Energy Consumption for Cryptographic Algorithms with Different Clocks on Smart Cards in Mobile Devices

Sneha Sinha
Department of Computer Engineering
MIT Academy of Engineering,Pune

R.M. Gaudar
Department of Computer Engineering
MIT Academy of Engineering, Pune

ABSTRACT

In mobile devices, smart cards become the trend and are used in numerous applications and services. Since mobile devices are battery-powered, so it is important to find energy saving solutions to reduce energy consumption. Most mobile devices are powered by batteries with limited power capacity. In order to protect information during the communication process, security system designers use many cryptographic algorithms to protect user data. The encryption technology will consume considerable power. The Cryptographic algorithms are implemented on a security chip that is embedded in a smart card. When the CPU clock changes the execution time and the energy consumption will thus change. In this paper LabView2010 and related hardware are used to build a power measurement environment. Two sets of experiments are conducted i.e. in fixed clock experiment, which shows that the algorithm complexity affect the power saving and increase execution time, mean while reducing the clock rate has more impact to the execution time than the energy consumption. Second one in random clock experiment, which is used to focus energy consumption distribution of different key.

General Terms

Secret key, security, authentication, cryptographic algorithms

Keywords

Cryptographic, LabView, Smart card, CPU clock, Energy consumption

1. INTRODUCTION

In the past, financial transactions are usually carried out with a personal computer. With the fast development of the 3G network and mobile devices in recent years, applications such as login network banking, online shopping and financial transactions only used on a personal computer in the past can be ported in mobile devices now. Since e-commerce activities in an insecure network has the risk of leaking information. Therefore, service providers often use smart cards to protect consumer information. Smart cards can be used as tokens for identity authentication and can be used to encrypt transferred data. To avoid being stolen by Trojans viruses, a secret key can best stored in the card and the encryption and decryption processes are executed completely inside the card the secret key. On the other hand, people often use mobile devices to watch TV or listen to online music. If the service provider's software on mobile devices is cracked, people can enjoy services without paying which will hurt the rights and interests of service providers. In order to protect their interests, service providers can encrypt meaningful information through the smart card. How does a smart card work on mobile devices? At practice, the smart card reader can access the smart card through USB. But this way is considerably troublesome, since people must carry the reader along. Another approach is to access smart card through the microSD slot on mobile devices, as shown in Figure1.In Figure1,the microSDcard, known as the Security microSD Card (SSDC), consists of a smart chip and flash memory, with both storage and security services functions. By SSDC, mobile devices use smart card services without the need of extra external devices and programmer can develop many applications.

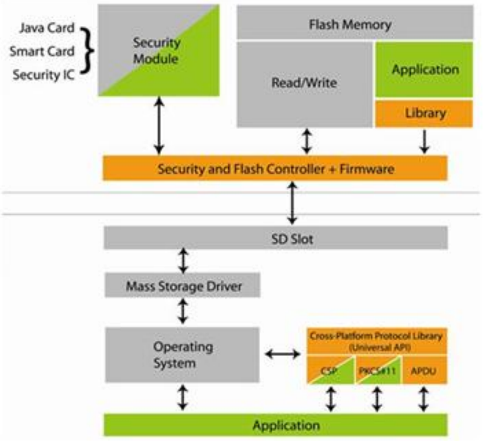


Fig1: The Security micro Card (SSDC), from top to bottom

2. BACKGROUND

This section will describe the symmetric, asymmetric and hash algorithm.

2.1 Symmetric encryption

Before the advent of the asymmetric encryption method, the symmetric encryption method is the only encryption method. Compared to the asymmetric encryption, the symmetric encryption has faster encryption and decryption processes, shorter key length and lower computational cost. Currently the symmetric encryption is used more than the asymmetric encryption. One feature of the symmetric encryption and decryption method is to use of the same key.The communicating parties must use the same key to correctly transmit messages. The symmetric encryption method can be divided into two types, i.e. stream and block cipher encryption. The stream encryption such as RC4, select a byte or a bit to encrypt each time and so it encrypts data instantly without the need to wait until the encryption block is filled with data. On the other hand, the block cipher encryption such as DES,3DES, AES has to wait until the block is filled with data and then starts to do encryption and decryption**.** For communications, a pre-shared key or agreement key is used to encrypt data. The same pre-shared key is used for encryption all the time if no other mechanism is used to change it. Thus, the session key is cracked easily and the communication has a high risk of eavesdropping. By using a key agreement, a key is randomly generated.Although the encryption key for each session is different and without careful analysis of the key agreement, theattacker may find a loop hole in the existing agreement and be able to get the key to tap messages.Since symmetric encryption algorithms have security problems.

