uOttawa

L'Université canadienne
Canada's university

FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTOCTORALES

uOttawa

L'Université canadienne
Canada's university

FACULTY OF GRADUATE AND POSDOCTORAL STUDIES

Rui Zhao

AUTEUR DE LA THÈSE / AUTHOR OF THESIS

M.Sc. (Systems Science)

GRADE / DEGREE

Department of Systems Science

FACULTÉ, ÉCOLE, DÉPARTEMENT / FACULTY, SCHOOL, DEPARTMENT

A Public Key-Based Encryption/Decryption Technique for Real-Time Signals

TITRE DE LA THÈSE / TITLE OF THESIS

Professor Tet Yeap

DIRECTEUR (DIRECTRICE) DE LA THÈSE / THESIS SUPERVISOR

CO-DIRECTEUR (CO-DIRECTRICE) DE LA THÈSE / THESIS CO-SUPERVISOR

EXAMINATEURS (EXAMINATRICES) DE LA THÈSE / THESIS EXAMINERS

Professor Ahmed Karmouch

Professor Voicu Groza

Gary W. Slater

Le Doyen de la Faculté des études supérieures et postdoctorales / Dean of the Faculty of Graduate and Postdoctoral Studies

A Public Key-Based Encryption/Decryption Technique for Real-Time Signals

RUI ZHAO

THESIS SUBMITTED TO THE
FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF MASTER OF SYSTEM SCIENCE

SCHOOL OF MANAGEMENT
SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING
UNIVERSITY OF OTTAWA

© Rui Zhao, Ottawa, Canada, 2007

Library and
Archives Canada

Published Heritage
Branch

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque et
Archives Canada

Direction du
Patrimoine de l'édition

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence
ISBN: 978-0-494-49304-5
Our file Notre référence
ISBN: 978-0-494-49304-5

NOTICE:
The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:
L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.

Canada

Abstract

Pay-TV Satellite Broadcast Service is very common today. However, protecting signals from being pirated is a principal issue. That is done using a conditional access system. In this thesis, we introduce and analyze different existing conditional access system design methods. Modification of the current method is proposed, and significant performance improvement is obtained. Satellite communication and cryptology are studied theoretically, which enables us to design public key-based encryption/decryption techniques for satellite broadcast that can supply higher secret solutions. Our simulation results show that the new design system is superior and more practical.

Acknowledgment

First of all, I would like to express my deepest thanks to my thesis supervisor, Dr. Tet H. Yeap, for his guidance and encouragement during the course of my M. Sc. program.

Special thanks to my parents; without their support and encouragement, I wouldn't have come to Canada and studied for a Master degree.

I extend a special thanks to my husband, Dafu Lou, for his love and support; without him I wouldn't have finished my studies.

Contents

List of Figures

List of Tables

Glossary

AES	Advanced Encryption Standard
ATSC	Advanced Television Systems Committee
BSS	Broadcast Satellite Services
CA	Conditional Access
CAM	Conditional Access Module
CATV	Cable Television
CI	Common Interface
CSA	Common Scrambling Algorithm
CW	Control Word
DBS	Direct Broadcast Satellite
DC-II	Digicipher-2
DES	Data Encryption Standard
DTH	Direct To Home
DVB	Digital Video Broadcast
DVB-S	Digital Video Broadcasting over Satellite
DVB-T	Digital Video Broadcasting for Digital Terrestrial Television
DW	Decryptoworks
ECC	Elliptic Curves Cryptography
ECM	Entitlement Control Message
EMM	Entitlement Management Message
ETSI	European Telecommunications Standards Institute
FSS	Fixed Satellite Services
GSO	Geostationary Orbit
HDTV	High Definition Television
IDEA	International Data Encryption Algorithm
IRD	Integrated Receiver Decoder
ISL	Intersatellite Link
ITU	International Telecommunication Union
ITU-R	ITU Radiocommunication Sector

LDTV	Low-Definition Television
LNB	Low-Noise Block Converter
MPEG	Moving Picture Experts Group
MSS	Mobile Satellite Services
Mux	Multiplexer
NGSO	Non-Geostationary Orbits
NIT	Network Information Table
NTSC	National Television System(s) Committee
PAL	phase alternation line
PAT	Program Association Table
PES	Packetized Elementary Stream
PGP	Pretty Good Privacy
PID	Packet Identifier
PSI	Program-Specific Information
PSIP	Program and System Information Protocol
PSTN	Public Switched Telephone Network
QPSK	Quadrature Phase-Shift Keying
RC4	ARCFOUR an algorithm for symmetric key cryptography
RS	Reed Solomon
RSA	An algorithm for asymmetric key cryptography
SDTV	Standard-Definition Television
SECAM	Séquentiel Couleur à Mémoire, French for "color sequential with memory"
SI	Service Information
SMATV	Satellite Master Antenna Television
SMS	Subscriber Management System
STB	Integrated Receiver Decoder, commonly referred to as a Set-Top Box
SSH	Secure Shell
SSL	Secure Sockets Layer
TDM	Time Division Multiplex
TS	Transport Stream
VCT	Virtual Channel Table

WARC World Administrative Radio Conference

Chapter 1

Introduction

1.1 Background

The first commercial communication satellite, INTELSAT I (known as "Early Bird"), was launched in April 1965. Since then, satellite communications have become a major method of international and internal communications over long or moderate distances. Although the initial task of satellite communications was the transmission of telephone and television signals, its mission has been extended to cover other applications. However, in many applications, the sender wants to restrict access and to control which receivers can receive broadcast information; for example, in Pay-TV Satellite Broadcast Service.

