Design and Implementation of Encryption System for Mobile Hard Disk

Si-ming He[1, a],Yong-hai Yu[2],Da-chuan Chen[1],Jing-quan Li[1]

[1]Aviation University of Air Force,130022,Changchun China

[2]Changchun University of Science and ,130600, Changchun China

[a]hsmfly1982@163.com

Keywords:hardware encryption;FPGA;AES;key;

Abstract. At present,in order to solve the data leakage of a hardware encryption system for mobile hard disk and the changing key that is not flexible,the hardware encryption system for mobile hard disk drive based on FPGA—AES system is designed and implemented.This method not only achieves the real-time encryption for the data of the mobile hard disk，but also modifies the key according to the need. Meanwhile,it can destroy the key after data encryption.Experimental results show this method improves the efficiency of data encryption,the security and the reliability.At last,making procedure take up general resource 50% by QuartusII 11.0 development tools enhances the resource utilization ratio.

Introduction

With the rapid development of information technology and digital society,it is an increasing needs of Information security storage,especially civil and criminal judicial investigation during which the proportion of forensic evidence is more and more big in electronic document forms,and how to solve the divulgence of secret data on mobile hard disk may be the one mostly concerned.Meanwhile,information security storage also has important significance in National defense and military and other special areas. However, at present, Most of the mobile hard disk use the algorithm of MD5,SHA-1and DES,but These algorithms have been decoded by experts at home and abroad and cann’t ensure data security,so most of the data on the hard disk is encrypted by using the software of AES encryption which bases on computer. Although AES disk algorithm is published in domestic or foreign journals, but the key is fixed in the hard disk—not only makes key change not agile but also gives data reveal certain risks once the data loss[1][2].In order to solve these problems,this article introduces an FPGA combined with USB interface,AES encryption technology and EDA technology,and designs the hardware encryption system for mobile hard disk drive based on FPGA. In addition, without using of computer hardware resource condition,it realizes data copy to a mobile hard disk real-time encryption.

In this paper,AES core module is analysed and designed emphatically.According to the needs,any key is changed in order to achieve effectively for hard disk data protection and this paper uses of QuartusII 11.0 software to program the line optimization.The overall design of mobile hard disk encryption system

The system mainly composed of the main modules of this system includes: the main control module, the AES algorithm module, the USB interface module, the ATA interface module, SRAM and the voltage conversion circuit[3][4][5].Block diagram of the system structure is as shown in Fig.1.

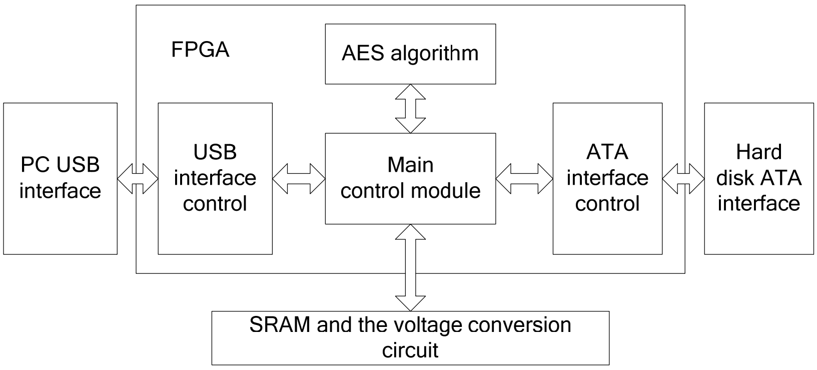


Fig.1 Block diagram of the system structure

To begin with, This system set up key.Furthermore, it through the USB port will transmit data to the FPGA.Meanwhile,according to the SEA algorithm, FPGA encrypt data.At last,it copy encrypted data to ATA hard disk interface. This design lays emphasis on the research of the AES algorithm module design,implementation and function,which bases on the peripheral conventional circuit platform.

The detailed design of AES algorithm module

This design uses 128 key algorithm. The core module of AES algorithm consistes of four parts as follows: key expansion module, subBytes module, shiftRows module and mixColumns module[5][6]. A 128 - bit data block complete a encryption process is as shown in Fig.2.