AES by NIST replaces DES and has become the most widely used encryption algorithm. The inventor of the AESRijndael,submitted the original version, which can designate their respective block length and key length of 128,192or256 bits to have nine combinations. But the final version of the AES key length has the three choices, but the block length is fixed as 128 bits.

2.2 Asymmetric encryption

The asymmetric encryption algorithm or the public key encryption method uses different keysnamely the public key and private key for encryption and decryption. There are problems by using the symmetric encryption such as the key sharing.In order to ensure the key be known only by the two communication parties, symmetric key encryption must use a secure protocol to send the key.Public key cryptography solves the key distribution problem by using two paired keys,one used to encrypt and the other used to decrypt.The public key cryptographic algorithm has characteristics that it is not feasible find the private key when the public key is only.The public key scheme not only can be used to encrypt confidential information,but also can be used for identity authentication and non-repudiation functions. The identity of the receiver can be determined, because the only the legitimate recipient holds the unique private key.In the same way,the private key scheme can be used to do data signatures with non-repudiation.RSA is an asymmetric encryption method and widely used in security systems.

2.3 Hash algorithm

Hash algorithmcan output input messages of any length to a fixed length hash code.A small change of the input message,such as 1bit or 1byte, will change the output of the hash algorithm.Thus,hash algorithms are often used to test whether a message has been tampered with Common hash algorithms are MD5, SHA1 and SHA256.For MD5,a message of arbitrary length can be entered to output.128-bit message digest During the hash code generation process the input message is divided into several 512 bits blocks.

3. EXPERIMENTAL SETUP

In this section experimental setup, hardware and software used in the experiment are described along with the method used to measure energy consumption.

3.1 Hardware and software

National Instruments LabVIEW (NI LabVIEW) 2010 software and related hardware is used to build the power measurement system.Through graphical lines and diagrams, NI LabVIEW is used to establish flow charts to develop a complete measurement, testingand control system. LabVIEW integrate thousands of hardware devices and built libraries to work for high-level analysis and present information, provide a strong virtual instrumentation functions .LabVIEW platform can work on variety of operating systems.

The security chip used in the experiment is ST33F1M produced by STMicroelectronics.ST33F1M include Secure CoreRSC300 CPU Core designed by ARM, and the core is 32-bit RISC core based on ContextM3core with high performance.The CPU clock is up to 25MHz and the chip has 30K bytes user RAM and 1280K bytes user flash memory.The flash memory has10-year data retention 100,000 erase/write cycles.The ST33F1M can be used in mobile communications, multimedia and banking. The PC used in this experiment has a 2.60GHz Intel Pentium Dual Core CPUE5300 and 4GB of RAM and running the Windows OS.The security cryptographic algorithms are provided from Open SSL0.9.8.o project (The latest version is 1.0.0.d).

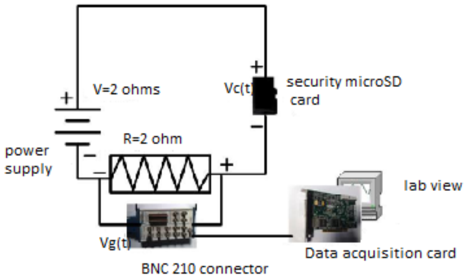


Fig2: Experimental environment

As shown in Figure2,the Vcc pin of SSDC is used to connect a power supply. A 2 ohm resistor is in series with the 3 voltage power supply. A BNC-2110 measures the voltage drop across the resistor and connects to a data acquisition card.LabView on the PC performs data analysis and statistics.

