TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol.12, No.4, April 2014, pp. 3001 ~ 3009
DOI: http://dx.doi.org/10.11591/telkomnika.v12i4.4995

Research on Design Method Based on Hardware Encryption and Two-way ID Authentication for Security Mobile Hard Disk

Huanchun Yang
School of Business, Wenzhou University, Wenzhou, China
email: yhchyhch@126.com

Abstract

The design Method of the "Security Mobile Hard Disk Based on Hardware Encryption and Two-way ID Authentication" adopts the smart card-based technology of two way ID authentication, thus enables higher authentication strength than ordinary password authentication and USB-KEY one way certification; adoption of dedicated hardware encryption chip on encrypting the hard disk data enhances the encryption speed; since this encryption is a hardware level encryption, it is completely transparent to users, and do not rely on the operating system or other applications, with almost no impact on system performance; that the key of the encryption system will be loaded before the system initialization (system boot) prevents malicious code attacks from hard drive, and even when the mobile hard disk was stolen, the thief cannot read out any encrypted data from it on any other computer as long as the thief has no access to the encryption key. Therefore, this "encrypted mobile hard disk" is more secure with better reading and writing performance, and thus can effectively protect Important and sensitive data on the mobile hard disk.

Keywords*: secure mobile hard disk, hardware encryption, two-way ID authentication, mobile hard disk*

1. Introduction

As mobile mass storage is widely used and popularized, mobile hard disk is becoming the commonly-used tools among the government, enterprises and individuals; when people enjoy the convenience brought by mobile storage devices, they also suffer from the problem of data leakage followed by theft of the devices. According to a survey, 60% of the enterprises and institutions get victimized in cases of theft of mobile storage devices. Surveys from U.S. Federal Bureau of Investigation (FBI) and Computer Security Organizations (CSI) also show that businesses and government agencies suffer more losses in cases of theft of important information than those caused by virus infection and hacker attacks, and more than 80% of security threats come from inside. China National Information Security Testing Evaluation and Certification Center displayed in its survey that the security issues of sensitive data mainly derive from disclosure and crimes, rather than the virus and external hackers.

In use of mobile hard disk, if sensitive data are stored in clear text, theft of the device will directly cause disclosure of important documents. In addition, due to incomplete removal of files, temporary data cache, disk fragmentation and other operations in use of mobile hard disk, the media will have a lot of residual data, which will indirectly incur leakage problem if data recovery techniques are adopted to obtain the user's sensitive information from the residual data. Moreover, tampering of data users by illegal users is also a major threat to data security.

Therefore, to ensure security of the data storage medium, it is necessary to introduce data storage security-related technologies such as ID authentication, data encryption and data integrity verification to research and design for two-way ID authentication and hardware encryption-based secure mobile hard disk.

2. Research Status

The following related materials have been sorted out from domestic and foreign documents as well as resources on the Internet:

The voice and graphic digital mobile hard disk (Patent) put forward a mobile hard disk

Received September 18, 2013; Revised November 17, 2013; Accepted December 1, 2013

allowing only reading and disabling functions of copy or editing clear text without permission, the essential point of which is access control. The invention introduced particular type of encryption chip between IDE interface and hard disk for interactive data encryption and decryption. The encryption chip subjects to Serial Port Communication Protocol of smart card, with a slow encryption speed and relies on operating system and file unit to encrypt data. Also, security risk remains as the key resides in memory.

The encrypted removable storage devices and their data access method (Patent) published a method of mobile memory device along with its data storage method based on hardware encryption. The storage media is restricted to FLASH with key information stored in the device, likely to cause key enclosure. Meanwhile, safety performance remains low since user passwords are directly used for data encryption.

Hardware encryption system for mobile storage devices (Thesis by Tianjin Polytechnic University) designed an embedded encryption system between PC and USB disk that the key is stored in smart card. The key encrypts data when writing disk and decrypts data when reading disk under the control of pre-installed hardware encryption and decryption algorithm. It chose symmetric key DES algorithm and designed Triple DES for higher security concern and as for hardware architecture, it chose TMS32OVC54XDSP as CPU which performs relatively well in both calculation and control. CH375 chip, as the main-control chip for communication with USB port, implements features for communication and encryption. When system processes keys, random sequence generator produces random keys, stored when IC card is initialized, and used as keys to the encryption platform via card reader circuit.

