ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Design Area efficient of Advanced Encryption Standard Based on FPGA

Dr. Arvind Kundu, M.Tech, Ph.D
HOD,
Department of ECE,
Scient Institute of Technology,
Ibrahimpatnam.

Mr.M.Suresh Kumar, M.Tech
Assistant Profesor,
Department of ECE,
Scient Institute of Technology,
Ibrahimpatnam.

M Karthik
M.Tech,
Department of ECE,
Scient Institute of Technology,
Ibrahimpatnam.

Abstract:
A new FPGA-based implementation scheme of the AES-128 (Advanced Encryption Standard, with 128-bit key) encryption algorithm is proposed in this paper. For maintaining the speed of encryption, the pipelining technology is applied and the mode of data transmission is modified in this design so that the chip size can be reduced. The 128-bit plaintext and the 128-bit initial key, as well as the 128-bit output of ciphertext, are all divided into four 32-bit consecutive units respectively controlled by the clock. The synthesis verification based on HJTC0.18um CMOS process shows that this new program can significantly decrease quantity of chip pins and effectively optimize the area of chip.

I INTRODUCTION:

With the rapid development and wide application of computer and communication networks, the information security has aroused high attention. Information security is not only applied to the political, military and diplomatic fields, but also applied to the common fields of people's daily lives. With the continuous development of cryptographic techniques, the long-serving DES algorithm with 56-bit key length has been broken because of the defect of short keys. The "Rijndael encryption algorithm" invented by Belgian cryptographers Joan Daemen and Vincent Rijmen's had been chosen as the standard AES (Advanced Encryption Standard) algorithm whose packet length is 128 bits and the key length is 128 bits, 192 bits, or 256 bits.

Since 2006, the Rijndael algorithm of advanced encryption standard has become one of the most popular algorithms in symmetric key encryption. AES can resist various currently known attacks. Hardware security solution based on highly optimized programmable FPGA provides the parallel processing capabilities and can achieve the required encryption performance benchmarks. The current area-optimized algorithms of AES are mainly based on the realization of S-box mode and the minimizing of the internal registers which could save the area of IP core significantly. One new AES algorithm with 128-bit keys (AES-128) was described in this paper, which was realized in Verilog Hardware Description Language.

The 128-bit plaintext and 128-bit key, as well as the 128-bit output data were all divided into four 32-bit consecutive units respectively. The pipelining technology was utilized in the intermediate nine round transformations so that the new algorithm achieved a balance between encryption speed and chip area, which met the requirements of practical application. Cryptography is the science of writing the secret codes, enabling the confidentiality of communication through an insecure channel. It provides protection against unauthorized parties by preventing unauthorized alteration of use. It uses a cryptographic system to transform a information from paintext to cipher text, using private and public key. Basically, there are different types of cryptographic algorithm.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

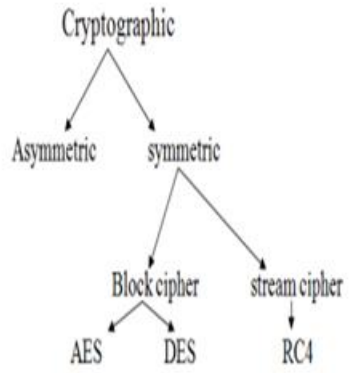


Fig.Classification of Cryptographic algorithm

The Fpga Implementation Of Area-Optimized Aes-128:

Brief Description of Rijndael Algorithm Rijndael algorithm consists of encryption, decryption and key schedule algorithm. The main operations of the encryption algorithm among the three parts of Rijndael algorithm include: bytes substitution (SubBytes), the row shift (ShiftRows), column mixing (MixColumns), and the round key adding (AddRoundKey). It is shown as Fig. 1.

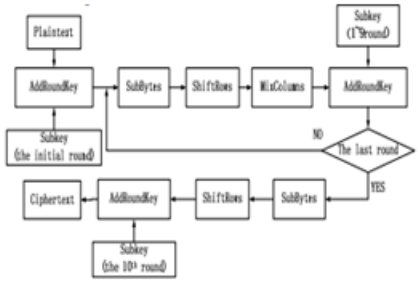


Figure 1. The structure of Rijndael encryption algorithm

Encryption algorithm processes Nr+1 rounds of transformation of the plaintext for the ciphertext. The value of Nr in AES algorithm whose packet length is 128 bits should be 10, 12, or 14 respectively, corresponding to the key length of 128,192,256 bits. In this paper, only the (AES-128) encryption scheme with 128-bit keys is considered.

