CONDITIONAL ACCESS IN DIGITAL TELEVISION

Dr. P.C. Jain, Smita Joshi**, V. Mitra*

Himachal Futuristic Communication Ltd.
286, Udyog Vihar, Phase-II, Gurgaon, Haryana-122016
Tel: 0124-6349059-62, 6397635
*jainpc@lycos.com, **joshi_smi@hotmail.com

ABSTRACT

The boundaries between the IT world, Internet System and broadcast TV technologies have blurred. The result of this blurring effect has been the development of a new computing paradigm that is focused on the home entertainment market. A low cost consumer electronic device called digital set-top box is poised and ready to take center stage in this new digital world we are about to enter. The Conditional Access (CA) role is to ensure that viewers see only those programs that they have paid to view. CA helps to attract more subscribers by offering greater program choice than ever before. Subscribers see the program when they want to see them.

1. INTRODUCTION

Digital Television (DTV) is a completely new way of broadcasting and is the future of television. It is a medium that requires new thinking and new revenue-generating business models. Digital TV is the successor to analog TV and eventually all broadcasting will be done in this way. Around the globe cable, satellite and wireless operators are moving to a digital environment. Most industry analyst are predicting that the transition to digital TV will be an evolution rather than a revolution, changing the way of life for hundreds of millions of families around the world. Companies are acknowledging that the convergence between PC, TV and Internet has already begun and are positioning themselves to maximize revenue from this computing paradigm. Today digital TV usually requires a set-top box (STB), which is used to decode and tune digital signals, and converts them to a format that is understood by analog TV. In a STB, the tuner receives a digital signal from a cable, satellite or terrestrial network and isolates a particular channel. The signal is then forwarded to digital demodulator to be converted into binary format. The binary data will be checked for errors using Forward Error Correction (FEC) decoder and then sent to demultiplexer. This demultiplexer will then extract audio, video and data from binary stream and send digital data to appropriate decoders. Before demultiplexer the security subsystem determines subscriber's access rights to various digital TV services. The digital decoders will transform the digital data into a format suitable for viewing on analog television.

Broadcasters and TV operators are now interacting with their viewers on many levels, offering them a greater program choice than ever before. Additionally, the development of a security system or CA provides them with unprecedented control over what they watch and when. A CA system is best described as a virtual gateway that allows viewers to access a new world of digital services. The main goal of any CA system is to control subscriber's access to digital TV pay services and secure the operators revenue streams. Consequently, only customers that have a valid contract with the network operator can access a particular service. Using today's CA systems, network operators are able to directly target programming, advertisements and promotions to subscribers by geographical area, market segment or according to personal preferences. The CA system is, therefore, a vital aspect of digital TV business. CA is not only meant for digital TV. It can be used for digital radio broadcasts, non-broadcast information and interactive services.

HFCL has already developed a free-to-air set-top box for Direct to Home (DTH) applications. In this paper, conditional access system has been designed to implement in HFCL set-top box.

2. CONDITIONAL ACCESS SYSTEM

Conditional Access (CA) is a security technology used to control the access to broadcast information, including video and audio. Access is restricted to authorize subscribers through the transmission of encrypted signals and the programmable regulation of their decryption by a system such as smart card. Restricting access to a particular service is accomplished by using cryptography. It protects the digital service by transforming the signal into an unreadable format. The transformation process is known as 'encryption'. Once a signal is encrypted, it can be decrypted by means of a digital set-top box. Decryption is the process used to convert the message back to its original format. This is carried out using a decryption key. A key is best described as a secret value, consisting of random string of bits, which is used by a computer in conjunction with mathematical formulas called algorithms to encrypt and decrypt information.

The decryption device incorporates the necessary hardware and software subsystems to receive and decrypt the signal. These components are comprised of a decryption chip, a secure processor and device drivers. The decryption chip is responsible for holding the algorithm section of the CA. Secure processor contains the necessary keys needed to decrypt the various services.