3.2 Measuring energy consumption scheme

Two CPU clock rates: 25MHz and 12.5MHz are used to run the cryptographic algorithm to find their effect on the energy consumption and execution time.In the experiment,the voltage drop across the resistor is measured which can be used to find the voltage over the security chip and to calculate its energy consumption. From the Kirchhoff voltage law, the voltage over the SSDC is calculated as:

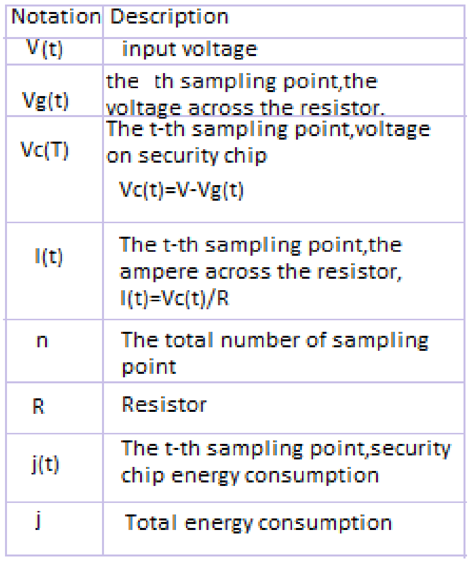
$$V_C(t)=V-V_R(t)$$

The instantaneous energy consumptions on the SSDC are:

$$J_{(t)}=I_{(t)}*V_C(t)$$

Sampling frequency is summed up to find the total energy consumption ***J***.

Table 1-Experimental Parameter



Notation	Description
V(t)	input voltage
Vg(t)	the th sampling point,the voltage across the resistor.
Vc(T)	The t-th sampling point,voltage on security chip Vc(t)=V-Vg(t)
I(t)	The t-th sampling point,the ampere across the resistor, I(t)=Vc(t)/R
n	The total number of sampling point
R	Resistor
j(t)	The t-th sampling point,security chip energy consumption
j	Total energy consumption

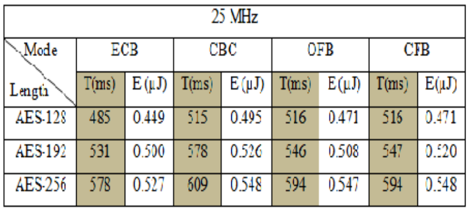
3.3 Experimental result

The cryptographic algorithm is executed in the experimental platform and actual data are retrieved to find the effect on the execution time and energy consumption by reducing the clock rate.

3.3.1 Symmetric algorithm-AES

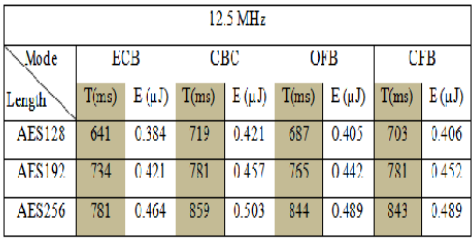
Table 2 shows the execution time and energy consumption for AES by using the25MHz clock rate in different keylengths and four operation modes.Table3 shows the execution time and energy consumption for AES using the 12.5MHz clock in different key lengths and the four operation modes.Among the four modes,the ECB mode does not use an initial vector,so its energy consumption is the lowest.In three key lengths, the AES-256 has most computation time and energy consumption.

Table 2- Energyconsumptionsand execution times of AES using25MHz



25 MHz								
Mode / Length	ECB		CBC		OFB		CFB	
	T(ms)	E (µJ)	T(ms)	E (µJ)	T(ms)	E(µJ)	T(ms)	E(µJ)
AES-128	485	0.449	515	0.495	516	0.471	516	0.471
AES-192	531	0.500	578	0.526	546	0.508	547	0.520
AES-256	578	0.527	609	0.548	594	0.547	594	0.548