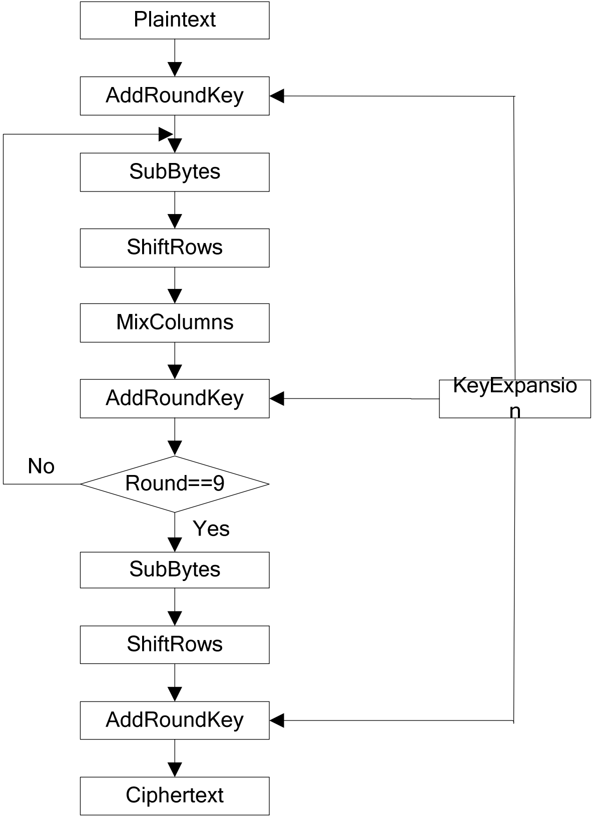


Fig.2 FPGA internal AES working principle

1. Key expansion module

The module employs Non-parallel extensions to expand the key in order to turn 128 key into 128 x 11 key sequence. It involves three kinds of operations—Subword,Rotword and Rcon and the array pointer arithmetic. It gets a new array Round_key[11] after full key extensions. Finally,this way gets the need of Addroundkey operation—Round_key. Top-Level Schematic of key expansion module is as shown in Fig.3.

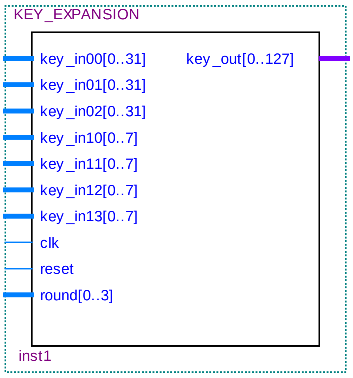


Fig.3 Top-Level Schematic of key expansion module

2. SubBytes module

This module functions as S box operation.It consistes of Limited domain of GF for multiplication inverse and polynomial multiplication.In order to reduce the operation complexity,speed up the execution ,improve performance , consider the FPGA chip structure characteristics and rich resources,this system for subBytes operation directly uses search S box.Firstly, 128 - bit data is as 16 bytes.Then,it looks up table so as to replace each byte.Finally,it gets a Aa group of new 128 bit data. Top-Level Schematic of subBytes module is as shown in Fig.4.

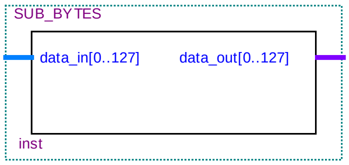


Fig.4 Top-Level Schematic of subBytes module

3. ShiftRows module

ShiftRows in state matrix carries out lateral displacement by row as the unit,but keeps on the first line. Firstly, The 128 bit data expresses as 16 bytes of 8 bits form.Then according to the listed subscript,this 16 bytes is arranged for a 4×4's matrixes.Finally, it transposes in accordance with the principle which is keep on the first line and last three rows respectively changes a place towards the right in circle. Top-Level Schematic of shiftRows module is as shown in Fig.5.

4. MixColumns module

MixColumns module carries out Limited domain of GF for multiplication inverse on every column. 128 - bit data is as a 4×4's byte matrixes. In each column of the matrix. Top-Level Schematic of mixColumns module is as shown in Fig.5.

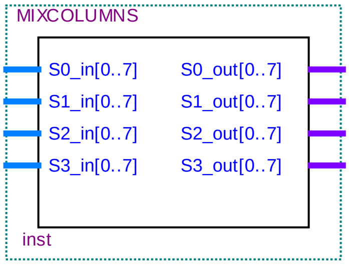


Fig.5 Top-Level Schematic of mixColumns moduleSimulation result

Techshine's E-PLAY-EP3C80 development board is selected as the system's FPGA hardware development platform because of CycloneⅢ series of FPGA has rich programmable resources,which chooses the EP3C80F484C8N chip of CycloneⅢ series and regards QuartusⅡ11.0 as System development tools in order to realize encryption function.

Design is finished in QuartusII 11.0 software environment and the circuit has carried out synthesis and the optimization on design.Firstly, The user settings mobile hard disk key by using key software,and copies plaintext to the mobile hard disk.Meanwhile, the mobile hard disk is pulled out after it encryptes plaintext according to the key.This makes the key lose so as to prevent leak problem because mobile hard disk is lost,stolen,waste,which enhances system security. Simulation result is as shown in Fig.6.

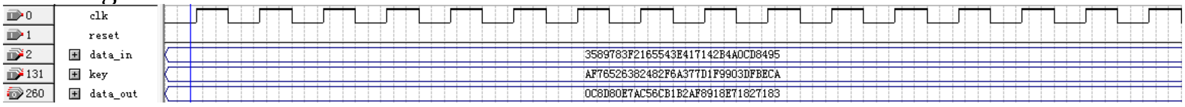

0
clk
1
reset
2
data_in
3589783F2165543E417142B4A0CD8495
131
key
AF76526382482F6A377D1F9903DFBECA
260
data_out
0C8D80E7AC56CB1B2AF8918E71827183