Thesis USB data storage encryption technology based on FPGA and DM by Shanghai Jiao Tong University designed a highly efficient encryption and decryption system with USB port based on MEMS strong link, USB controller and FPGA, using AES encryption algorithm of physical certification and hardware implementation. Normal IDE hard drives become encrypted USB hard drives of strong security after connecting to the system, with an average data processing rate closed to normal USB, reaching 10MB/s.

Tianjin Agricultural University studied a design applying permutation code to encrypted USB hard drive system, proposing to improve data encryption and decryption speed by specialized feature units designed by Maxplus II from ALTERA. In this way it solved speed bottleneck of encryption and decryption during data transmission and created a high transmitting speed USB hard drive system that supports encryption.

NetDisk Mini of Ximeta controls access in drivers to memory by requiring users to enter passwords. Besides, the internal small server also contributes to making low-cost NAS solution possible. Clients in networks are able to access data in mobile hard disk through password when adding Ethernet connection ports.

BenQDP361 is a portable encrypted hard disk which adopts latest chip encryption technology that separates encryption algorithm from password. That is to say, password will not be stolen even if the hard disk has been lost. No one knows information stored in the hard drive except the user.

CendaC803 mobile HDD with fingerprint encryption adopts live fingerprint recognition and AES-256 bit encryption that supports 10 different finger prints. Data is protected by examining unique finger prints to confirm identity. EagetE810 has embedded the most updated AES-256 encryption algorithm as well. Travelstar's encrypted mobile HDD, adopts hardware encryption key with unknown explanation. There are also other types of encrypted mobile hard disk.

All in all, the conclusion is that research regarding mobile hard disk encryption has made achievements in the world today along with corresponding products, yet no disk among which adopts both strong authentication algorithms and encryption algorithms.

3. Scheme Design

The "encrypted mobile hard disk" in this paper took FPGA (PLD) as the core processing components, selected cipher units including SCB-2 algorithm ASIC chips certified by the State Encryption Administration, adopted smart cards with safe computing to achieve the key storage and ID authentication, and chose USB2.0 analog transceiver for designing the USB physical layer protocol. Among all, FPGA chip is the control center of this "encrypted mobile hard disk." The design block diagram is shown in Figure 1.

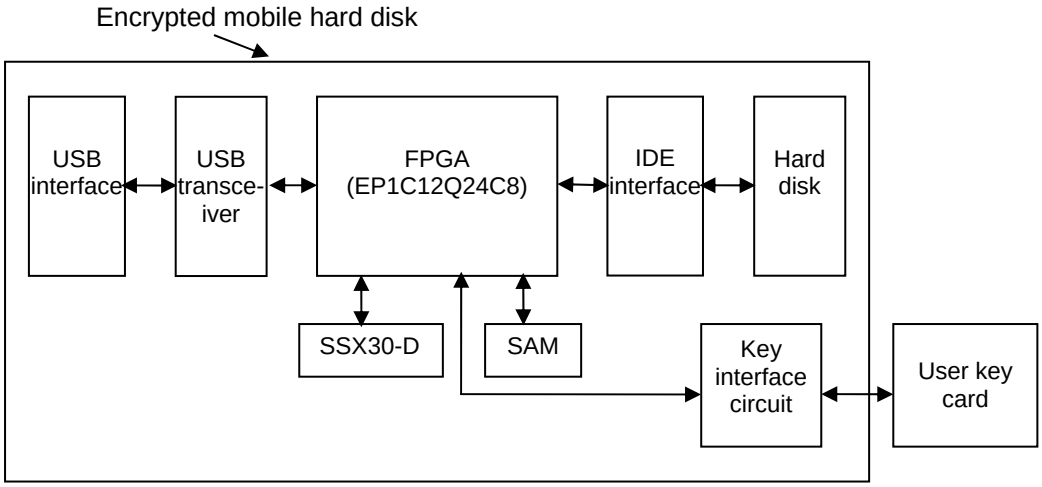

Figure 1. The Design Block Diagram of the Encrypted Mobile Hard

3.1. USB Transceiver

As the analog front-end of USB2.0, USB transceiver unit is used for NRZI encoding/decoding of differential signal, bit manipulation and serial-parallel conversion, complying with UTMI specification. The transceiver can use the readily available analog transceiver chip of USB 2.0.