The Design of Improved AES-128 Encryption Algorithm:

1) Two main processes of AES encryption algorithm:
The AES encryption algorithm can be divided into two parts, the key schedule and round transformation. Key schedule consists of two modules: key expansion and round key selection. Key expansion means mapping Nk bits initial key to the so-called expanded key, while the round key selection selectesNb bits of round key from the expanded key module. Round Transformation involves four modules by ByteSubstitution, ByteRotation, MixColumn and AddRoundKey Key points for the design: In the AES-128, the data in the main process mentioned above is mapped to a 4×4 two-dimensional matrix. The matrix is also called state matrix, which is shown as Fig.2.

a_{00}	a_{01}	a_{02}	a_{03}
a_{10}	a_{11}	a_{12}	a_{13}
a_{20}	a_{21}	a_{22}	a_{23}
a_{30}	a_{31}	a_{32}	a_{33}

Figure 2. The state matrix

Take the independent and reversible bytes substitution operation of S-box as example. Firstly, the state matrix is divided into four columns. And then byte replacement is achieved by the operation of look-up table shown as Fig. 3.

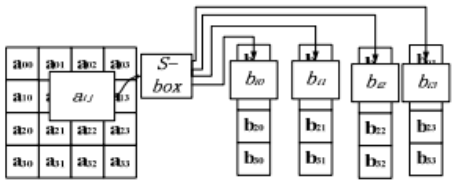


Figure 3. Bytes segmentation and replacement processing

III PROPOSED SYSTEM:

From the above analysis, we can find that the process of AES encryption can be mainly divided into two parts: key schedule and round transformation. The improved structure is also divided into these two major

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

processes. The initial key will be sent to the two modules: Keyexpansion and Keyselection, while the plaintext is to be sent to the round transformation after the roundkey is selected. But the operand of data transmission is turned into a 32-bit unit. The process of new algorithm is shown as Fig. 4.

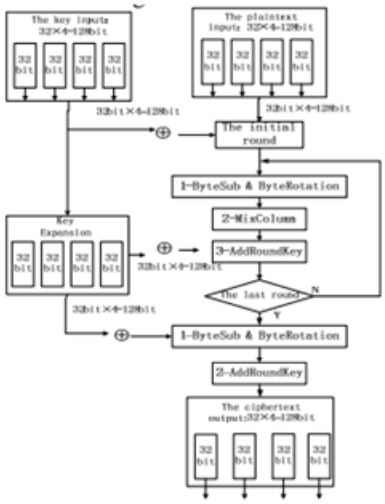
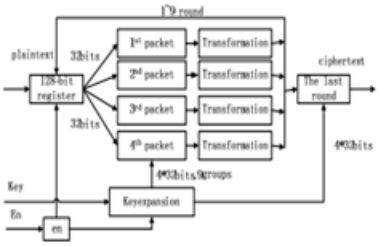


Figure 4. The new improved structure of AES algorithm

Round Transformation in the intermediate steps: A round transformation mainly realizes the function of SubBytes and MixColumns with 32-bit columns. Four packets of round transformation are processed independently. Then the results of MixColumns and the 32-bit keys sourced from Keyexpansion are combined by using XOR operators.

Here, the round transformation is a module with 64 input ports (32- bit plaintext+32-bit key) and 32 output ports. Fig.5 is a block diagram for the introduction of pipelining technology used in the round transformation.



In the process of pipelining, the 128-bit data is divided into four consecutive 32-bit packets that take round transformation independently. The operation of the above four groups of data can be realized in pipelining technology. In brief, it can be described as follow: store the unprocessed data in the 128-bit register, and control the clock for re-starting the 128-bit register to read the new data when the four groups' operations have been overcome. Thus the 128-bit round-operating unit has been transformed into four 32-bit round-operating elements. The internal pipelining processing should be implemented during the whole nine intermediate Round Transformations of the four packets before achieving the 128-bit ciphertext. The process of the last round The final round is a 128-bit processor.

