2002 International Computer Symposium(ICS2002)
Workshop on Computer Systems

Title: New architecture for Java Card :Utilizing Pure Java CPU and MRAM

Abstract

One year ago, we proposed a Java Card architecture named JavaCard1.1.In this implementation, we found the performance of JavaCard1.1 is not very well because of the interpreter of JCVM[1] and endurance of Flash is not enough to conquer great demand of multi-applications. We also realized that JavaCard1.1 is not secure with just random number generator (RNG).We reconsider these problems to propose new Java Card architecture(named Jixco). Jixco uses pure Java CPU to increase performance and substitutes MRAM for Flash to solve sector-write restriction. Besides, we incorporate cryptography modules including RSA, DES and AES in Jixco for security reason.

Name :*Chi-Hyi Peng*
Affiliation:*Industrial Technology Research Institute*
Computer & Communications Research Laboratories
Address:*X300,CCL/ITRI*
Bldg. 51, 195-11 Sec. 4, Chung Hsing Rd.Chutung, Hsinchu, Taiwan 310, R.O.C.
Email: ekhan@itri.org.tw
Phone :*(03)5914628*
Fax:*(03)5820234*

Name :*Shau-Yin Tseng*
Affiliation:*Industrial Technology Research Institute*
Computer & Communications Research Laboratories
Address:*X300,CCL/ITRI*
Bldg. 51, 195-11 Sec. 4, Chung Hsing Rd.Chutung, Hsinchu, Taiwan 310, R.O.C.
Email:tseng@itri.org.tw
Phone :*(03)5915670*
Fax:*(03)5820234*

Contact Author: Chi-Hyi Peng

Keyword: Smart Card, Java Card, Java Card Virtual Machine : JCVM, MRAM,RSA,AES,DES

New architecture for Java Card : Utilizing Pure Java CPU and MRAM

Abstract

One year ago, we proposed a Java Card architecture named JavaCard1.1.In this implementation, we found the performance of JavaCard1.1 is not very well because of the interpreter of JCVM[1] and endurance of Flash is not enough to conquer great demand of multi-applications. We also realized that JavaCard1.1 is not secure with just random number generator (RNG).We reconsider these problems to propose new Java Card architecture(named Jixco). Jixco uses pure Java CPU to increase performance and substitutes MRAM for Flash to solve sector-write restriction. Besides, we incorporate cryptography modules including RSA, DES and AES in Jixco for security reason.

1.Introduction

As the prosperity of internet, e-commerce becomes more and more popular. E-commerce model has evolved from the traditional face-to-face in store transaction to the on-line transaction. Therefore, information security is very important. A smart card is a type of solution to the security problems. Basing on the security, VISA international organization is now in the process of changing magnetic card as smart card to prevent the fraud.

Because of the portable and secure characters, smart card is not only paying conveniently, but also applies to the life widely, such as campus card, tour card, the highway fee card and passport, etc. Mainland of China plan to popularize smart card to finance, traffic, communication, medical treatment, education, identity and government administration etc. service.

People do not bring a pile of smart cards to cope different applications will be a trend. A multi-applications smart card can be a e-purse, passport and identity authentication. As more and more applications are stored in smart card, it is serious issue to guarantee information security.

As we know, for the past few years, many new attack methods to smart card are published. These attack skills are more and more clever, even with low price facility and a little information, the code of system would be easily broken through. How to protect private data of cardholder and how to establish security mechanism is great important.

In recent two years, we devote on multi-applications and security mechanism of the Java Card technology. From implementing JavaCard1.1, we found some problems including performance, sector-write restriction of Flash and security. Therefore we propose new Java Card architecture named Jixco to solve these problems. In this paper, we will introduce Jixco hardware architecture. The next section we describe

some evaluation of Jixco design.We will introduce Jixco hardware architecture in more detail in section 3.Finally, we make a conclusion and find a way for future researches .

2.Evaluation of Jixco design

From previous description, we know there are three problems existing in JavaCard1.1. According to these problems, we propose some evaluation of Jixco design which describe following：

1. Do we need pure Java CPU?
2. Is MRAM suitable to substitute Flash?
3. Establishing security mechanism of Jixco

2.1 Pure Java CPU

Generally, there are three ways to implement Java Card Virtual Machine(JCVM). The first and perhaps the most commonly used way is to interpret the bytecodes[2][3][4][5][6].The advantage of interpreters is simple to build but cause poor performance. Secondly, and more recently, there has been growing interest to develop hardware runtime support, such as Java CPU, to execute the bytecodes. Many studies have focused on enhancing each of the bytecode execution techniques, for

example, Java accelerator. The benefit of Java accelerator is the efficiency of execution bytecodes. However, the complex to design accelerator and the relevance of system software and experimental platform are expected. Basically, the Java accelerator is developed in hardware to support to perform all but the most complex Java bytecode. For the reason of complexity the third way is Java accelerator executes the simpler bytecodes and VM interpreter executes the more complex bytecodes.