Electronic communication technology has advanced at a very fast pace during the past few decades. Today we can send a multimedia message to or receive one from virtually anyone around the world in seconds through the Internet. To protect the transmitted data from eavesdropping by someone other than the desired receiver, we need to disguise the message before sending it into the insecure communication channel. This is achieved by a

cryptosystem. It is widely recognized that data security plays a central role in electronic communication. Examples include security for wireless phones, wireless computing, pay-TV, and copy protection schemes for audio/video consumer products and digital cinemas, banks, etc. All modern security protocols use symmetric-key algorithms (private-key algorithms) and asymmetric-key algorithms (public-key algorithms). [1]. In private-key algorithms, both the sender and receiver are required to have knowledge of the secret key used for encrypting the data, since the same key is used for decryption. Thus, care has to be taken to exchange the key using very secure and trusted channels. Public-key algorithms use different keys for encryption and decryption, thereby avoiding the necessity to exchange the secure key between the sender and receiver [2]. Now cryptosystems are applied in very wide areas. I will focus on the digital satellite broadcast system.

However, the most difficult issue is how to restrict access. That is what the encryption system does. For satellite broadcasting, several encryption systems have been developed by leading companies all over the world. Well-known systems are Irdeto, Nagravision, Cryptoworks, Seca, Betacrypt, VIAccess, and Digicipher 2. Experiences of the past years show that developing an encrypting system is a very great challenge [5]. This proposal will discuss other possible encryption solutions for Digital Pay-TV Satellite Broadcast Service.

1.2 Motivation

Today, the problem of pirating satellite TV program is very ubiquitous. Currently, various pirate technologies completely compromise ExpressVu satellite signals. The current systems have crashed. There are no practical and secure systems for satellite broadcast service. Bell Canada needs to find a more effective way to protect the satellite signal.

1.3 Contributions

We have proposed a new secure scheme for satellite broadcast service with the following features:

- Integrated key management
- Auto key exchange
- Auto upgrade
- High secure level, which is ECC algorithm-based

A simulation program needs to be built to test the proposed scheme. The simulation results show that the new scheme is practical.

1.4 Outline of the Thesis

In Chapter 2, we introduce the principle of satellite communication and cryptography. Some key features of the satellite TV system and some major cryptographic algorithms are also introduced in this chapter. Current satellite TV control access systems are discussed in Chapter 3. A modified design method and a new control access design method are presented in Chapter 4. In Chapter 5, the simulation results are given, and different methods are compared. Conclusions and future enhancements are given in Chapter 6.

Chapter 2

Background

2.1 Satellite Communication

A satellite communications network plays a significant role in supporting access to the Internet through a hybrid, satellite/terrestrial, or a two-way satellite IP network infrastructure. A satellite communications network is distinguished by several characteristics such as global coverage, scalability, broadcast capability, bandwidth-on-demand flexibility, multicast capability, and reliability. Satellite is an excellent candidate for providing broadband integrated Internet access. The current satellite systems operate in C and Ku frequency bands. Most of the proposed satellite network architectures use geostationary orbits (GSO), non-geostationary orbits (NGSO), and multi-spot beams at Ka-band frequencies.

2.1.1 Architecture of a Satellite Broadcast System

A space segment and a ground segment (Figure 2.1) compose the satellite system for communications and broadcasting.