3. CRYPTOGRAPHIC ALGORITHMS

A CA system will typically use three to four different cryptographic techniques to perform the various required functions. A symmetric key technique, such as Data Encryption Standard (DES) can provide high-speed encryption that can be used to encrypt the individual services. However, the key distribution can be a problem. A public key system such as RSA solves the Key-distribution problem but is too slow to encrypt services. Digital Signature algorithms can provide that the source of a communication is valid, and Message Authentication codes (MAC) can be used to ensure that a message has not been tampered with.

3.1 Data Encryption Standard

The algorithm is designed to encrypt and decrypt blocks of data consisting of 64 bits under control of a 64-bit key. Blocks are composed of bits numbered from left to right, i.e., the left most bit of a block is bit one. Decrypting must be accomplished by using the same key as for encrypting, but with the schedule of addressing the key bits altered so that the decrypting process is the reverse of the encrypting process. A block to be encrypted is subjected to an Initial Permutation **IP**. After an initial permutation, the plain text block is divided into left half of 32 bits and right half of 32 bits. The permuted input is then subjected to 16 iterations of a key dependent computation and finally to a permutation which is the inverse of the Initial Permutation $\mathbf{IP^{-1}}$. The key-dependent computation can be simply defined in terms of a function ***f***, called the encryption function, and a function **KS**, called the key schedule.

3.2 RSA

The Rivest-Shamir-Adleman (RSA) is an exemplary methodology for public key cryptographic system where encryption key and decryption key are different**.** RSA Algorithm provides a block encryption. The RSA algorithm is based on the fact that it is computationally simple to find large prime numbers, but believed to be computationally infeasible to factor the product of two such numbers.

The algorithm is described below:

1. Choose two large primes, p and q.
2. Compute n = p X q and z = (p-1)X (q-1)
3. Choose a number relatively prime to z and call it d.
4. Find e such that e X d = 1 mod z

To encrypt a message, P, compute $C = P^{e}$ (mod n). To decrypt C, compute $P= C^{d}$ (mod n). Therefore, the public key consists of the pair (e, n) and the private key consists of (d, n).

3.3 MD5

Message Digest 5 (MD5) algorithm takes a message of arbitrary length as input. The output is a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.

In this CA system C language has been used to make a robust system which uses all good features of DES, RSA and MD5 encryption techniques.

4. USAGE OF CRYPTOGRAPHIC ALGORITHMS

Digital broadcasting system uses a scrambler unit to implement encryption. The bitstream out of MPEG-2 encoder/ multiplexer is fed to the scrambler unit along with the scrambler key, called the control word (CW). CAS encrypts the control word within the ECM (Entitlement Control Message) using a hierarchical key structure. The ECM contains a program description and the actual control word, encrypted with the current period key. The CA subsystem in the set-top box will decrypt the control word only when authorized to do so. Thus, any subscriber who is entitled to the service at that time is able to decrypt the control word. The entitlement can be provided in the form of an electronic smart card that is plugged into the STB. The authority to decrypt control word is sent to the set-top box in the form of Entitlement Management Message (EMM), which is subscriber specific. Consequently, the number of EMMs that need to be sent over the broadband network is proportional to the number of STB on the network. In addition to sending EMMs to specific customers, operators can also broadcast EMMs to groups of subscribers in different geographical areas. ECMs and EMMs are generated and broadcasted at the TV operations center using specialized hardware devices. They are then transmitted to the viewer's smart card. This card will check access rights and descramble the requested digital services. The ECM changes continuously in order to maximize security on a digital network. A typical smart card is capable of storing upto a hundred entitlement message, which means that each subscriber on the network is capable of ordering 100 pay TV events at one time. The subscriber information necessary for authority is maintained in the database.

The head-end equipment at the broadcast station determines the configuration of the Transport Stream. Besides one or more audiovisual programs, the TS contain Program Specific Information (PSI) and PSI tables (PAT, PMT, CAT). The Program Association Table (PAT) lists all current programs and indicates the Packet Identifier (PID) values of the Program Map Table (PMTs). There is only one PAT but there are as many PMTs as programs. Each PMT gives information about the component streams (audio, video, data) and lists all parameters necessary for decoding the components. There is one Conditional Access Table (CAT) per TS and it consists of a list of all the CA suppliers that work with programs found in the Transport Stream. The CAT carries the list of CA suppliers that provide services for programs found in the TS. A unique identifier called the CA_system_ID recognizes CA suppliers. The CAT also gives information about EMM and ECM. The TS carries packets corresponding to the scrambled signals but also simultaneously there will be packets from programs offered without access restrictions. It is at the head-end where the packets are multiplexed and encrypted if required. A set-top box will demodulate the signals and will pass the Transport Stream to the security module for possible descrambling. If the module decides that the user is in good standing, and he/she is allowed to watch (or download) certain programs in the TS, then decryption proceeds, and the descrambled TS is passed back to the host for decoding and display.

