of Rijndael algorithm are variable. In order to meet the requirements of AES, group length is fixed to 128 bits, key length is respectively represented by 128/192/256 bits. During the operations of encryption and decryption of AES, first, the inputted data of 128 bytes are first arranged into 4 * 4 byte matrix, then 10 (128 bit key), 12 (192 bit key) or 14 (256 bit key) rounds of transformations are conducted according to different key lengths, the number of round is decided by key length. The implementation of AES encryption algorithm includes key extension process and encryption process [8]. For example, if key length is 128 bits, then encryption process includes an initial round of key addition (AddRoundKey), nine times of round transformations (Round), and the final round of transformation (FinalRound), as shown in Fig. (**1**).

Every round transformation is composed of four layers, which are listed below. The first layer is byte substitution (SubBytes), meaning that S box whose input is 8 bits, and output is also 8 bits acts on each byte of state matrix; The second and the third layer are respectively ShiftRows, and column transformation (MixColumns), meaning that 4 * 4 state matrix is transformed by line shift and mixed in the column; The fourth layer is key addition (AddRoundKey), meaning that each byte of the key and corresponding byte of state matrix are performed xor operations [9]. The process of each round is shown as Fig. (**2**).

1874-110X/15 2015 Bentham Open

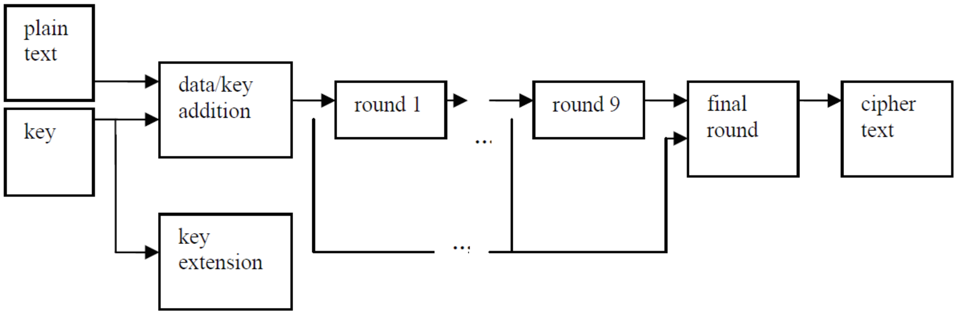

Fig. (1). The whole process of encryption (key length is 128 bits).

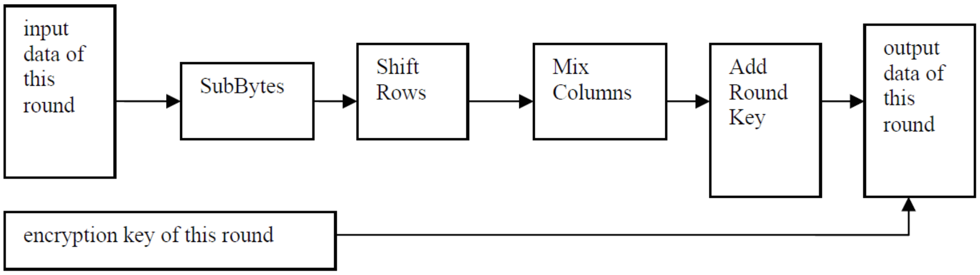

Fig. (2). The structure of every round.

Similarly, the realization of AES decryption algorithm includes key extension process and decryption process. Decryption process is similar to encryption process, and is the inverse operation of encryption process. The encryption and decryption process of AES algorithm for data group size of 128 bits and initial key length of 128 bits is shown as Fig. (**3**).

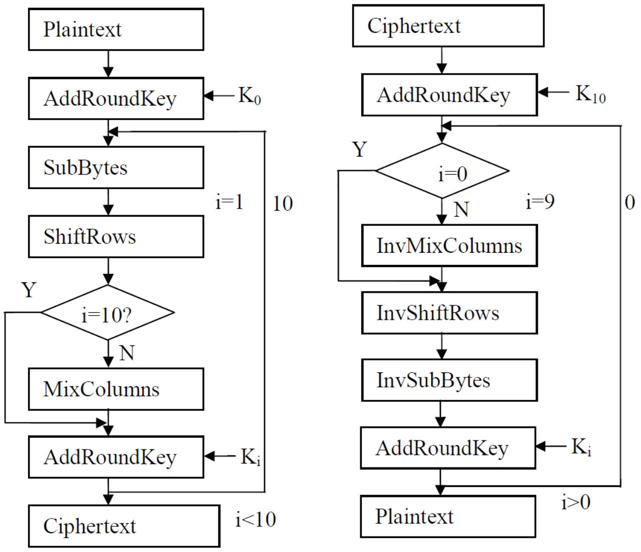

Fig. (3). The encryption and decryption process of AES algorithm (128 bits key).