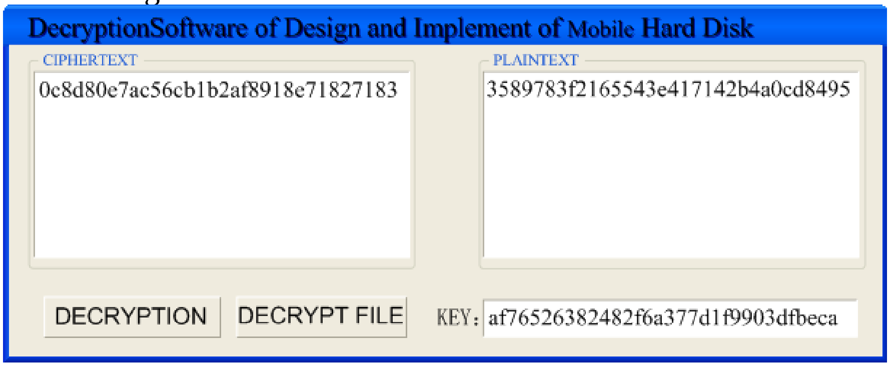
Fig.6 Imulation result of system function

Plaintext is“3589783f2165543e417142b4a0cd8495”

Key is“af76526382482f6a377d1f9903dfbeca”

Ciphertext is“0c8d80e7ac56cb1b2af8918e71827183”

In order to verify the correctness of the system function, using the decryption software does verification as shown in Fig.7.


DecryptionSoftware of Design and Implement of Mobile Hard Disk

CIPHERTEXT: 0c8d80e7ac56cb1b2af8918e71827183

PLAINTEXT: 3589783f2165543e417142b4a0cd8495

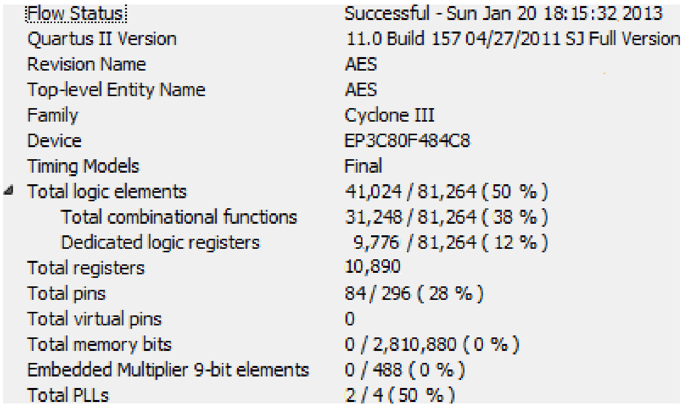
KEY: af76526382482f6a377d1f9903dfbeca

Fig.7 The decryption software

Basic on the above tests data has been analysed previously,the design of system function completely correct and correctly implement AES encryption algorithm. In addition,the execution of encryption and decryption algorithm is the advanced encryption standard AES algorithm.

Conclusions

Using QuartusII 11.0 in device displays the general result. The results show that it occupies 47541 logic cells that occupies 58% of the total logic resources.After using Synplify Pro comprehensive optimization, it occupies 41024 logic cells that occupies 50% of the total logic resources.This is as shown in Fig.8.Moreover,this improves the system overall safety and further provide reliable guarantee for safety storage of user data because the Key temporarily has been deposited in the FPGA.



Flow Status	Successful - Sun Jan 20 18:15:32 2013
Quartus II Version	11.0 Build 157 04/27/2011 SJ Full Version
Revision Name	AES
Top-level Entity Name	AES
Family	Cyclone III
Device	EP3C80F484C8
Timing Models	Final
Total logic elements	41,024 / 81,264 (50 %)
Total combinational functions	31,248 / 81,264 (38 %)
Dedicated logic registers	9,776 / 81,264 (12 %)
Total registers	10,890
Total pins	84 / 296 (28 %)
Total virtual pins	0
Total memory bits	0 / 2,810,880 (0 %)
Embedded Multiplier 9-bit elements	0 / 488 (0 %)
Total PLLs	2 / 4 (50 %)

Fig.8 Resources occupation summary

References

[1] Xiaoyun Wang,Dengguo Feng,Xuejia,Hongbo Yu.Collisions for Hash Functions MD4,MD5,HAVAL-128 and RIPEMD. International Journal of Network Security.2007.

[2] NIST,Federal Information Processing Standards Publication 197:Advanced Encryption Standard (AES). http:/ / csrc.nist.gov/ publications/ PubsFIPS.html .Nov 2001.

[3] Kailai Zhang. The design and implementation of hard disk encryption based on DES algorithm [D]. Sian : Northwestern Polytechnical University ; ,2003.

[4] Xinjia Zhang, Kailai Zhang. Design and implementation of hard disk data encryption based onFPGA chip [J]. Journal of Northwestern Polytechnical University,2004,(2):161- 165. [5] Kaer Huang. Implementation of FPGA AES encryption algorithm [D].Shanxi：North University of China. 2011.5. [6] Huang Yu-jung，Lin Y S，Hung K Y，et al.Efficient implementation of AES IP[C]//IEEE Asia-Pacific Conference on Circuits and Systems，2006.