4.1 Key Distribution and Management for CAS

The structured messages (ECM and EMM) are transmitted from sending end to receiving end using the three-level key distribution and management scheme. The three levels of keys are control word (CW), period key (P) and distribution key (D). Every level of keys is used to encrypt and distribute the former level of keys. Making use of this 3-level architecture we have designed the conditional access system (CAS) for digital TV.

Following is the keys description.

1. Control Word (CW): The control word is used for scrambling the broadcasting program. This is unique for each service channel. In order to increase the security, the control word should be updated with short (1 ~ 10 seconds) period whenever transmission occurs using ECM.
2. Period Key (P): The Period key is used for encrypting the control word and to access Entitlement Control Messages. Period key in each channel is different. The key is never revealed to the subscriber and should be updated periodically.
3. Distribution Key (D): The distribution key is used for encrypting P. This key is unique for each subscriber. The key must be stored in the smart card and never revealed to the subscriber.

A service provider normally receives content from variety of sources including local video, cable and satellite channels. The contents needs to be prepared for transmission to the customer's home by passing the signal through a digital broadcasting system.

At the transmitter (Figure 1), a control word for scrambling is selected. This key is a truly random number as it is derived from a physical process, i.e. the noise in the diode. It is used to encrypt the video and audio for a service. The control word is encrypted with the period key using DES encryption.

The period key, the CW and upto 320 bits of stream description information are combined as the "message" and authenticated by the MD5 message authentication code (MAC). The stream description consists of information like program number, service provider number, blackout information, free time on/off, preview on/off, PPV (Pay Per View) event number, etc.

