Design and Implementation of Cryptographic Systems Using 68HC05 Microcontrollers

Chung-Huang Yang
National Kaohsiung First University of Science and Technology
Kaohsiung, Taiwan 824, ROC
chyang@ccms.nkfust.edu.tw
http://www.nkfust.edu.tw/~chyang/

Abstract

Here we describe the design and implementation of 6805-based cryptographic systems, such as conditional-access control systems. We select Motorola's 68HC705B16 microcontroller to act as a security module and our cryptosystems contain Data Encryption Standard (DES) and Advanced Encryption Standard (AES) private-key algorithms to ensure high levels of broadcast security. Performance of implemented DES algorithm is about 15ms per key schedule and encryption or decryption and for AES is about 5ms per key schedule and encryption.

Keywords: cryptography, private-key cryptography, DES, AES, Rijndael, one-way authentication, embedded, smart card.

1. Introduction

In a typical conditional-access control system [1-2], a group of channels are transmitted in the scrambled form and all the decoders in each subscriber's home receive the same signal consisting of scrambled or encrypting components and access control parameter. Successful descrambling occurs only in the homes of those who have been authorized. A conditional-access system is user transparent and could be very secure. It is capable of providing pay-per-view service or send personalized message service to individually addressable subscribers.

Strong scrambling or encrypting operation is generally based upon the usage of a cryptographic algorithm controlled by a secret *key*, changed at very frequent intervals, while a decoder at subscriber's home would reproduce the original data of certain programs (or services) if a correctly encrypted descrambling key ("*session key*") was received.

In practice, for reason of security, a set of secret keys is resident in the key manager device or inside IC card. Each subscriber will have a decoder that contains a unique ID stored on the built-in security module and identical scrambled or enciphered information is received by every decoder. Successful decipher occurs when proper deciphered key is received by the authorized decoders. Furthermore, in such an addressable system, the decoder could be completely activated or deactivated according to subscriber's status or the program (service) in use. Figure 1 shows a typical broadcasting system.

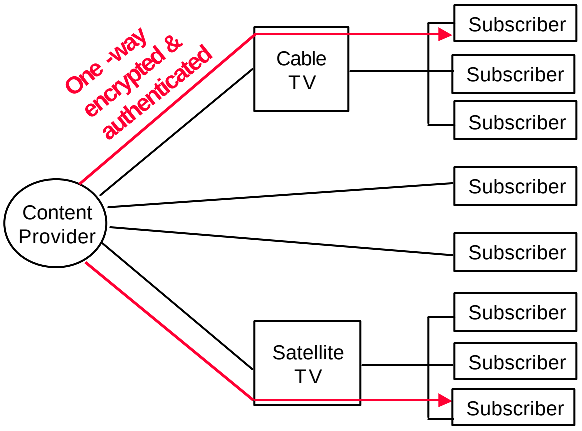

Figure 1. Secure Broadcasting Systems

We want to find an effective and secure mechanism to implement a conditional-access system for broadcasting information. The increase in the number of homes with CATV and lots of cable channels render CATV as the best candidate for information delivery. Data could be encrypted then converted into analog signals and transmitted in the active portion of available TV lines, the unused lines in vertical blanking interval (VBI). The similar technique is used for closed caption or teletext [3].

The very nature of broadcasting is that the programs and data are transmitted in downlink direction and the subscriber needs some assurance that the data is from the alleged service provider. Therefore, in addition to protection from pirates, one-way authentication is also needed to verify the origin of services.

Session key cannot be sent with broadcast signal in the clear form, it must be encrypted with another key. Encryption of our conditional-access system is based on the private-key cryptography of NIST's Data Encryption Standard (DES) [4] or Advanced Encryption Standard (AES) [5-9]. The main idea is to encrypt the broadcasting data with periodic session key while separately encrypt the session key directly or indirectly for authorized subscribers. The following figure illustrates the involved operations.

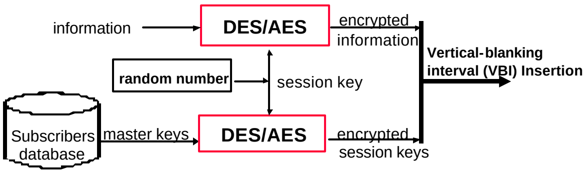

Figure 2: Secure Information Broadcasting

Large amounts of information are broadcasting and protected through the use of dynamically generated session keys, the data-encrypting keys. Session keys are in turn encrypted and guarded by the key-encrypting key, the master key, stored in a physically secure device at subscriber’s decoder. The master key stored in each security device is unique to each subscriber for reasons of system security. But to encrypt and distribute the session key to each subscriber would be impractical, since there may be a huge number of subscriber. In order to overcome this problem a hierarchy of cryptographic key is deployed.