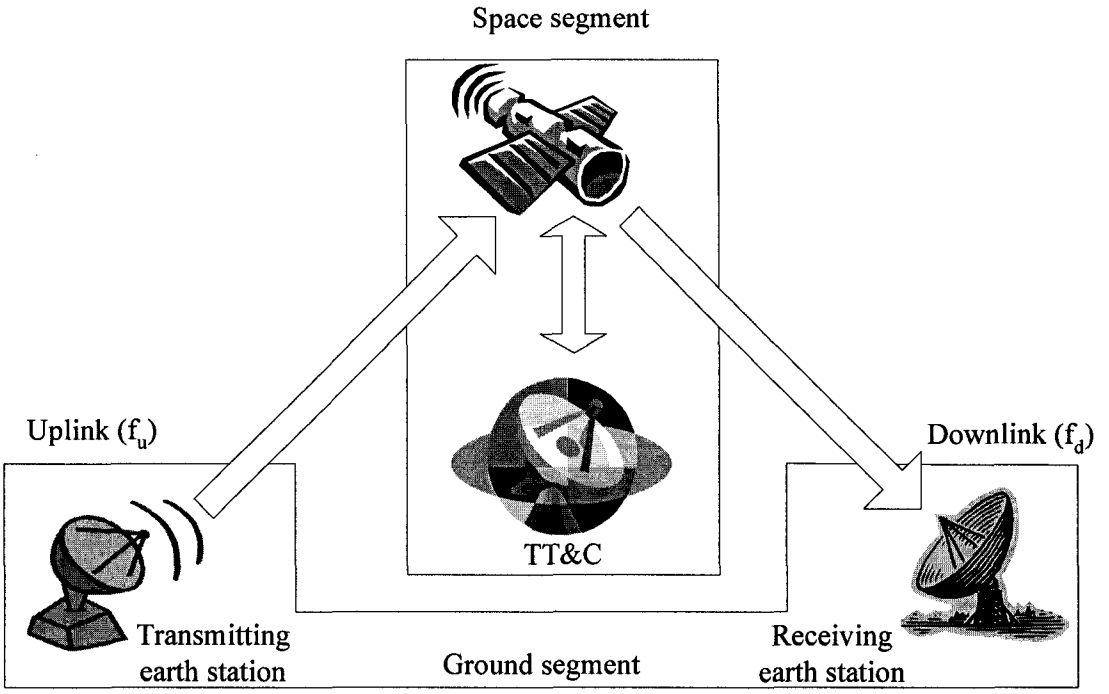


Figure 2.1 Satellite Broadcast System Elements [1]

The space segment contains the satellite and all ground facilities for the monitoring and control of the satellite (e.g., orbital position and adequate pointing to the coverage area on Earth). Communication can be established between all ground stations located within the coverage area, also called the satellite footprint.

In an operational system, one or more in-orbit spare satellites usually back up the satellite in use. Many of the present communication satellites are in the geostationary orbit, and they are called geostationary satellites. The ground segment consists of all Earth stations directly connected to end-user equipment, such as transmitters and receivers.

2.1.2 Satellite Services

Satellite communications have three types of satellite services, Fixed Satellite Services (FSS), Mobile Satellite Services (MSS), and Broadcast Satellite Services (BSS). These are described in the following paragraphs. ITU-R (International Telecommunication

Union Radiocommunication Sector) has been involved in standardization activities of satellite systems for these services.

❖ Fixed Satellite Services (FSS)

Figure 2.2 shows Fixed Satellite Services, which concern all radio communication services between earth stations at given positions. The given position can be a specified fixed point or any fixed point within specified areas. These services provide transmissions nationally or internationally on the basis of a network topology, which can be transit, distribution, or contribution types. The applications supported include video, TV, audio, and data types, primarily on a point-to point basis (transit mode). [2]

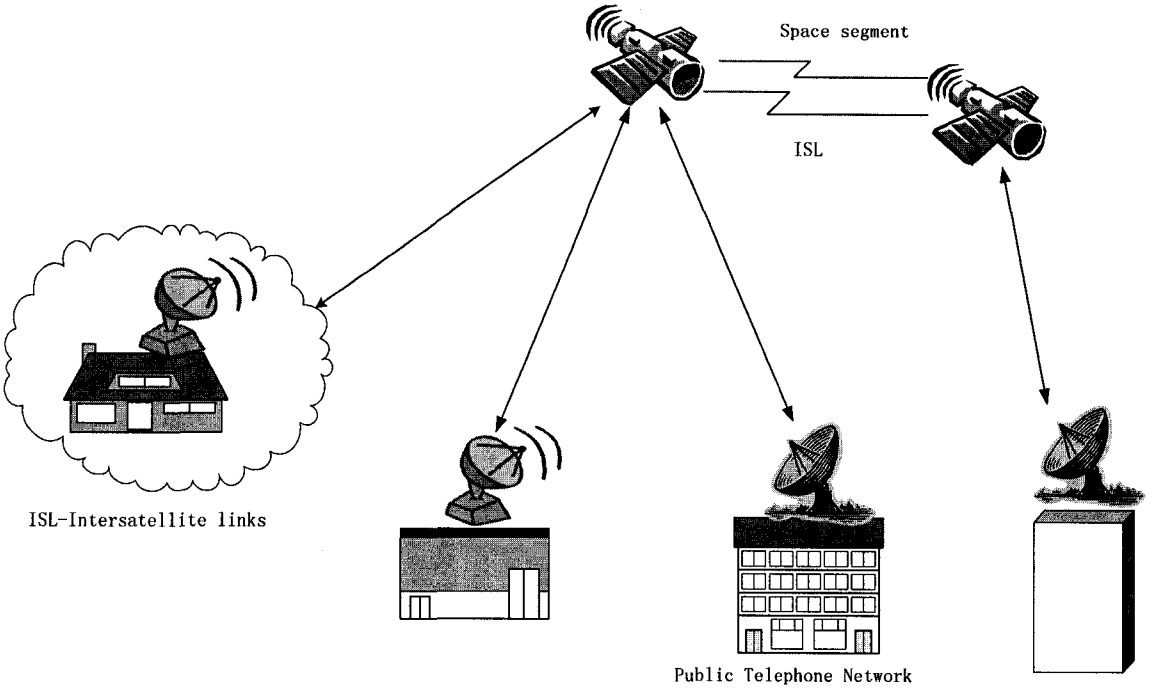


Figure 2.2 Fixed Satellite Services (FSS) [2]

❖ Mobile Satellite Services (MSS)

Mobile Satellite Services, shown in Figure 2.3, include all radio communications between a mobile earth station and one or more satellites.