3.2. FPGA

FPGA is mainly used to achieve the following functions:

First, control the mutual authentication between user key card and the SAM card.

After the mutual authentication between the user key card and SAM card is done, FPGA will obtain the key material from the user key card through cipher text, and then the SAM card will make calculations with the key material to produce the working key for SCB2 algorithm in decrypting mobile hard disk data.

Then, it receives the parallel data sent by USB transceiver and classifies data into “to be encrypted" and "not to be encrypted". Those data to be encrypted will be sent to SSX30-D and get encrypted through SSX30-D, while those data not to be encrypted will just get through.

In accordance with the commands received from USB, it will send commands to hard disk to read or write. All reading and writing operations on the hard drive follow the ATA specification.

Data read out by the hard drive will be classified into “to be decrypted" and "not to be decrypted". Those data to be decrypted will be sent to SSX30-D and get decrypted through SSX30-D, while those data not to be decrypted will just get through.

3.3. SSX30-D

SSX30-D, as certified by the State Encryption Administration, is a chip of high-performance block cipher algorithm, which implements the SCB2 cryptographic algorithms. The cipher block length is 128 bits with 128-bit key length. SSX30-D includes multiple operating modes such as ECB, CBC and OFB and two working means as "single-bus" and "dual bus." In the ECB mode and dual bus operation, the encryption and decryption rates up to 1.4Gbps. In the "encrypted mobile hard disk", ECB operation mode and dual bus means are adopted.

3.4. SAM

SAM is realized with the smart card authenticated by State Encryption Administration. It is adopted to complete the mutual authentication between "encrypted mobile hard disk" and the user key card, and to obtain the key material in user key card for computing the working key with SCB2 algorithm.

3.5. User Key Card

User key card is realized through the smart card approved by the State Encryption

Administration, mainly used to store the key material which is to generate the working key under SCB2 cryptographic algorithm. In order to prevent an intruder from stealing the key material, this design realized mutual authentication between user key card and SAM in “encrypted mobile hard disk".

4. Module Design

Module design of the "encrypted mobile hard disk" is shown in Figure 2.

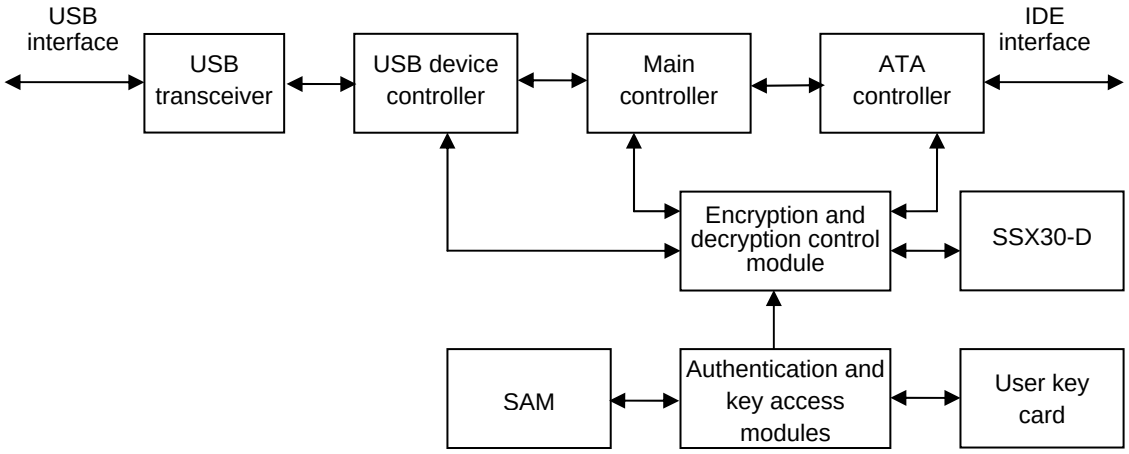

Figure 2. The Module Design Diagram of the Encrypted Mobile Hard Disk

4.1. Authentication and Key Access Modules

Authentication and key access modules take charge of the mutual authentication between user key card and "encrypted mobile hard disk". After authentication is through, authentication and key access modules will obtain key material from under key card through cipher and then apply SAT to generate the working key for hard disk data encryption and decryption with SCB2 algorithm. Figure 3 and 4 show the process of ID authentication and key access.