3. FPGA-BASED IMPLEMENTATION OF AES ENCRYPTION AND DECRYPTION SYSTEM

Hardware implementation of AES encryption and decryption system in this paper is under the condition of satisfying timing requirements, and reducing the whole chip area. Hardware implementation improved the structure of each module within the algorithm and the structure of the whole system. Specifically speaking, it adopts internal and external mixing pipeline, and at the same time, byte substitution, column mixing transformation and key extension operation are respectively optimized to achieve the aim of improving the processing speed of AES encryption and decryption system and realizing the balance between speed and occupied resources [10-12]. The design process of the whole system is shown as Fig. (**4**).

The system is composed of the following modules: data input and output module, encryption and decryption operation module, key extension module, and control unit to control the whole process. Specifically speaking, Control unit generates control signals required for each module; key extension module completes the production and dispatching of keys for each round; encryption and decryption operation module finishes data round transformation [13-15]. Note that control signals enter from input interface, data and keys come from data bus to conduct data transmission, substitute keys and conduct encryption and decryption operations according to control signals of control modules.

3.1. The Work Pattern and Structure of Encryption and Decryption Module

The work pattern of AES algorithm is divided into feedback model and non-feedback. In feedback work pattern, the operations of group encryption and decryption can only be performed in sequence, that is to say, encryption or decryption steps in all the groups must be executed in serial sequence; In the non-feedback work pattern, subsequent group data block operations have nothing to do with previous group data block, therefore all operations can be concurrently performed in theory. In addition, encryption and decryption speed is different under different work patterns. Encryption and decryption speed of AES algorithm refers to the number of bits performed in unit time to complete the

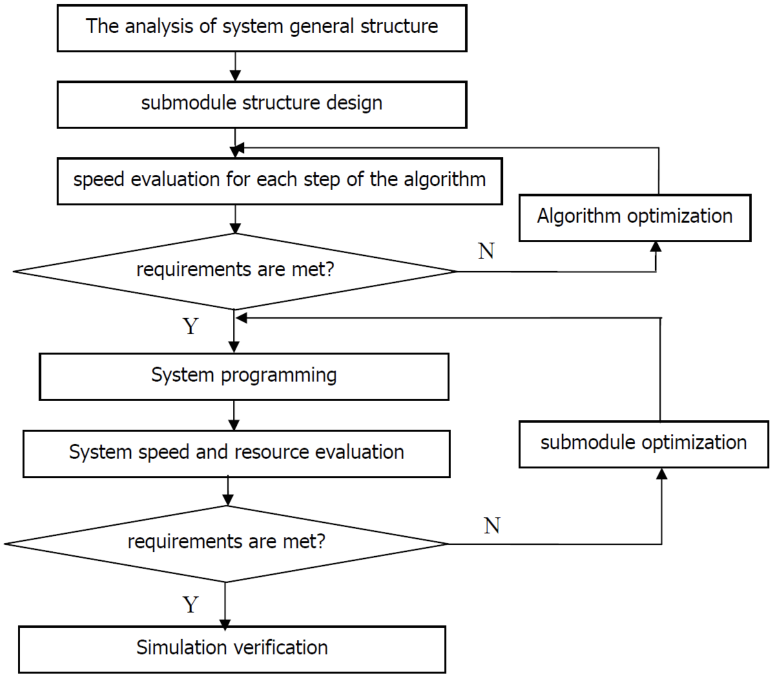
The analysis of system general structure
submodule structure design
speed evaluation for each step of the algorithm
Algorithm optimization
N
requirements are met?
Y
System programming
System speed and resource evaluation
submodule optimization
N
requirements are met?
Y
Simulation verification

Fig. (4). System design flow chart.

encryption or decryption process, or called throughput, also known as a unit for megabits per second (Mbit/s). The structure of encryption and decryption module has a close relationship with its work pattern, whose basic structure can be divided into the following three kinds: external pipeline structure, internal pipeline structure and loop unrolling structure.

3.2. The Design of Encryption and Decryption Module

In AES encryption and decryption system, in order to improve speed and reduce resource utilization and realize the balance of speed and resource, internal and external mixing pipeline structure based on non-feedback work pattern was adopted. Internal and external mixing pipeline structure of encryption unit is shown as Fig. (**5**). Similarly, internal and external mixing pipeline structure of decryption unit is shown as Fig. (**6**).