A three-level key hierarchy is generally being deployed. At the top level is the master key; a unique distribution keys each information decoder. In the middle level are the group keys (or period key or area key or member key), common to each group of subscribers. The lowest level keys are session keys that are associated with the broadcast information for a short period of time. The group key is used to carry the session key and itself carried by the master key. As a consequence, only a small number of group keys, encrypted session keys, need to be broadcasting. This would significantly reduce the operational difficulties in distributing the session keys to huge number of subscribers.

2. The 68HC705B16 Device

In order to make low cost approach, we select an embedded device instead of smart card approach. We select the Motorola 68HC705B16 [10] microcontroller that offers an 8-bit CPU, 15K-byte ROM, 256-byte EEPROM, 352-byte RAM, a timer, a serial communication interface, and four general-purpose input/output ports. Figure 3 shows block diagram of this chip.

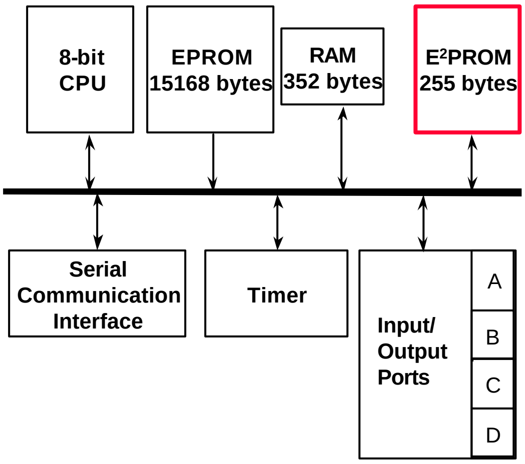

Figure 3. Block Diagram of MC68HC705B16

The CPU's core has an accumulator, an index register, a 5-bit stack pointer, and a 5-bit condition code register. The instruction set features 10 uncomplicated addressing modes including 8 and 16-bit indexing from the 16-bit program counter. Bit manipulation instructions are provided to set, clear, test, or jump based on a bit value anywhere in the memory map. Math functions include add, subtract, and multiply. The EEPROM area is where we store unique ID and cryptographic keys.

The 68HC705B16 is Motorola's most popular one-time programmable (OTP) microcontroller that includes both EPROM and byte erasable EEPROM memories. The vendor provides an in-circuit simulator kit, M68ICS05B, which is an extremely economical tool - with suggested retail price of US$99 [11], for developing and debugging target systems incorporating the 68HC05 microcontroller under Windows 95 environment. A one-time programmable device, 68HC705B16, with suggested list price of US$6.45, is also available for fast prototype development.

3. Implementation of the cryptographic algorithms

We implement both the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) algorithms on the 68HC705B16. The 56-bit DES algorithm, illustrated in Figure 4, is the most well-known cryptographic algorithm since mid 1970s.

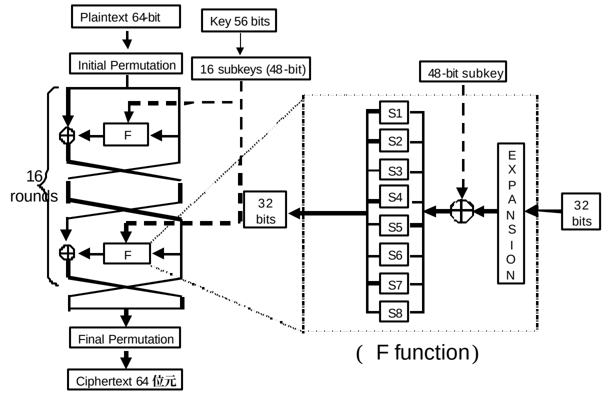

Figure 4. Data Encryption Standard (DES)

DES was designed with hardware implementation in mind. Several permutations are performed in DES, but although permutation is easy to handle in hardware but it is costly in software or firmware implementation. We wrote assembly codes and performance of implemented DES algorithm is less than 15 ms per encryption or decryption at 4MHz external clock (0.5us internal cycle time), which is appropriate for key management. Program size is about 2.5K bytes, including table.

Although DES is very popular in the financial applications, it was shown that the 56-bit DES encryption algorithm could be cracked within one-day [12].

On October this year, NIST announced that Rijndael has been selected as the proposed AES (Advanced Encryption Standard) and it is expected to become an official standard within one year and will replace the aging DES. The key length of AES can be independently specified to 128, 192 or 256 bits with input block length of 128, 192 or 256 bits. This gives approximately 3.4 x 10^{38} possible 128-bit AES keys compared with 7.2 x 10^{16} possible 56-bit DES keys, therefore AES could withstand "brute-force" attacks.