4.2. USB Transceiver Module

They readily available USB physical layer transceiver is used to receive the serial data from USB interface, and after serial-parallel conversion these data will be sent to USB device controller module while USB bus state will also be sent to USB device controller module and the parallel data thus get serialized and driven to USB interface.

4.3. USB Device Controller Module

USB device controller module is achieved through VHDL language hardening. It receives parallel data and bus state from the USB transceiver module, writes the data packet of transmission control into the control endpoint buffer module, and sends the request of control output break to the main controller module; the bulk transmission data packet will be written into bulk endpoint buffer module and sent the request of batch output break to the main controller module.

USB device controller module receives the request of control input break from the main controller module, reads out data from control endpoint buffer module, and forwards it to the USB transceiver module; it also receives the request of batch input break from the main controller module, reads out data from bulk endpoint buffer module, and forwards to the USB transceiver module. Figure 5 displays the structure of this device controller.

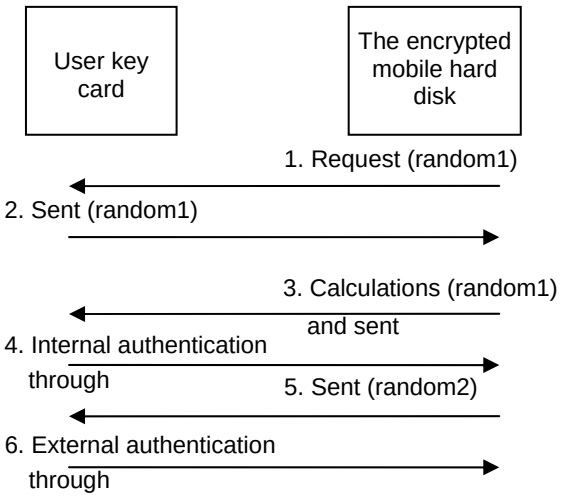

Figure 3. The Process of Two-way ID Authentication

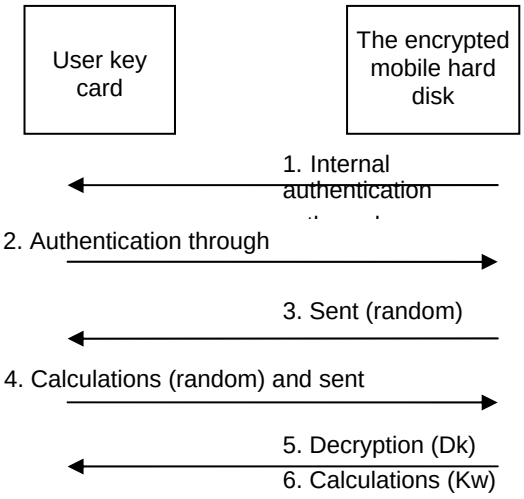

Figure 4. The Process of Key Access

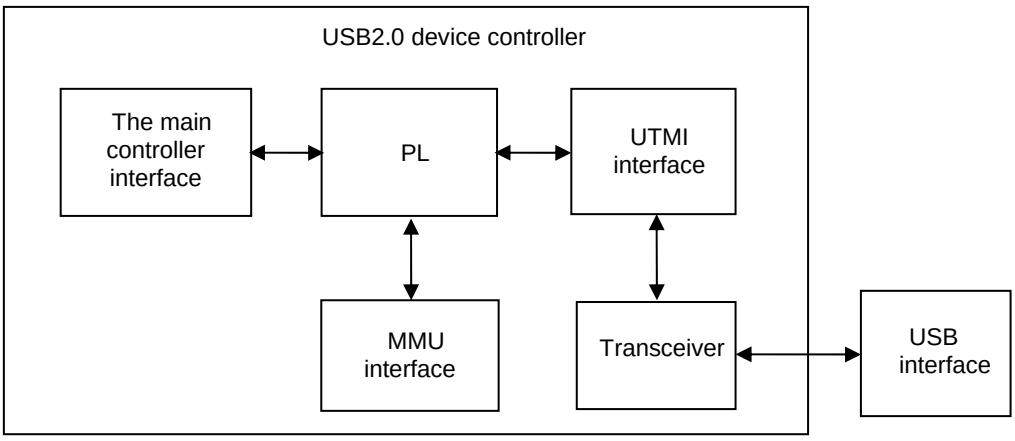

Figure 5. The Structure of USB Device Controller

4.4. Main Controller Module

Main controller module is realized through VHDL language hardening. It receives the request of control break from the USB device controller module, reads out the order packet or data packet from control endpoint buffer area, and then writes the response data of transmission control order into control endpoint buffer zone based on the type of command in the order packet, and sends the request of control input break to the USB device controller.

Main controller module receives the request of batch output break from USB device controller module, writes the ATA transmission order parameters into ATA controller module, writes the working parameters of encryption and decryption into the decryption and encryption control module, writes the response date of batch transmission order from ATA controller module or encryption and decryption module into the batch endpoint buffer module, and sends the request of batch input break to USB device controller module, or directly forwards the output data packet to encryption and decryption controller module.

Main controller module receives the status information from encryption and decryption control module, allowing or prohibiting the reading or writing operations on the encryption and decryption control module from main controller module and ATA controller module. Figure 6 displays main controller module working process.