In the consideration of complexity, JavaCard1.1 adopted the third way. The CPU of JavaCard1.1 with instruction sets including 185 JVCM 2.1.1 bytecodes and 60 native codes is accomplished. In this CPU instruction sets, 66 more complex bytecodes of 185 JVCM bytecodes are complied by 60 native codes. When executing the complex bytecodes, the CPU draws a software interrupt and jumps to the related complex instruction interrupt service routines to execute. The correlation of system software such as JCVM and JCOS are improved in[7]. The performance from the Java Card CPU is increasing but not very well because of many complex bytecodes and the related service routines.

To go a step further, we consider to design a pure Java CPU called Cix CPU with Java-only instruction sets for reducing execution time compared with that stated above.

2.2 MRAM

Current smart cards commonly use EEPROM or Flash to store applications. But general EEPROM or Flash has problem of Page-Write restriction, namely endurance problem. For instance, Flash of JavaCard1.1 is offered with a guaranteed Page-Write endurance of 20,000 cycles. It means any byte of Flash can typically be written to in excess of 20,000 times. If exceeding the amount, it is possibly damage.

In the future a more functional smart card is trend mainstream, namely a piece of smart card must store many types of application. Once Flash is written more than 20,000 times, smart card may be abnormal and cause executive error, even result smart card broken.

According to JavaCard1.1 banking application, Flash would be written more than hundred times in a simple execution of transaction. Once smart card function is expanded, this will be a great problem. From reports[8][9] showed, include Infineon the manufacturer of smart card also found that Java Card runtime environment need huge amount of demand to access EEPROM. Therefore, MRAM which has typical endurance of 10^{10} cycles can be thought to solve the endurance problem.

2.3 Security Mechanism

Because of the portable and secure characters, smart card gradually substitutes for magnetic stripe card. Unfortunately, For the past few years many new types of methods to attack smart card are published[10], such as single power analysis(SPA), differential power analysis(DPA), radiation, power consumption, power peak, and execution run time ,etc low price facility and little information can attack smart card.

Basing on the thought of security, JavaCard1.1 designed random number generator (RNG) that generate regular random number to prevent systematic attack. However, because attack skills develop rapidly, the security mechanism of JavaCard1.1 is not enough to prevent attacks. It is necessary to enhance security technology of JavaCard1.1.Recently, we have developed successfully cryptography modules of RSA,AES and DES. Therefore we will incorporate these modules in Jixco to establish security machanism.

3. Jixco architecture

The concepts of Jixco design mainly reference evaluation stated in section 2 and we propose the improvement to enhance operation efficiency and security mechanism. The block diagrams of Jixco as Figure 1 shown contain MMU (Memory Management Unit), pure Java CPU called Cix, single type memory (MRAM),7816IO,timer,security circuit, random number generator(RNG) and interrupt controller(INTC).Jixco also

incorporates accelerator of RSA,AES and DES.