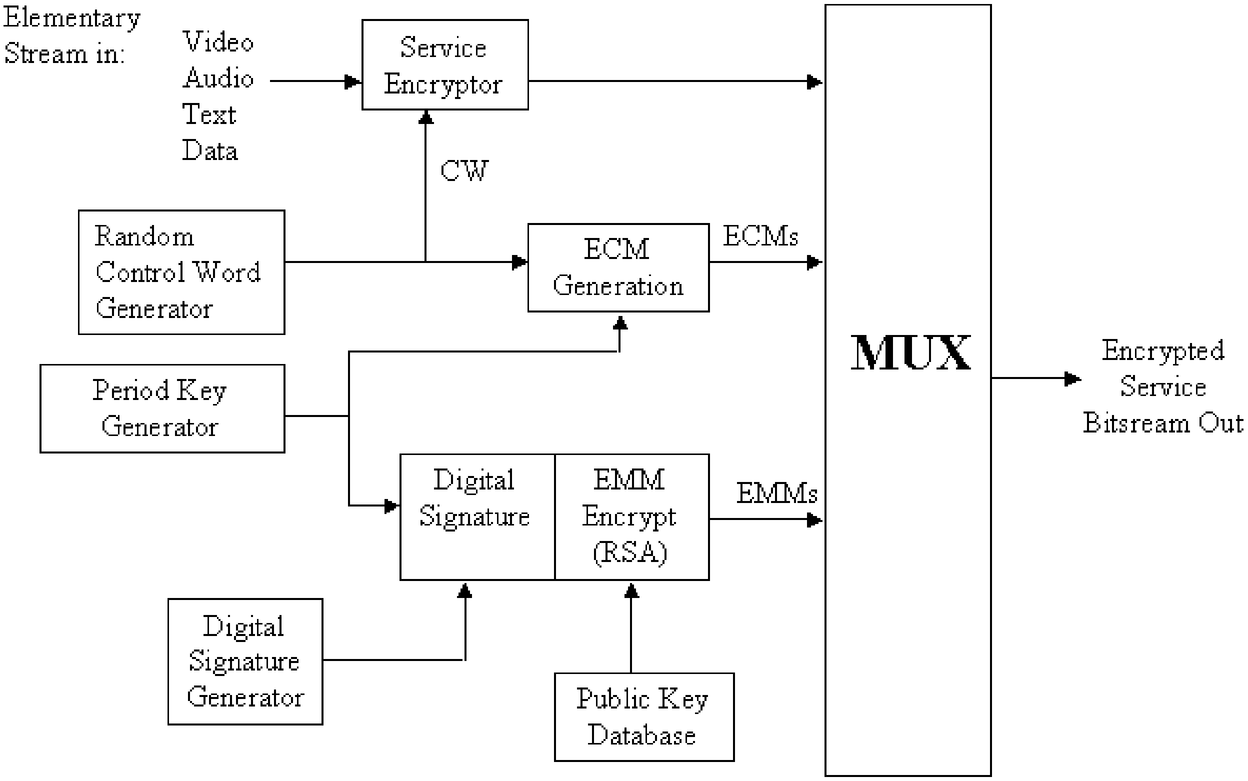

Figure1. *Generic CA Encoder*

The encrypted CW, the MAC, and the stream description bits become the ECM. The period key is signed with a digital signature and then encoded with the public key of an RSA public encryption system.

EMMs are addressed to individual subscribers to authorize them for program viewing. They are encrypted with the card holders Distribution Key (D). These messages give the subscriber the access information it needs to access the ECM messages. These messages are retransmitted periodically. The number of subscribers and the required update time determines the period. The ECMs and the EMMs are multiplexed together to form the encrypted service bitstream.

4.2 CA Decoding

The security module, usually in the form of a smart card, extracts the EMM and ECM necessary for decrypting the transmitted programs. The security module is either integrated in the set-top box or embedded in a PCMCIA (PC card) designed for digital TV reception. The set-top box houses the security module that gives authorization for decrypting the transmitted programs. The encrypted service bitstream is demultiplexed in set-top box to get EMM. The EMM is decrypted with the private part of the RSA key. Digital Signature of the Period Key is checked. If it is valid then ECM is selected. If ECM-MAC is valid then stream description information is stored in appropriate place in the memory of set-top box. Period Key is used to decrypt the control word. Thereafter the DES key is used to decrypt the individual services. The decrypted transport stream is then demultiplexed and decoded to obtain audio and video outputs.

5. CONCLUSION

The need to have channels with restricted access has lead to the development of CA system. Typical applications are pay-per-view television, broadcast of professional conferences, broadcast of university lectures, and others. The most important feature is that the system is based on a renewable security module that, when attached to the host, performs all the CA functions such as entitlement message decoding and TS packet decryption.

Key distribution and management is rather important control scheme to implement CAS. We find that three-level key-hierarchical architecture is suitable for PPV services. The same scheme can be used for authorized users in accessing any other digital data from other service providers. The transmitted data is of no significance for unauthorized users who attempt to access on the network.

Common Interface (CI) module contains the CAM (Conditional Access module) and a smart card reader in one unit. Each consumer can decide for himself which program package he wants to subscribe to. The CI will become a legal requirement in the next few years in USA and Europe. With this consumer can buy any digital set-top box with built in CI interfaces and then decide individually later, which pay package he wishes to subscribe to. A second technical solution conforming to the DVB (Digital Video broadcasting) standard is Simulcrypt. With this, the digital set-top boxes only have a single CA system permanently built in. Program packages wanting to be received with this must support this encryption standard.

6. REFERENCES

[1] ETS 300 468, Specification for Service Information (SI) in DVB systems, February 1998

[2] A045, Head-End Implementation of DVB SimulCrypt, June 1999

[3] FIPS 46-1, Specifications for the Data Encryption Standard

[4] Harold A. Rosen, Leonardo Chiariglione, *Direct Broadcast Satellite Communication, Prentice Hall*, NJ, 2000

[5] Don J. Torrieri, *Principles of Secure Communication systems, Artech House Inc*, 1985

[6] ISO /IEC –13818-1, Generic coding of moving pictures and associated audio system

[7] RFC 1321: “ The MD5 Message-Digest Algorithm”