Table 3- Energy consumptions and execution times of AES using12.5 MHz

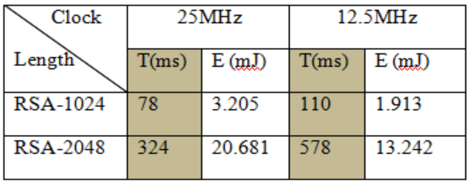


12.5 MHz								
Mode / Length	ECB		CBC		OFB		CFB	
	T(ms)	E (µJ)	T(ms)	E (µJ)	T(ms)	E (µJ)	T(ms)	E (µJ)
AES128	641	0.384	719	0.421	687	0.405	703	0.406
AES192	734	0.421	781	0.457	765	0.442	781	0.452
AES256	781	0.464	859	0.503	844	0.489	843	0.489

3.3.2 Asymmetric algorithm-RSA

Table4 shows the execution time and energy consumption of RSA with signature operations. RSA-2048 needs more computation than RSA-1024. Using 1024 bits at 25MHz, the execution time is 78ms and the energy consumption is3.205mJ.Using 1024 bits at 12.5MHz, the execution time is 110ms and the energy consumption is 1.913mJ.Using 2048 bits at 25MHz, the execution time is 324 msand the energy consumption is 20.681 mJ. Using 2048 bits at 12.5 MHz, the execution time is 578ms and the energy consumption is13.242 mJ.

Table4- Energy consumptions and execution times of RSA



Clock / Length	25MHz		12.5MHz	
	T(ms)	E (mJ)	T(ms)	E (mJ)
RSA-1024	78	3.205	110	1.913
RSA-2048	324	20.681	578	13.242

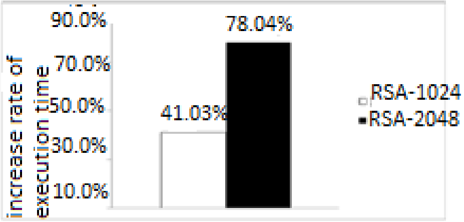


Fig3: Shown to the impact of reducing clock to execution time

Figure3 shows the effect on the execution time by reducing the clock rate for the two key lengths cases.The execution time of 1024 bits is increased by 40% and the execution time of 2048 bits is increased by 70% .It shows that by reducing the clock rate the execution times increase faster when the needed amount of computations rises.

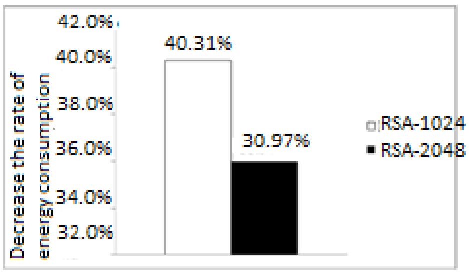


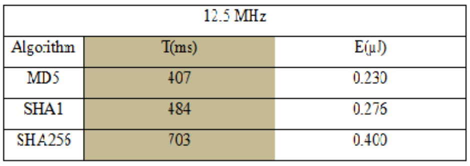
Fig 4: Shown to the impact of reducing clock to energy consumption

Figure4 shows the effect on the energy consumption by reducing the clock rate for the key lengths cases. The energy consumption of 1024 bits is reduced by 41% and the energy consumption of 2048 bits is reduced by 36%.It shows that by reducing the clock rate the energy consumption is reduced slower when the needed amount of computations rises.

3.3.3 Hash algorithms-MD5, SHA1, SHA256

Table5 shows the execution time and energy consumption using the 25MHz clock rate to execute hash algorithms.SHA256 needs the most computation.The execution time of MD5 is 321ms and the energy consumption of each input byte is 0.305µJ.The execution time of SHA1 is 375ms and the energy consumption of each input byte is 0.333µJ.The execution time of SHA256 is 500ms and the energy consumption of each input byte is 0.439 µJ.