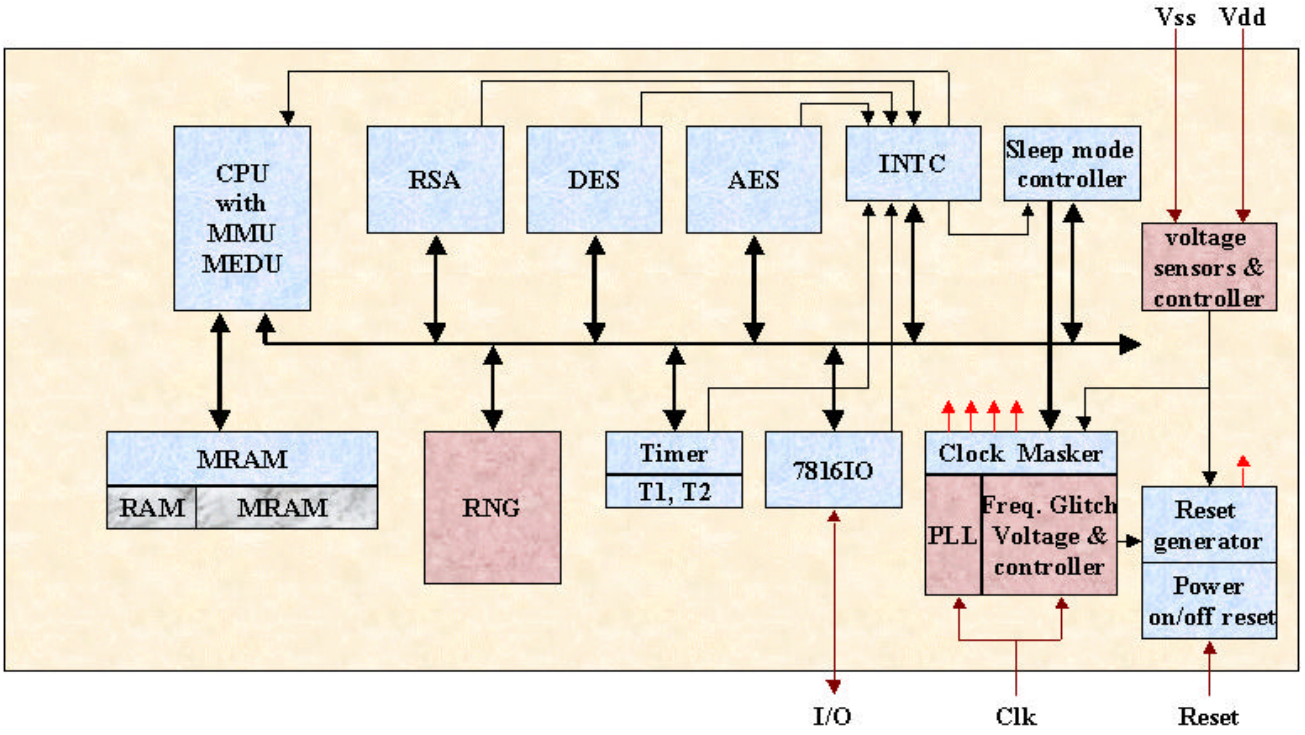

Figure 1：Jixco hardware architecture

Cix CPU：The designs specially for Java Card. It uses 32-bit Cix CPU and supports 185 javacard bytecodes definited by JCVM 2.1.1. The hardware can not only directly execute 176 instructions, but also execute firmware combined from above instructions to accomplish another 9 complex instructions. From memory encryption and decryption unit(MEDU), Cix CPU can access memory. Also, when Cix CPU access memory, it must be across from hardware firewall. This mechanism is design for security. For detail information of Cix CPU design, please reference[11]. Cix CPU has the following features:

- Support 185 JCVM 2.1.1 javacard bytecodes
- 32-bit CPU

- 64KB memory
- Firewall
- Encryption and Decryption Unit
- CISC architecture

Memory：Generally, smart card contains RAM, EEPROM and ROM three kinds of memory. Generally, ROM stores operating system, JavaCard runtime environment [12] and JavaCard interface application [13] etc. EEPROM is used for the permanent data managemt. SRAM is mainly used for variables of the mask and input/output buffer. For research and development convenience, Jixco has only one kind of MRAM which has 64KB capacity. MRAM is also belong to non-volatility memory which is the same with EEPROM. The device offers access times to 100 ns and it has 10^{10} times endurance. This 64KB memory is divided into two areas：First area contains 6Kbyte of memory which is used for executing real time application and mainly offered for Java Stack, encryption ,decryption units and peripherals of system. Among of this memory, 1KB is arranged for real time access of encrypting and decrypting, 1.75KB is arranged for Java Stack and Transient Object, 128B is for peripherals of system and special immediate address of JCVM, 64B is for interrupt table which can contain about 32 interrupts. Second area with 58Kbyte of memory is designed for storing permanent applications. For example it is provided for storing

JavaCard system environment (include JCRE,JCVM and JCOS) and applets.

Cix CPU also includes 6KB of internal ROM to store BOOT program, interrupt service routine, Complex Instruction routine and Java Exception Handler routine. External memory has 64KB immediately address and Internal ROM has 6KB immediately address. Also External RAM overlap internal ROM..Jixco memory map is shown figure 2 .