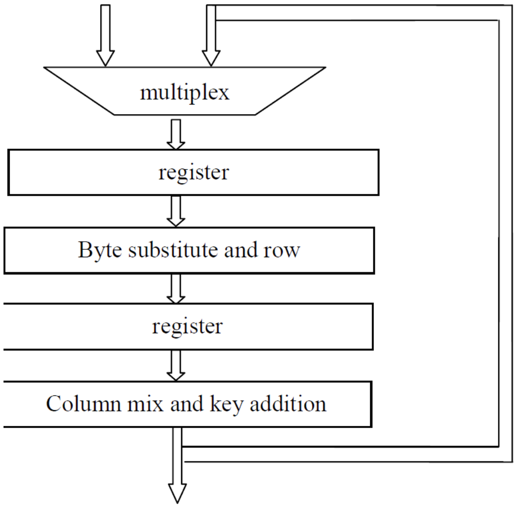

Fig. (5). Internal and external mixing pipeline structure of encryption unit.

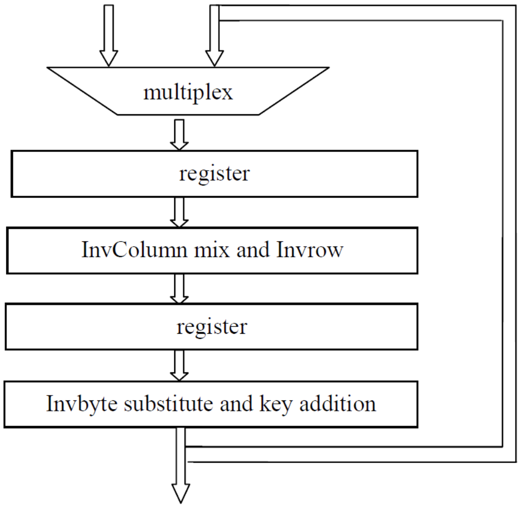

Fig. (6). Internal and external mixing pipeline structure of decryption unit.

4. SIMULATION RESULTS AND ANALYSIS

First, we performed function simulation with the purpose of verifying the correctness of system logic function. Under the condition of data group of 128 bits, initial key length of 128 bits, system function simulation was performed to verify the correctness of logical function of AES encryption and decryption system. A set of test data used by simulation (using hexadecimal representation) are listed as follows:

Plaintext (128 bits): 3243f6a8885a308d313198a2e0370 734;

Key (128bits): 2b7e151628aed2a6abf7158809cf4f3c;

Ciphertext (128bits): 3925841d02dc09fbdc118597196a0 b32;

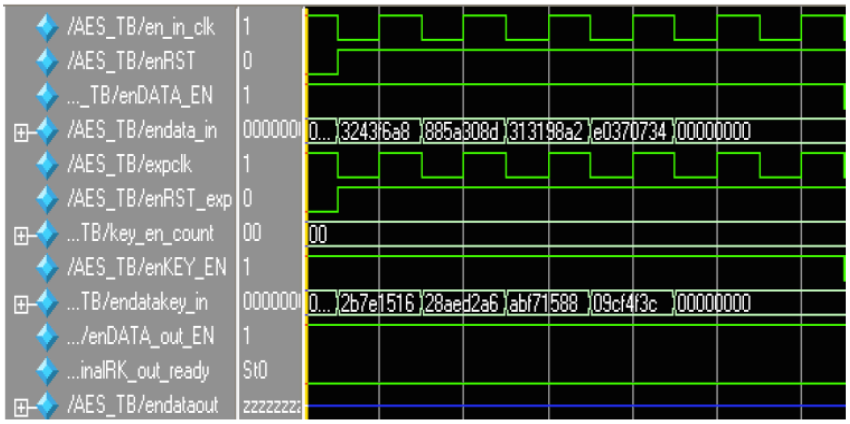
/AES_TB/en_in_clk 1
/AES_TB/enRST 0
..._TB/enDATA_EN 1
/AES_TB/endata_in 000000 0... 3243f6a8 885a308d 313198a2 e0370734 00000000
/AES_TB/expclk 1
/AES_TB/enRST_exp 0
...TB/key_en_count 00 00
/AES_TB/enKEY_EN 1
...TB/endatakey_in 000000 0... 2b7e1516 28aed2a6 abf71588 09cf4f3c 00000000
.../enDATA_out_EN 1
...inalRK_out_ready St0
/AES_TB/endataout zzzzzzz

Fig. (7). Data input of encryption part of this system.