AES was designed with speed and code compactness in mind [7]. Figure 5 shows the operations involved in AES encryption. Since 128-bit input with 128-bit key will be the most likely usage on 68HC705B16, we only implemented assembly codes to support this case.

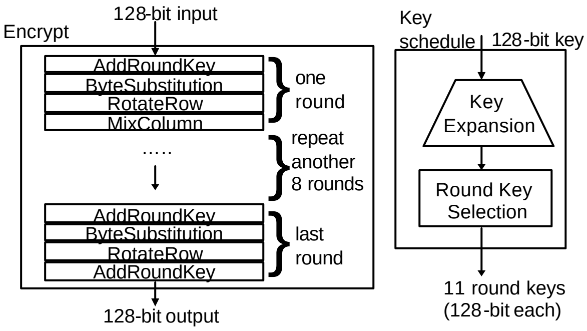

Figure 5. Advanced Encryption Standard (AES), assuming 128-bit key and 128-bit input block

The MC68HC705B16 is suitable for AES implementation. Entire 11 round keys could put in RAM area to improve throughput. Two tables of 256 bytes each are used to implement *ByteSubstitution* operation and its inverse. *MixColumn* involves a multiplication by the polynomial $03\ X^3 + 01\ X^2 + 01\ X + 02$ modulo $X^4 + 1$ where coefficients are given in GF(2^8). We spent extra efforts to speedup performance and our implementation of AES algorithm is less than 5 ms per encryption at 4MHz external clock (maximum frequency is 4.2MHz for 68HC705B16). The ROM size for our AES implementation is about 2.5 Kbytes, about the same size of our implementation on DES. We summarize our implementation results on Table 1.

	DES 56-bit key 64-bit input	AES 128-bit key 128-bit input
Key Schedule	4.2 ms	1.2 ms
Encryption	10.4 ms	4.7 ms
Speed	6,100 bit/s	27,000 bit/s

Table 1. DES and AES performance on MC68HC705B16 running at 4MHz

4. Conclusions

Here we describe our cryptographic implementation efforts on the 68HC705B16 microcontroller. This low-cost device could be embedded with both AES and DES algorithms and is suitable for cryptographic applications.

References

1. Chung-Huang Yang, "A 6805-based Security System for Broadcasting Stock Information", *Proc. IEEE 34th Annual 2000 International Carnahan Conference on Security Technology*, Ottawa, Canada, October 2000, pp. 238-241.
2. D. Angebaud and J. Giachette, "Conditional Access Mechanisms for All-Digital Broadcast Signal", *IEEE Trans. Consumer Electronics*, Vol. 38, No. 3, August 1992, pp. 188-194.
3. B. M. Macq and J.-J. Quisquater, “Cryptology for Digital TV Broadcasting,” *Proc. IEEE*, Vol. 83, June 1995, pp. 944-957.
4. National Institute of Standards and Technology, Federal Information Processing Standard (FIPS) 46-3, *Data Encryption Standard*, October 25, 1999, http://csrc.nist.gov/ fips/fips46-3.pdf
5. "Request for Candidate Algorithm Nominations for AES", *Federal Register*, Vol. 62, No. 177, pp. 48051-48058, Sept 1997.
6. "NIST announces that Rijndael has been selected as the proposed AES", NIST, October 2, 2000, http://csrc.nist.gov/ encryption/aes/.
7. J. Demen and V. Rijmen, "The Rijndael Block Cipher," Document version 2, March 1999, http://csrc.nist.gov/ encryption/aes/round2/AESAlgs/Rijndael/Rijndael.pdf or http:// www.esat. kuleuven.ac.be/~rijmen/rijndael.
8. G. Keating, "Performance Analysis of AES candidates on the 6805 CPU core," April 1999, http://www.ozemail.com.au/ ~geoffk/aes-6805/paper.pdf.
9. S. Chari, C. Jutla, J.R. Rao, P. Rohatgi, "A Cautionary Note Regarding Evaluation of AES candidates on Smart-Cards," *The Second AES Conference*, Feb. 1999. http://www.research.ibm.com/security/aes2.ps.
10. MC68HC05B4/705B5/05B6/05B8/(7)05 B16/705B16N/(7)05B32 Technical Data, Rev. 4, Motorola Ltd., 01-JAN-1999, http://ebus.motorola.com/brdata/PDFDB /MICROCONTROLLERS/8-BIT/68HC 05_FAMILY/DATABOOK/MC68HC05 B6.pdf.
11. *M68ICS05B In-Circuit Simulation Operator's Manual*, Motorola Ltd., May 1998.
12. "Cracking DES code all in a day's work for security experts", http://cnn.com/ TECH/computing/9901/21/descrack.idg/ index.html. See also " RSA Code-Breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation (EFF) - DES Challenge III Broken in Record 22 Hours, " http://www.rsa.com/pressbox/html/990119-1.html.