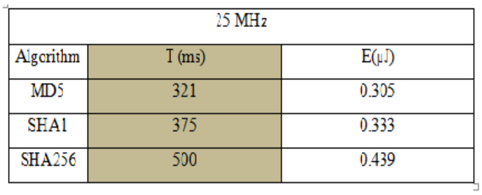
Table 5- Energyconsumption and execution time of hash algorithms using 25 MHz



12.5 MHz		
Algorithm	T(ms)	E(µJ)
MD5	407	0.230
SHA1	484	0.276
SHA256	703	0.400

Table6 shows the execution time and energy consumption using the 12.5MHz clock rate to execute hash algorithms.The execution time of MD5 is 407 msand the energy consumption of each input byte is 0.230µJ.The execution time of SHA1 is 484ms and the energy consumption of each input byte is 0.276µ.The execution time of SHA256 is 703ms and the energy consumption of each input byte 0.400 µJ.

Table 6- Energy consumption and execution time of hash algorithms using12.5 MHz



25 MHz		
Algorithm	T (ms)	E(µJ)
MD5	321	0.305
SHA1	375	0.333
SHA256	500	0.439

3.4 Performance analysis

In symmetric encryption part, AES-128 only has 10 rounds.so the energy consumption is minimal; the execution time is the shortest. In the energy consumption of the three modes, AES-256 has longest execution time and energy consumption is also the largest. ECB mode doesn’t use the initial vector, energy consumption is minimum and run fastest. So ECB mode is saving the most energy. From part of the hash algorithm it can be seen that MD5’s execution time increased by 1.18 times, 24% less energy consumption. SHA1’s execution time increased by 1.29 times, 17% less energy consumption. SHA256’s execution time increased by 1.4 times, 8% less energy consumption. In security, SHA1 is higher than MD5, and SHA256 is higher than SHA1. Comparison of computational complexity, SHA256 is the highest complexity, SHA1 is the second and MD5 is the lowest.

The results show that the clock speed on low complexity algorithms is more apparent than on the high complexity. But the execution time is the opposite result. When the execution of cryptographic algorithms takes too long time, the basic energy consumption of security chip will cancel out the saved energy of reducing clock. If the security system uses hash algorithms, that can select the appropriate algorithm according to demand.

4. CONCLUSION

Theenergy consumptions of smart chipembedded in microSDcard is measured and thisapproach adds many extra energy consumptionswhich determine that the energy consumption result is not real value that executes encryption algorithms.However,this approach is approximately practical inapplications.The practical applications exists extra energy consumptions of SSDC. Those extra energy consumptions need to be considered.From the experimental results following can be concluded:

a. For three types of cryptographic algorithms on SSDC by reducing the clock rate, the increase of the execution time is faster than the decrease of the energy consumption.
b. Reducing the CPU clock rate will have an impact on the execution time.In particular, the execution time increases faster when cryptographic algorithms need more amount of computations.
c. Reducing the CPU clock rate will have an impact on the energy consumption.In particular, the energy consumption decreases slower when cryptographic algorithms need more amount of computations.

5. REFERENCES

[1] Narn-YihLee, Yu-Chung Chiu, “Improved Remote Authentication Scheme with Smart Card,”Computer Standards&Interfaces,vol. 27, issue 2, Jan. 2005, pp. 177-180.

[2] YungFuChanga, C.S. Chenb, and HaoZhou, “Smart Phone for Mobile Commerce,” Computer Standards &Interfaces, vol.31, issue 4,June 2009

[3] N.R.Potlapally,S.Ravi,A.Raghunathan,and N.K.Jha, “A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and SecurityProtocols,”IEEETransl Mobile Computing, vol. 5, pp. 128, Feb. 2006.

[4] SecurityMicroSDCard,http://www.go-trust.com/

[5] RFC 2631:Diffie–Hellman Key AgreemenMethod, June1999.

[6] FIPS46-3: Data EncryptionStandard, Oct. 1999.

[7] FIPS197: Advanced Encryption Standard,Nov. 2001.

[8] IEEE 1363: Standard Specifications for Public-KeyCryptography.

[9] OpenSSLProject,http://www.openssl.org

[10] National Instruments Corporation,http://www.ni.com

[11] ST33F1M, http://www.st.com

[12] RFC 1321: The MD5 Message-Digest Algorithm, http://www.ietf.org

[13] RFC 3174: Secure Hash Algorithm 1, http://www.ietf.org