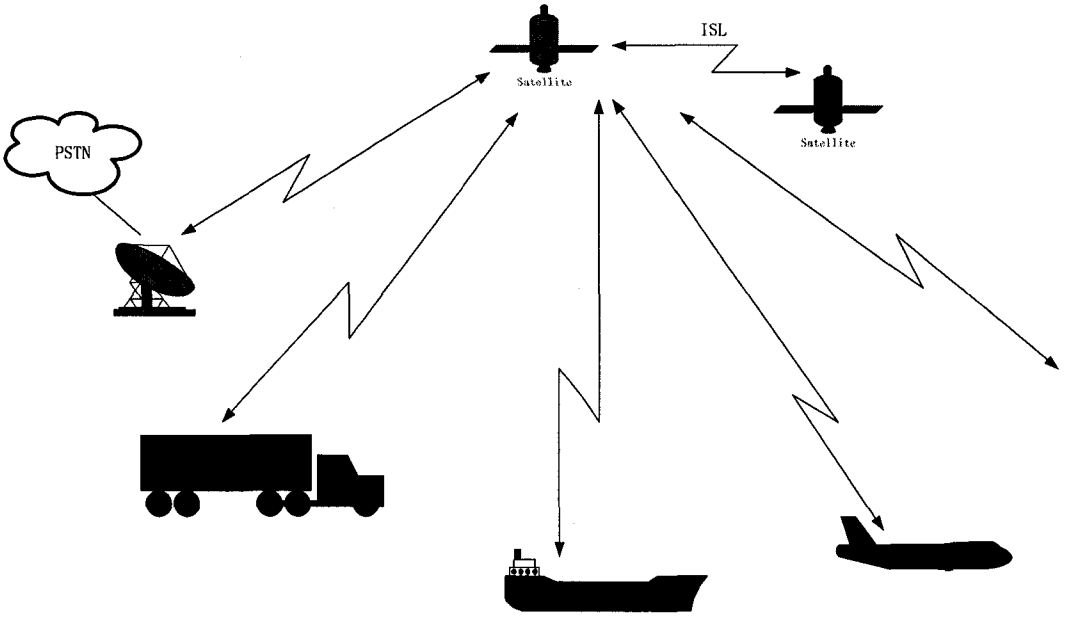


Figure 2.3 Mobile Satellite Services (MSS) [2]

❖ Broadcasting Satellite Services (BSS)

Broadcasting Satellite Services are radio communication services in which signals transmitted or retransmitted by satellite are intended for direct reception by the general public, as shown in Figure 2.4. Very small receiving antennas receive the signals (e.g., television is in a receiver-only mode). Broadcasting involves one feeder link, which is a link from an earth station located at a specific fixed point to a satellite or vice-versa, and a broadcast downlink to the user. [2]

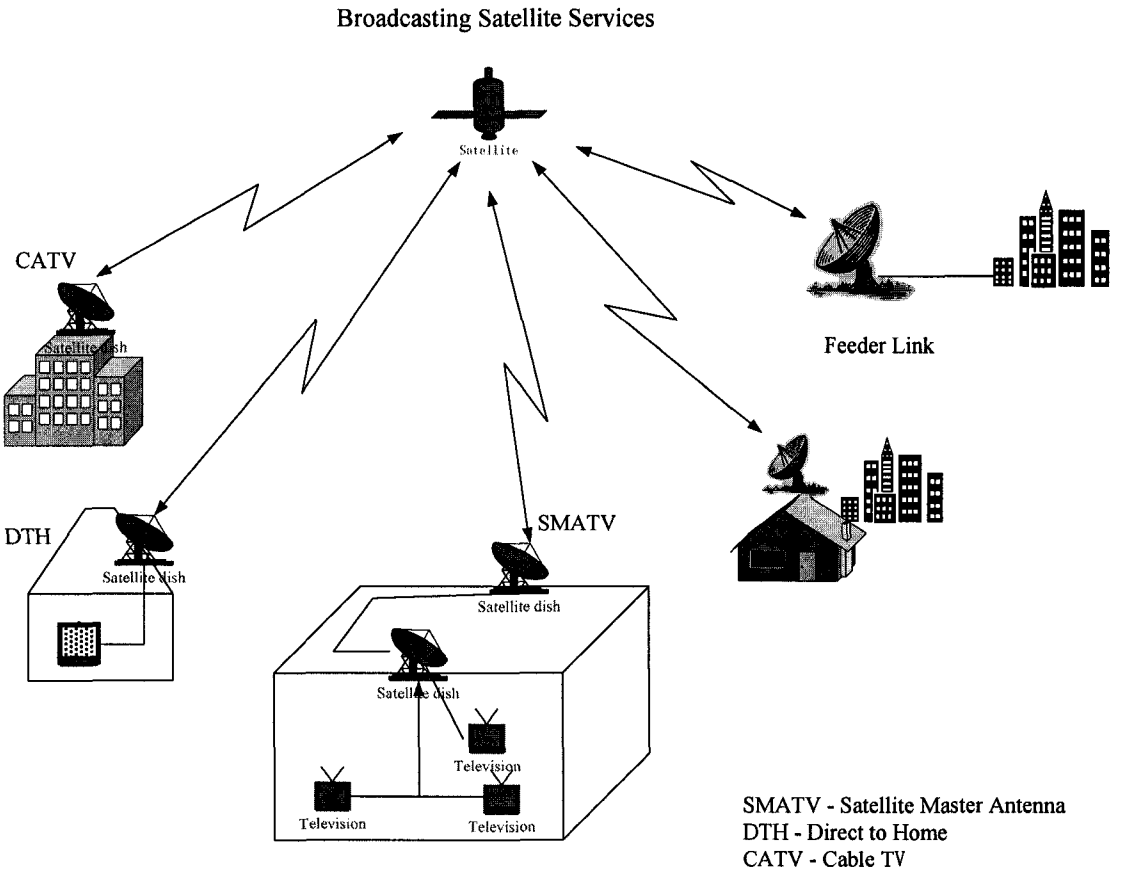


Figure 2.4 Broadcasting Satellite Services [2]