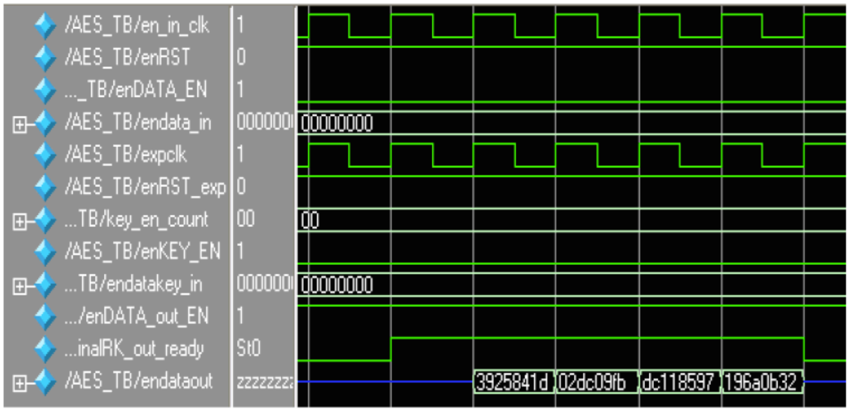

Fig. (8). Data output of encryption part of this system.

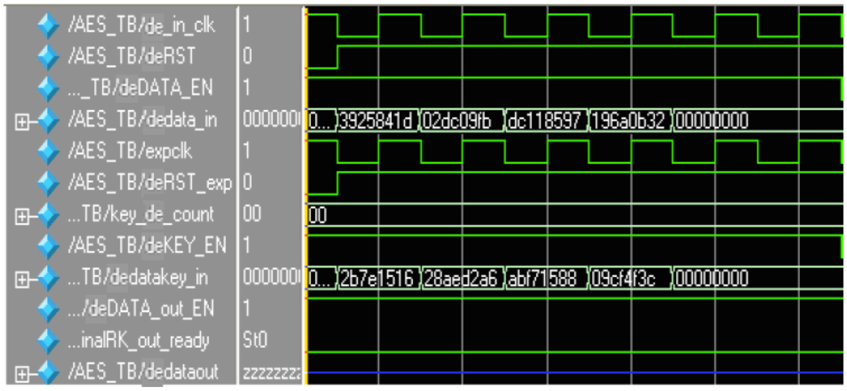
/AES_TB/de_in_clk 1
/AES_TB/deRST 0
..._TB/deDATA_EN 1
/AES_TB/dedata_in 000000 0... 3925841d 02dc09fb dc118597 196a0b32 00000000
/AES_TB/expclk 1
/AES_TB/deRST_exp 0
...TB/key_de_count 00 00
/AES_TB/deKEY_EN 1
...TB/dedatakey_in 000000 0... 2b7e1516 28aed2a6 abf71588 09cf4f3c 00000000
.../deDATA_out_EN 1
...inalRK_out_ready St0
/AES_TB/dedataout zzzzzzz

Fig. (9). Data input of decryption part of this system.

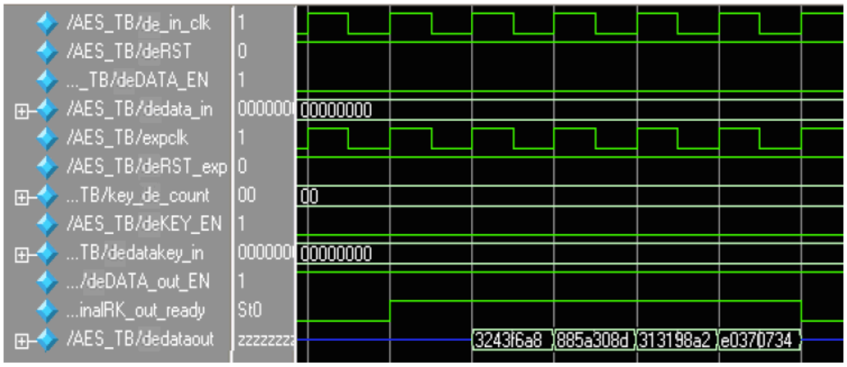

Fig. (10). Data output of decryption part of this system.

Data input and output of encryption part of this system is shown as Figs. (**7**) and (**8**).

Similarly, data input and output of decryption part of this system is shown as Figs. (**9**) and (**10**).

Test results shows that this system functions exactly, and correctly implements AES encryption and decryption system to encrypt and decrypt data under the condition of plaintext group of 128 bits, initial key length of 128 bits.