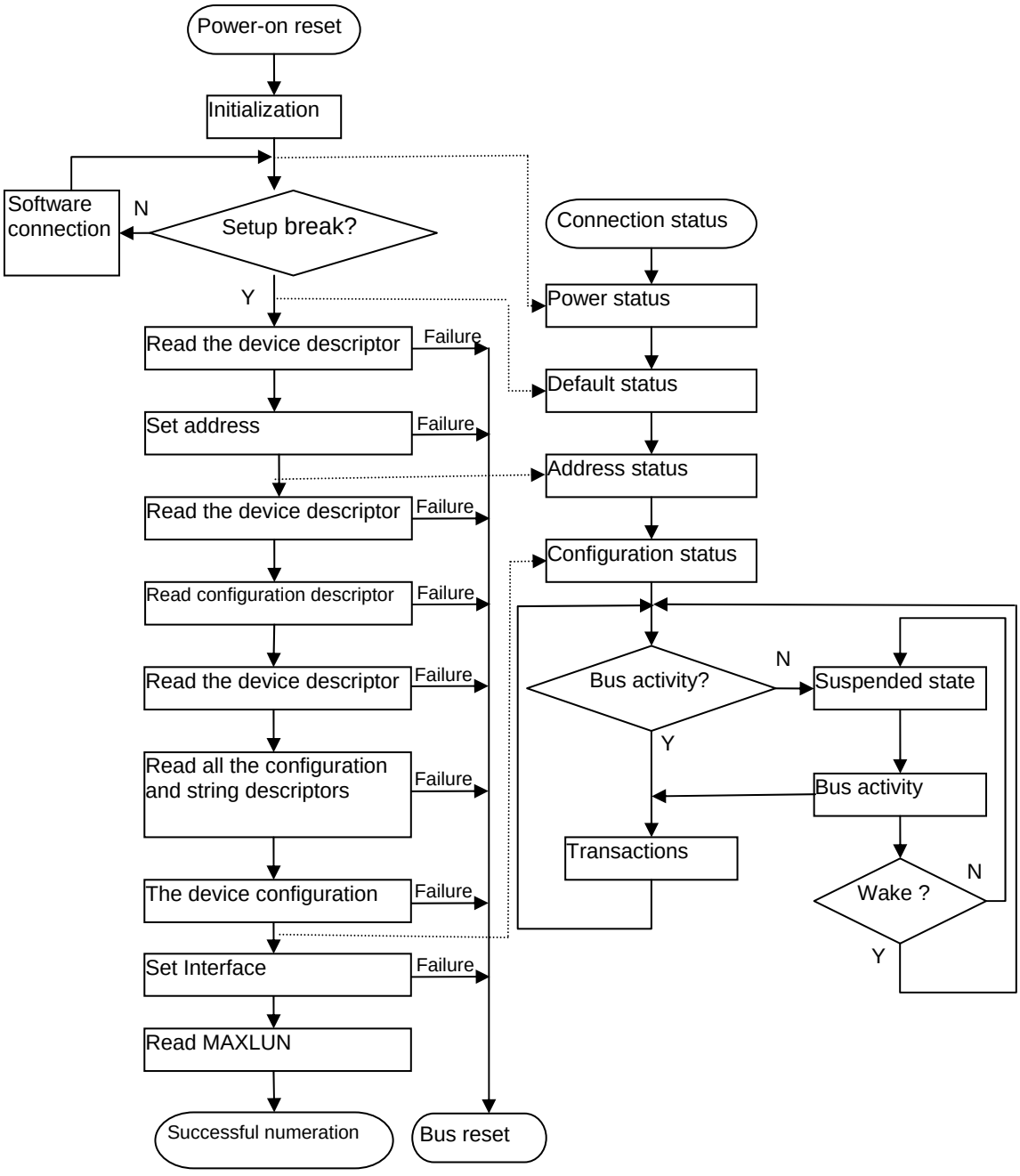

Figure 6. Main Controller Module Working Process

4.5. Encryption and Decryption Control Module

Encryption and decryption control module is realized through VHDL language description. It receives working key material from key access module and working parameters of encryption and decryption from main controller; it receives the output data packet from main controller, generates the write control signal for SSX30-D chip, writes the data into SSX30-D chip through SSX30-D host bus to get them encrypted, and after SSSX30-D chip finishes data encryption, the encryption and decryption control module will produce the read control signal for SSX30-D chip, thus the encrypted results will be read and driven to the ATA controller module; it receives the input data packet from ATA controller module, generates the write control signal for SSX30-D chip, writes the data isolated through IDE interface module into SSX30-D chip through SSX30-D host bus to get the data decrypted, and after SSX30-D chip completes data

decryption, the read control signal for SSX30-D chip will be generated by encryption and decryption module and the decryption results will be read out and driven to main controller module together with the status of encryption and decryption control module. Figure 7 and figure 8 separately show the working process of encryption and decryption module.