2.2 Direct Broadcast Satellite Services

Direct broadcast satellite, or DBS, is a relatively recent development in the world of television distribution. Direct broadcast satellite can refer either to the communications satellites themselves that deliver DBS services or to the actual satellite television service. DBS systems are commonly referred to as "mini-dish" systems.

There are three primary elements involved in the DBS system: the orbiting transponder satellite, the terrestrial uplink transmission station, and the downlink transmission to the home receiver dish. Together these elements provide for the transmission of television programming up to the satellite and the subsequent retransmission of the programming back down to multiple home reception dishes. (Figure 2.5)

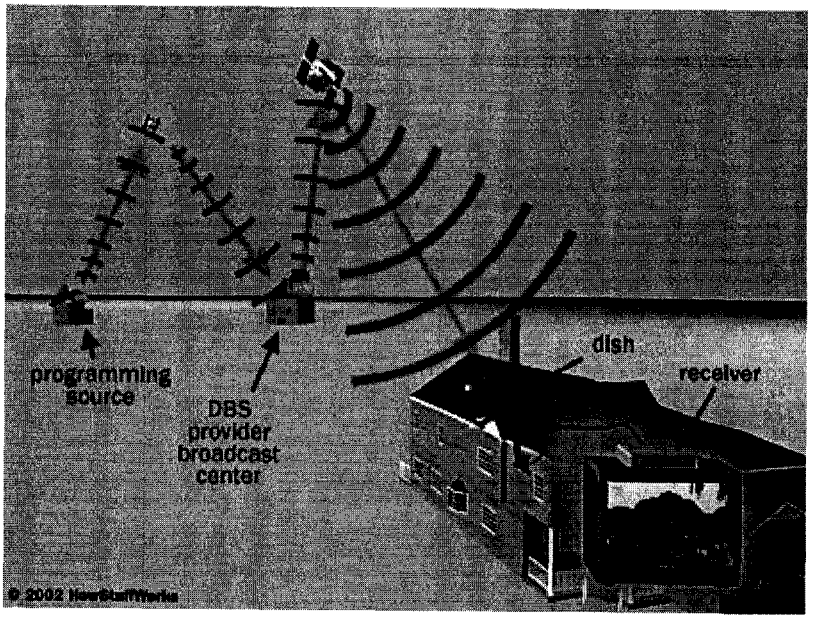


Figure 2.5 Direct Broadcast Satellite Systems [5]

DBS systems all use geostationary satellites and can be classified according to satellite power output as follows:

- Low-power systems (C band; FSS: 6/4 GHz);
- Medium-power systems (Ku band; FSS: 14/12; 14/11 GHz);
- High-power systems or direct broadcast by satellite (DBS) (Ku band BSS: 18/12 GHz).

Once a DBS satellite is parked in orbit, it can begin providing radio relay services for a broadcaster and its dish owner customers. Using a transponder makes this relay possible. The transponder accepts radio signals from a broadcast station's uplink transmitter and amplifies and changes that signal to a different signal. Changing the signal is necessary in order that signals coming into the transponder and signals leaving the transponder do not interfere with each other. During the downlink, the transponder transmits the new amplified signal back to the ground to be captured by multiple dish users. This arrangement results in what is known as a point-to-multipoint relay system.

Each orbital slot, or satellite slot, is allowed a designated frequency that is an amount designated by the World Administrative Radio Conference (WARC). DBS satellite transponders have frequency allotments that allow for the transmission of 32 analog TV channels ("Direct Broadcast Satellite Systems," 1992, pp. 326-327). This number can be less depending on the watts of power used for transmission. Development of digital compression technology, however, has allowed today's DBS broadcasters to increase their channel numbers by eight times or more. MPEG-2 compression technology can digitize and compress several analog channels into the space of one analog channel, thus a potential for 200 channels or more. MPEG-2 is the standard compression technology for most DBS broadcasters. Using digital compression, however, requires that all elements in the satellite broadcast system, from the broadcaster to the satellite to the dish owner, operate on the digital format.

The uplink, the broadcast transmission centre, is a second part of the DBS system. Here the program provider collects the programming in the service and transmits that information up to the satellite transponder. If they are not digitized, programs on DBS systems are converted into the digital format and compressed before transmission. All programming is encrypted in order to prevent access to use of signals by non-subscribers. Encryption basically breaks up the video information into coder information that requires a decoder, at the reception end, to rebuild the information back into a viewable image.