5. CONCLUSION

First, we finished software design code description and comprehensive compilation by QUARTUS Ⅱ software of ALTERA corporation based on the overall structure of AES encryption and decryption system. Next, we performed design simulation by MODELSIM software. Finally, system design and validation results were given. During the design of the whole system, we adopted comprehensive coding style. Open test vector was adopted by function simulation, and the fact that simulation results and test vector data are consistent verified the correctness of system logic functions.

This design does not have the fastest speed, however, its throughput is dominant in general. Furthermore, this design has good speed area ratio. At the same time, the design of the system combines encryption with decryption algorithm, which can be completely executed in parallel. In addition, it achieves the balance of speed and resources under the premise of ensuring encryption and decryption speed.

CONFLICT OF INTEREST

The author confirms that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

We would like to thank the research foundation of water conservancy department of Zhejiang province of China for contract RC1339, under which the present work was made possible.

REFERENCES

[1] H. Kim, S. Hong, and J. Lim, “A fast and provably secure higher-order masking of AES S-box”, *Proceedings of CHES LNCS*, vol. 6917, pp. 95-107, 2011.

[2] C. Carlet, L. Goubin, E. Prouff, M. Quisquater, and M. Rivain, “Higher order masking schemes for S-boxes”, *Proceedings of FSE LNCS*, vol. 7549, pp. 366-384, 2012.

[3] J. D. Golic, “Techniques for random masking in hardware”, *IEEE Transactions on Circuits Systems*, vol. 54, no. 2, pp. 291-300, 2014.

[4] D. Canright, and L. Batina, “A very compact ‘perfectly masked’ S-box for AES”, *Proceedings of ACNS LNCS*, vol. 5037, pp. 446-459, 2008.

[5] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. New York: Spinger-Verlag, 2013.

[6] Z. Yuan, Y. Wang, J. Li, R. Li, and W. Zhao, “FPGA based optimization for masked AES implementation”, In: *Proceedings of IEEE 54th International MWSCAS*, Seoul, Korea, 2011, pp. 1-4.

[7] M. Alam, S. Ghosh, M. J. Mohan, D. Mukhopadhyay, D. R. Chowdhury, and I. S. Gupta, “Effect of glitches against masked AES S-box implementation and countermeasure”, *IET Information Security*, vol. 3, no. 1, pp. 34-44, 2014.

[8] E. Trichina, T. Korkishko, and K. H. Lee, “Small size, low power, side channel-immune AES coprocessor: Design and synthesis results”, *Proceedings of AES LNCS*, vol. 3373, pp. 113-127, 2005.

[9] S. K. Mathew, F. Sheikh, M. Kounavis, S. Gueron, A. Agarwal, S. K. Hsu, H. Kaul, M. A. Anders, and R. K. Krishnamurthy, “53 Gbps native GF(24) 2 composite-field AES-encrypt/decrypt accelerator for content-protection in 45 nm high-performance microprocessors”, *IEEE Journal of Solid-State Circuits*, vol. 46, no. 4, pp. 767-776, 2011.

[10] M. McLoone, and J. V. McCanny, “Rijndael FPGA implementations utilizing look-up tables”, In: *Proceedings of IEEE Workshop Signal Processing Systems*, Antwerp, Belgium, 2001, pp. 349-360.

[11] A. Hodjat, and I. Verbauwhede, “A 21.54 Gbits/s fully pipelined processor on FPGA”, In: *12th Annual IEEE Symposium on Field-Programmable Custom Computing Machines*, Napa, CA, USA, 2004, pp. 308-309.

[12] S. Mangard, N. Pramstaller, and E. Oswald, “Successfully attacking masked AES hardware implementations”, *Proceedings of CHES LNCS*, vol. 3659, pp. 157-171, 2005.

[13] E. Oswald, S. Mangard, N. Pramstaller, and V. Rijmen, “A side-channel analysis resistant description of the AES S-box”, In: *Proceedings of FSE LNCS*, vol. 3557, pp. 413-423, 2014.

[14] R. Sakthivel, M. Vanitha, Harish M. Kittur, “Low power high throughput reconfigurable stream cipher hardware VLSI architectures”, *International Journal of Information and Computer Security*, vol. 6, no. 1, pp. 1 - 11, 2014.

[15] K. M. Abdellatif, R. Chotin-Avot, and H. Mehrez, “Low cost solutions for secure remote reconfiguration of FPGAs”, *International Journal of Embedded Systems*, vol. 6, no. 2/3, pp. 257 - 265, 2014.

Received: June 10, 2015 Revised: July 29, 2015 Accepted: August 15, 2015