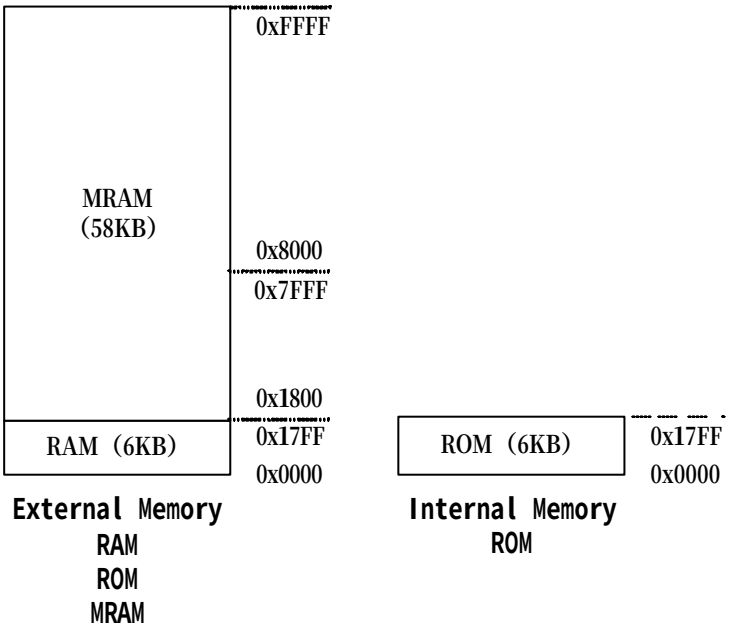

Figure 2：Jixco memory map。

7816IO：7816IO module is an important IO interface which is intednded for information exchange negotiated between Jixco and Card Reader. The interface mainly support T=0 and T=1 protocols definited from ISO7816.T=0 protocol transmit Character;T=1 protocol transmit Block.

Timer：Jixco contains two programmable Timers (Timer 1 & Timer 0)in order to supervise if internal application is suitable executing and suitable communicate with

system outside. Generally, a timer will be watchdog timer to supervise operation of system and monitor if application accurately execute. At certain time watchdog timer would generate a interrupt signal, than interrupt service routine checks program counter of stack to monitor if application execute within the allowable scope. When service routine has problem, it will let smart card enter pause status and suspend all the operation of chip. When reset signal is started, pause status would break away.

DES accelerator engine：DES accelerator engine supports DATA ENCRYPTION STANDARD [14] of the symmetrical cryptography algorithm which use 64-bits secret key. From secret key ,every 64-bits plaintext would encrypt as 64-bits ciphertext. DES can accomplish cryptography operation within only 16 clocks and if combining some software, it can support triple DES cryptography operation.

AES accelerator engine：AES accelerator engine supports ADVANCED ENCRYPTION STANDARD [15] of the symmetrical cryptography algorithm which use 128-bits secret key. From secret key ,every 128-bits plaintext would encrypt as 128-bits ciphertext. AES can accomplish encryption operation within only 21 clocks and decryption operation within 32 clocks. The most important character of AES accelerator engine is encryption and decryption system are incorporate in the same hardware module. Please reference[16] for detail design of AES accelerator engine.

RSA accelerator engine：RSA accelerator engine supports public key cryptosystem.

The system is mainly exponential operation and it means modular multiplication. Also , modular multiplication is design from concept of Montgomery algorithm. Right now RSA accelerator engine can support to 1024-bits and within just 0.5 second ,RSA operation can be accomplished. Please reference[17] for detail design of RSA accelerator engine.

Interrupt Controller(INTC) ：Jixco contains interrupt module which supports up to five interrupt sources. Five interrupts are used by integrated peripherals (Timers, RSA, AES, DES, 7816IO).When interrupt request signals are set, CPU would branch to corresponding interrupt sevice routine via interrupt vetor.

Random Number Generator(RNG) ：Different from traditional random number generator(RNG),this RNG uses system algorithm as base of generating random number. Jixco also establishes voltage amplifier, Voltage-Controlled Oscillator(VCO), compare circuit etc analog circuit to generate real random number. Besides, arranging power consumption circuit newly designed to prevent information of current consumption from analyzing and tamping by other equipment. Concurrently, protecting security of private information, when system is executed. Please reference[18] for detail design of random number generator.

Phase Lock Loop(PLL) ：Smart card chip contains Phase Lock Loop(PLL) which clock is provided from CLK pin by external clock, then PLL can offer clock to CPU

and cryptography accelerator. The frequency of CPU is the same with external clock but the frequency of cryptography accelerator is two or four times of external clock.

According to EMV 2000 specification[19], the maximum input current of input voltage must be 50mA. For saving power consumption, Jixco designs stop mode and power saving mode.