The technology needed at the subscriber end of the DBS system begins with the parabolic dish. The dish, when pointed in line of sight to the correct satellite, collects the frequency signals being downlinked from the satellite's transponder. The curvature of the dish reflects the signals toward the feedhorn. At the center of the feedhorn is the low-noise block converter (LNB). "This is the little gizmo that amplifies the very weak signals from the dish and also converts them to a more suitable band of frequencies" (Bourgois, 1996). Next the signal is transferred by cable line into a receiver in the home. The receiver can then decode, decompress, amplify, and convert the signal into a viewable TV image, thus completing the distribution of DBS television. [4]

2.3 Transmission Techniques and Standards for Digital Satellite TV Signals

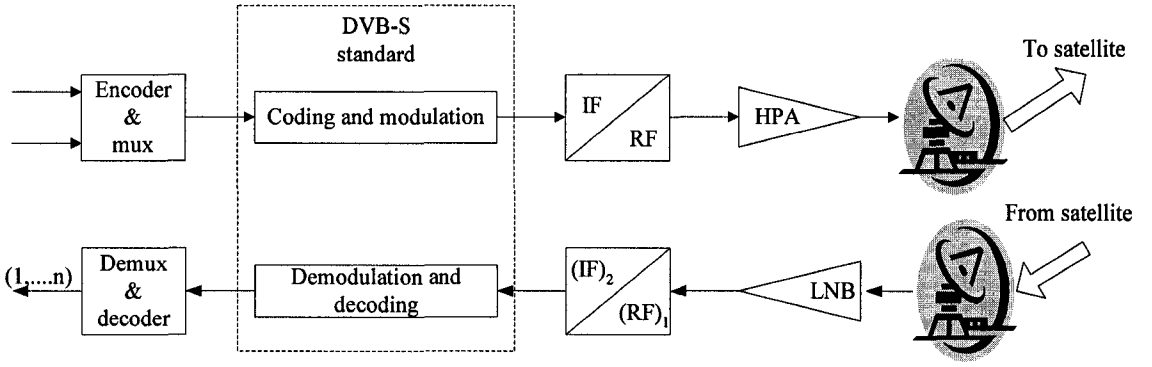
DVB stands for Digital Video Broadcast. DVB Standards and related documents are developed under the DVB Project (founded in 1993) and are published by the European Telecommunications Standards Institute (ETSI). Today, the DVB Project consists of over 220 organizations in more than 29 countries worldwide. The standards are based on the ISO MPEG-2 standard, but extend this to cover system-specific details to ensure a fully specified system. DVB has been adopted by most countries worldwide, with the exception of countries based on the US NTSC analogue TV system (these include the USA, Mexico, Canada, South Korea, and Taiwan). These countries have chosen a similar, but incompatible, system also based on MPEG-2. The alternate system is specified by the US Advanced Television Systems Committee (ATSC). A related (almost identical) system is known as Digicipher-2 (DC-II). Both DVB and ATSC/DC-II support normal and High Definition TV (HDTV) [5][6].

2.3.1 The European Satellite Standard - Digital Video Broadcasting over Satellite (DVB-S)

DVB standards may be grouped by the transmission method employed:

- DVB-C (Cable) DVB interaction channel for cable TV distribution systems (CATV)

- DVB-S (Satellite) Figure 2.6 shows a system block diagram and the scope of the DVB-S standard. The DVB-S provides a range of solutions that are suitable for transponder bandwidths between 26MHz and 72MHz, which includes all of the BSS and FSS satellite systems in existence or under development.



mux: multiplexer demux: demultiplexer

HPA: High-Power Amplifier LNB: Low-Noise Amplifier

Figure 2.6 System Block Diagram and Scope of the DVB-S Standard [1]

DVB-S is a layered transmission architecture [9]. At the highest layer we find the payload, which contains the useful bit stream. As we move down the layers, additional supporting and redundancy bits are added to make the signal less sensitive to errors and to arrange the payload in a form suitable for broadcasting to individually owned Integrated Receiver Decoders (IRDs). The system uses QPSK modulation and concatenated error protection based on a convolutional code and a shortened Reed Solomon (RS) code. Compatibility with the MPEG 2-coded TV services, with a transmission structure synchronous with the packet multiplex, is provided. All service components are time division multiplexed on a single digital carrier. Bit rates and bandwidths can be adjusted to match the needs of the satellite link and transponder bandwidth and can be changed during operation [8].

The video, audio, control data, and other data are inserted into payload packets of fixed length according to the MPEG transport system packet specification.

- DVB-T (Terrestrial TV) framing structure, channel coding, and modulation for digital terrestrial television (DVB-T) [8].

2.3.2 ATSC Direct-to-Home Satellite Broadcasting Standards

The ATSC Satellite Broadcast System comprises of two major subsystems:

1) Transmission System
2) IRD, commonly referred as a Set-Top Box (STB).

Transmission System

The transmission system comprises an emission nultiplexer (Mux), a modulator/encoder, and a transmitter.