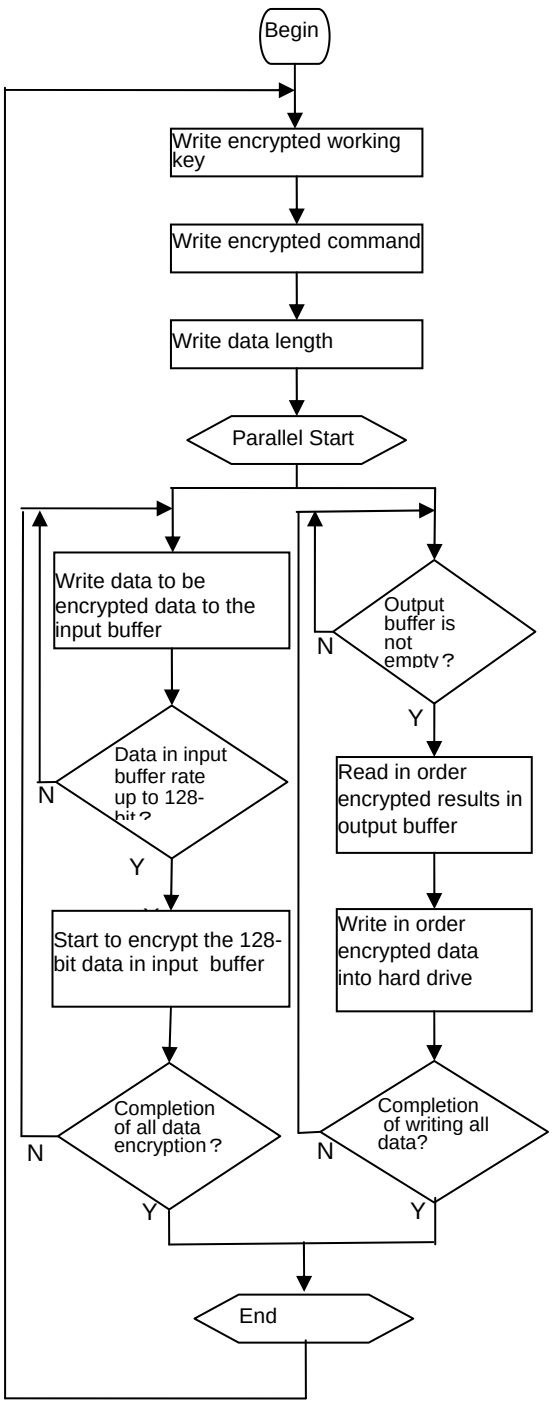

Figure 7. The Working Process of encryption

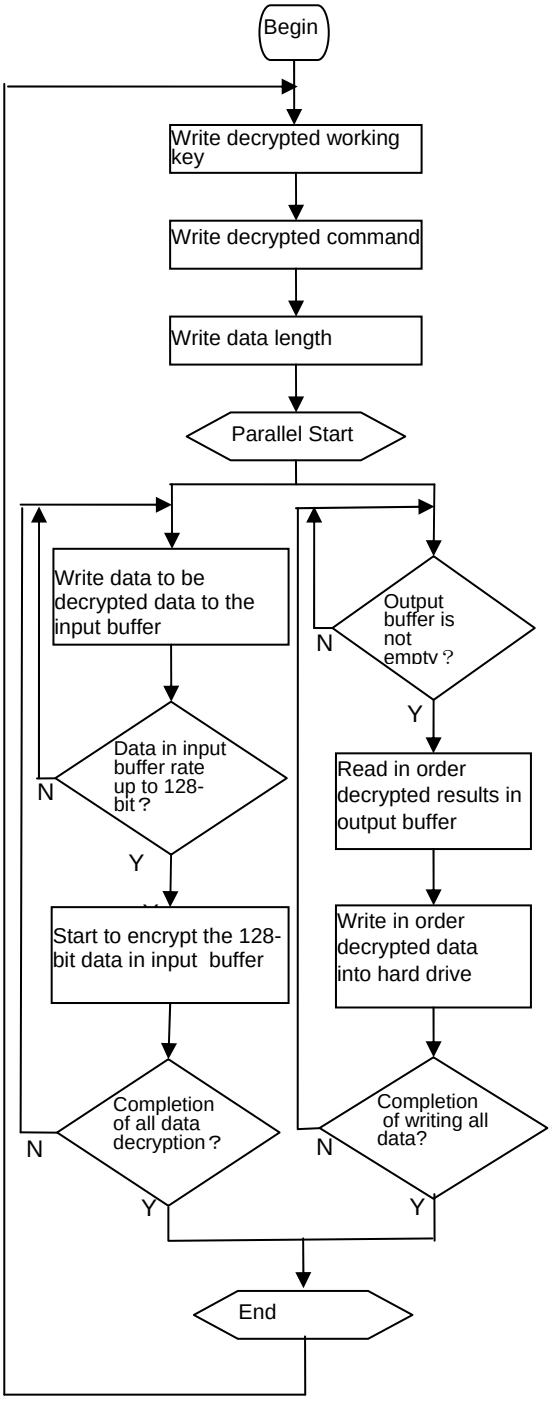

Figure 8. The Working Process of Decryption

4.6. SSX30-D Chip

SSX30-D chip is a crypt chip certified by the State Encryption Administration, which

enables that the SCB2 cryptographic algorithm can encrypt and decrypt the data to be encrypted or decrypted as parsed out by main controller module under the control of encryption and decryption control module.

4.7. ATA Controller Module

ATA controller module is realized through VHDL language description. It receives the parameter block of ATA transmission commands from main controller module, and writes them into the register group of ATA memory through the IDE interface; in accordance with ATA protocol it directly sends ATA memory parameter information from IDE interface to main controller module, and sends input data packet from IDE interface to the unit of encryption and decryption. ATA controller supports both PIO and UDMA transmission modes, and since it is of a higher degree of design complexity, the state machine is thus proposed to describe the timing as specified by ATA protocol.

5. Development Trend

5.1. Security Encryption Becomes Inevitable

Storage providers always aim to offer uses professional, secure and stable storage solutions. With the increasing data amount and its booming importance, data security has become one of the essential criteria when consumers backup data. However, software encryption mode no longer satisfies market demand. Hard ware encryption becomes users' first option such as Eaget'sE906 chip encryption and Lenovo's F117 fingerprint encryption in the sense that data remains under protection even if the hard disk storing it is lost. Consumers need not to worry about the disclosure of data or that being stolen. Encryption technology will become an inevitable trend of mobile hard disk development for sure!