Stop mode：Stop mode supports the clock stop mode of ISO 7816-3 to bring down the power consumption of system.

Power Saving mode：In Jixco ,two types of devices would have more power consumption :one is Cix CPU; the other is RSA accelerator engine. We found that their execution time can be distinguish. For the reason of saving power, Jixco designs a power saving mode. When smart card is beginning and CPU start to operate, RSA accelerator engine should be in sleep mode. Until system need execute encryption or decryption, RSA accelerator engine would be waked up. When RSA accelerator engine begin to execute, at that time CPU is in sleep mode. Until encryption or decryption is accomplished, can CPU be waked up.

When RSA accelerator engine is ready, it would transmit interrupt signal to wake up CPU, then CPU can continuously execute program. Every interrupt can wake up CPU. Therefore, when CPU will begin executing, it must check if the interrupt is happened. If the interrupt is expect, CPU continue to execute, otherwise, CPU must

enter sleep mode again.. For RSA accelerator engine, it is in the sleep mode when the system starts. When encryption and decryption is accomplished, it would generate interrupt to wake up CPU and right now RSA accelerator engine once again enters the sleep mode. Until cryptography system will be used, can RSA accelerator engine be started.

4.Conclusion

In this paper, we proposed Jixco architecture. At the same time, we has in the process of implementing Jixco in FPGA prototype board. Right now, pure Java CPU(named Cix) is successfully incorporated in FPGA prototype board with 176 simpler bytecodes and 9 more complex bytecodes and cryptography modules of RSA,AES and DES is ready to integrated in it. Besides, we also design circuit on FPGA prototype board for MRAM. In the Future we will aim on low power, multi-application and security of smart card technology.

Reference

[1] "Java Card™ 2.1.1 Virtual Machine Specification", Sun Microsystems, Inc.,2000.

[2] "IBM JCOP offerings", http://www.zurich.ibm.com/csc/infosec/jcop_tools/index.htm

[3] "GemXpresso 211 PK Card Reference Manual", GEMPLUS, July 2000.

[4] "CyberflexTM Access Developer's Series Programmer's Guide", version 3.1, July

1999.

[5] “Security & Chip Card ICs SLE88CX720P”, Infineon Technology, January 2002.

[6] “AE5 Series”, Hitachi, October 2001.

[7] Shau-Yin Tseng & Shien-Wen Dai, “The Implementation of CCL Java Card”, CCL Technical Journal, March 25, 2002.

[8] Chris Edwards, “32-bitters scramble for smart card silicon”, EE Times, October 25, 2001.http://www.eetimes.com/semi/news/OEG20011025S0062.

[9] “A Complete Vision in Smartcard Technology”, http://www.st.com/stonline/press/news/back2002/b951m.htm

[10] Shau-Yin Tseng, ”An Introduction to Smart Card Attacking Methods” ,CCL Technical Journal，March 25,2001

[11] Shau-Yin Tseng, Huan-Wen Wang, and Shien-Wen Dai, “CPU Design for Smart Card Running on Pure Java Environment”

[12] Java Card™ 2.1.1 Runtime Environment (JCRE) Specification. Revision 1.0. May 18, 2000. Published by Sun Microsystems, Inc.

[13] Java Card™ 2.1.1 Application Programming Interface. Revision 1.0. May 18, 2000.Published by Sun Microsystems, Inc.

[14] FIPS PUB 46-3, DATA ENCRYPTION STANDARD, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE / National Institute of Standards and Technology.

[15] FIPS PUB 197, ADVANCED ENCRYPTION STANDARD (AES), FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Reaffirmed November 26, 2001, U.S. DEPARTMENT OF COMMERCE / National Institute of Standards and Technology.

[16] Chih-Chung Lu and Shau-Yin Tseng，Integrated Design of AES (Advanced Encryption Standard) Encrypter and Decrypter，13th IEEE International Conference on Application-specific Systems, Architectures and Processors San Jose, California，July 17~19 2002.

[17] Chih-Chung Lu, “Hardware Design of RSA Accelerator”, CCL Technical Journal,

March 25, 2002.

[18] Inng-Lane Sun, Shau-Yin Tseng, ”An Analogic Random Number Generator Design” ,CCL Technical Journal，March 25,2002

[19] EMV2000 Integrated Circuit Card Specification for Payment Systems, BOOK 1 Application Independent ICC to Terminal Interface Requirements, Version 4.0, December, 2000.