Figure 2.7 shows a functional block diagram of a transmission system. The Emission Mux accepts and combines

- ATSC multi-program transport streams (A/53B, A/65B, A/70, and A/90 protocols) from different sources

- Satellite extensions to PSIP (Program and System Information Protocol)

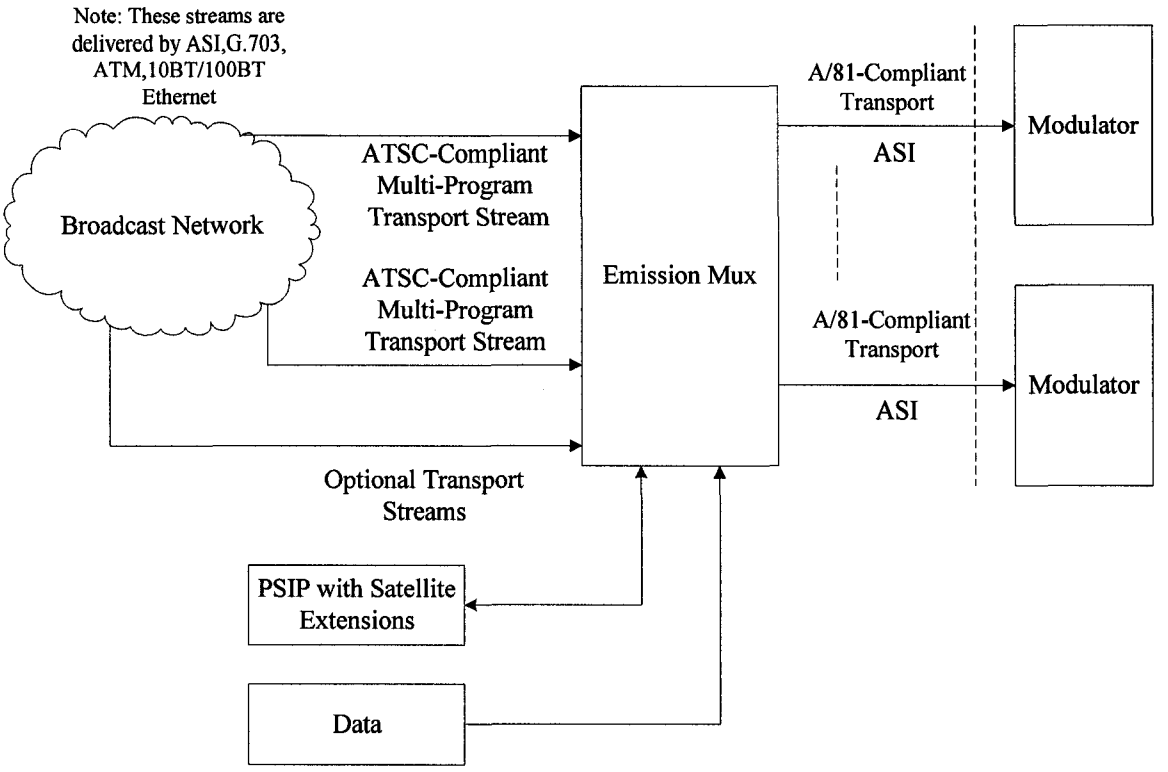


Figure 2.7 ATSC Transmission Systems

Additionally, the Emission Mux may accept

- MPEG-compliant (non-ATSC) transport streams
- Data streams such as A/90 and DVB data broadcast

All multi-program transport stream output from the Emission Mux to a modulator shall conform with

- Transport, audio, and video format extensions defined for satellite delivery in this standard
- System information with all the normative elements from A/65B (PSIP) and satellite extensions such as the satellite Virtual Channel Table (VCT) defined in this standard

Transport streams at the output of the Emission Mux may also carry additional information to support delivery system-specific needs (such as DVB-SI [26], A/56 [23],

control data, EIA-608B captions using ANSI/SCTE 20 2001 [1], and MPEG-1 Layer 2 audio [28]). When present, such information shall not conflict with the code points used in this standard.

IRD System

A functional block diagram of an IRD system is depicted in Figure 2.8. This system demodulates and decodes audio, video, and data streams.