After nine rounds of operations included Shiftrows, SubByte and Mixclumns, the 128-bit intermediate encrypted data will be used in XOR operation with the final expanded key(4*32bit), which is provided by the key expansion module. The output of final round in the processor is the desired 128-bit ciphertext. Similarly, the ciphertext is divided into four packets of 32- bit data by an external enable signal. Key expansion and Key extraction This module is implemented basically the same with the traditional way as another part of the AES encryption algorithm. The only difference lies on the mode of data transmission. The initial key and expanded keys are divided into four 32-bit data before being extracted.

IV RESULTS

Simulation results

Rtl schematic

Timing report

Area report

V CONCLUSION:

A FPGA implementation of area-optimized AES algorithm which meets the actual application is proposed in this paper.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

After being coded with Verilog Hardware Description Language, the waveform simulation of the new algorithm was taken in the ModelSim SE PLUS 6.0 and Quartus Ċ 7.2 platform. Ultimately, a synthesis simulation of the new algorithm has been done. The result shows that the design with the pipelining technology and special data transmission mode can optimize the chip area effectively. Meanwhile, this design reduces power consumption to some extent, for the power consumption is directly related to the chip area. Therefore the encryption device implemented in this method can meet some practical applications. As the S-box is implemented by look-up-table in this design, the chip area and power can still be optimized. So the future work should focus on the implementation mode of S-box. Mathematics in Galois field (2^8) can accomplish the bytes substitution of the AES algorithm, which could be another idea of further research.

REFERENCES:

[1] J.Yang, J.Ding, N.Li and Y.X.Guo, "FPGA-based design and implementation of reduced AES algorithm" IEEE Inter.Conf. ChalEnvirSci Com Engin (CESCE).,Vol.02, Issue.5-6, pp.67-70, Jun 2010.

[2] A.M.Deshpande, M.S.Deshpande and D.N.Kayatanavar, "FPGA Implementation of AES Encryption and Decryption" IEEE Inter.Conf.Cont, Auto, Com, and Ener., vol.01,issue04, pp.1-6,Jun.2009.

[3] Hiremath.S. and Suma.M.S., "Advanced Encryption Standard Implemented on FPGA" IEEE Inter.Conf. Comp ElecEngin. (IECEE), vol.02 ,issue.28, pp.656-660, Dec.2009.

[4] Abdel-hafeez.S.,Sawalmeh.A. and Bataineh.S., "High Performance AES Design using Pipelining Structure over GF(28)" IEEE Inter Conf.Signal Proc and Com.,vol.24-27, pp.716-719,Nov. 2007.

[5] Rizk.M.R.M. and Morsy, M., "Optimized Area and Optimized Speed Hardware Implementations of AES on FPGA", IEEE Inter Conf. DesigTes Wor.,vol.1,issue.16,pp.207-217, Dec. 2007.

[6] Liberatori.M., Otero.F., Bonadero.J.C. and Castineira.J. "AES-128 Cipher. High Speed, Low Cost FPGA Implementation", IEEE Conf. Southern Programmable Logic (SPL), vol.04, issue.07, pp.195-198,Jun. 2007.

[7] Abdelhalim. M.B., Aslan.H.K. and Farouk.H. "A design for an FPGA based implementation of Rijndaelcipher", ITICT. EnaTechn N Kn Soc. (ETNKS), vol.5, issue.6, pp.897-912, Dec.2005.

Author's Details:

Dr. Arvind Kundu, He did B. Tech from H.P. University (SHIMLA) in Electronics & Communication. He did M. Tech from M.D. University (ROHTAK) in Electronics & Communication Engineering. He did Ph. D from Ranchi University and area of research is ADHOC Networks, EMBEDDED System, Cryptography, Message authentication Protocol, Image Processing, Routing protocol etc. He is working as HOD ECE Department at Scient Institute Of Technology, Ibrahimpatnam.

Mr.M.Suresh Kumar, He did B. Tech from Geetanjali institite of science and technology (JNTU Hyderabad) in Electronics & Communication. He did M. Tech from sri vidyanikethan engineering college (Autonomous), Tirupathi in Digital Electronics & Communication Systems. He is Currently working as **Assistant Profesor** ECE Department at Scient Institute Of Technology, Ibrahimpatnam.