5.2. B. Hardware Encryption is the Only Approach to Breaking Speed Bottleneck of Encryption and Decryption

Although software encryption is far more flexible, it is also more complicated. If implemented by CPU, the method will use lots of CPU capacity; if adopting coprocessor, CPU will then be able to deal with other applications but its capacity will still be hampered due to the occupied bus during data transmission between coprocessor and main memory. Embedded CPU inside portable hard drive controller for encryption can reduce CPU usage impressively albeit this method requires highly proficient embedded processor, thus increasing the cost. Encryption algorithm using FPGA or ASIC with data stream processing features eschews drawbacks of the above implementation approaches. Hardware encryption, with high security as well as high speed, is the only path to unblocking speed bottleneck of encryption and decryption.

5.3. Key Safety is more Significant than Cryptographic Algorithms

Most modern cryptographic algorithms are based on particular math problems for data encryption protections. Nevertheless, advanced applications of encryption algorithms all require algorithms to go public such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES). Hence, the safety of cryptographic algorithms relies more and more on that of keys instead of that of the algorithms. Encrypted keys should be stored for safety issues and random number generator is used to generate the master encryption key. In addition, advanced identification algorithm will verify the legitimacy of users.

6. Conclusion

In this study, centered on CYCLONE chip series (by Altera Corporation) and applied with a specialized crypt algorithm chip approved certified by the State Encryption Administration, a mobile hard disk with two-way ID authentication and hardware encryption technology is designed and characterized with higher safety, higher performance and better transparency. In addition, the "encrypted mobile hard disk" adopts the low-end FPGA products of CYCLONE chip series, so it has lower cost and better price-performance ratio and good market prospects. Therefore, the "encrypted mobile hard disk" can be widely applied to government agencies, enterprises and individual users who have urgent needs for safe mobile storage.

References

[1] Freescale. MPC8260 IDMA Timing Diagrams. 2006; Rev.4: 07.
[2] Wu Zhendong, Chen Lin. Research on Use Control of Mobile Storage Devices. *Communications Technology.* 2008; 05: 142-144.
[3] Cao Xiaoli. Based on DES Encryption Algorithm. *Computer Knowledge and Technology*. 2011; 02: 295-296.
[4] Huang Shengchun, Xi Yong, Wei Jibo, Zhao Haitao. MPC8260 and FPGA-based DMA Interface Design. *Microcontrollers and Embedded Systems*. 2007; 09: 23-26.
[5] Yang Dong, Xie Yongqiang. A Public Key System-based Mutual Authentication and Key Agreement Scheme. *Network & Computer Security*. 2008; 01: 25-28.
[6] Xia Shuhua. DES and RSA encryption algorithm based on the data security transmission technology research. *Manufacturing Automation*. 2011; 02: 180-182.
[7] Yang Xiaoming. Hybrid Based on DES and RSA Encryption Algorithm. *Computer Study*. 2011; 1: 2-3.
[8] Qiu Huimin, Yang Yixian, Hu Zhengming. A New Smart Card-based Scheme Design of Two-way ID Authentication. *Application Research of Computers*. 2005; 12: 103-105.
[9] Hu Wei, Mu Dejun, Liu Hang, et al. Design and Realization of Hardware Encryption in Mobile Hard Disk. *Computer Engineering and Applications*. 2010; 22: 62-64.
[10] Wu Dianshuang, Liu Hang, He Dequan. Design and Realization of Encrypted Solid-state Disk in Integrated Hardware Encryption. *Computer Measurement & Control*. 2009; 17: 951-957.
[11] Jia Ling. Research and Implementation of Cryptographic system in software and hardware. *Computer Programming skills and Maintenance*. 2010; 14: 132-133.
[12] Wang Qingbin, Chen Shaozhen. Broadcast encryption scheme with constant-size public key and private key. *Journal on Communications*. 2011; 02: 114-119.
[13] Jinhui Sun, Geng Zhao, Xufei Li. An Improved Public Key Encryption Algorithm Based on Chebyshev Polynomials. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2013; 11(2): 864-870.
[14] Xiaoqiang Guo, Shuai Zhang, Ying Li. Key Technologies and Applications of Secure Multiparty Computation. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2013; 11(7): 3774-3779.