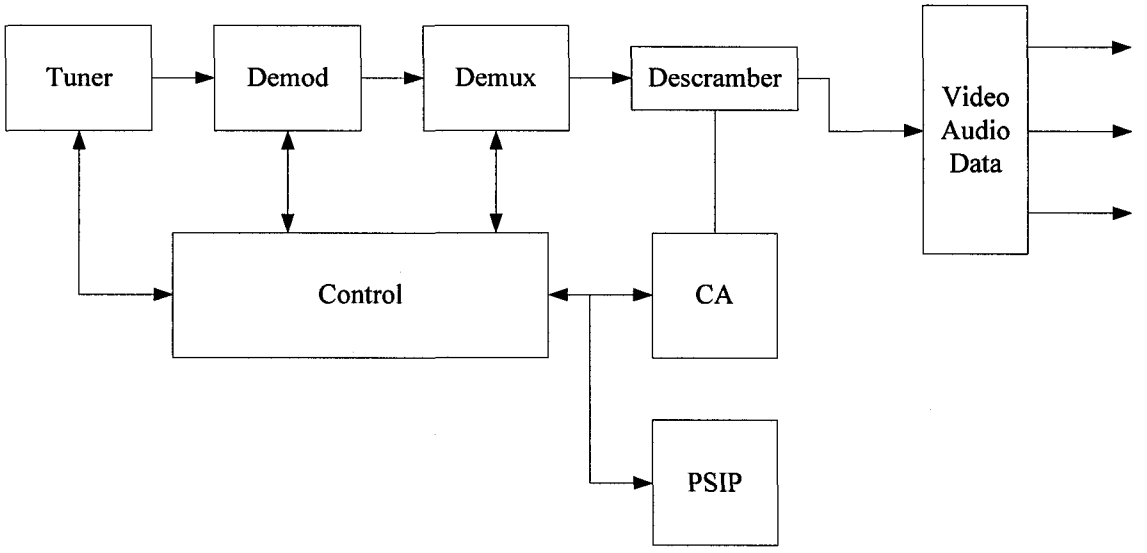


Figure 2.8 Functional Block Diagram of IRD

2.3.3 MPEG 2

The ISO/IEC JTC1 SC 29 MPEG produces most common standards for the digital coding of audio and video signals. This group has specified and upgraded several standards for digital audio-visual coding [10]. Television programs technically consist of three elements: audio and video information as well as additional information to support these programs. These elements have to be provided to the IRD in an orderly way. For this purpose, MPEG-2 has defined a standard [11], referred to as the MPEG-2 systems. This standard describes the multiplexing of the (MPEG) encoded audio signal, the (MPEG) encoded video signal, and the required additional information. Figure 2.9 presents a functional representation of the MPEG-2 systems [10].

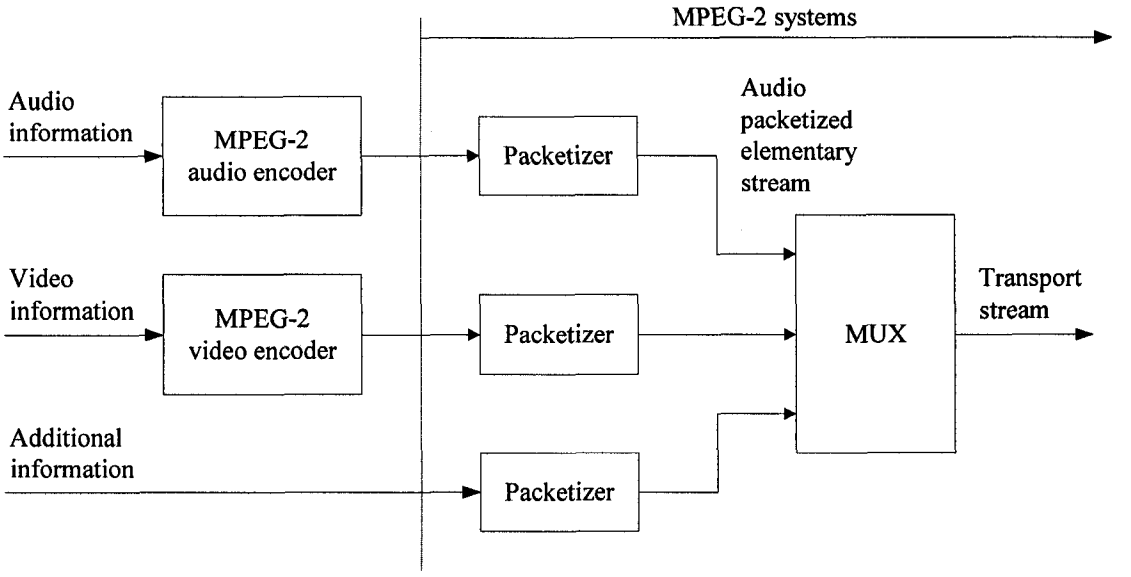


Figure 2.9 Functional Representations of the MPEG-2 Ssystems [14]

The encoded audio signal is provided to a packetizer, which produces a stream of standardized packets, each including a header, an additional header (optional), and encoded audio information. This stream is called the packetized elementary stream (PES). As it concerns an audio signal, this PES is referred to as the audio PES. The same process applies to the encoded video signal and the additional data. Next, these tress PESs are provided to a multiplexer, which eventually produces a standardized data stream, including a header, an adaptation field (optional), and a payload including the information from the several PESs. This stream is referred to as the transport stream (TS) [14]. Figure 2.10 shows the TS syntax. The TS packets have a length of 188 bytes so that the payload is 184 bytes. The fixed length of transport packets is used to ease introduction of error control methods in the transmission process. The packet identifier (PID) identifies what kind of program the payload contains (e.g., a pay-TV program) [7].

sync byte	Transport error indicator	Payload unit start indicator	Transport scrambling control	Transport priority	PID	Adaptation field control	Continuity counter	Payload
8	1	2	2	1	12	2	4	

Figure 2.10 MPEG-2 TS Syntax [7]

The MPEG-2 implements a flexible architecture to allow a multi-standard environment where one system is able to output video and audio signals in low-definition TV (LDTV); standard-definition TV (SDTV) like NTSC, PAL, and SECAM; and HDTV. The most important contribution of MPEG-2 is that it gives an integrated transport mechanism for multiplexing the video, audio, and other data through packet generation and time division multiplex (TDM) [7].

2.3.4 Conditional Access

Satellite TV systems use conditional access (CA) methods to avoid unauthorized access to the offered programming. The insertion of CA into IRDs is an essential factor in the economics of broadcast services.

CA systems are based on two basic techniques: scrambling and encryption. Scrambling is required to render the transmitted signal meaningless to the IRD unequipped with a means of descrambling the received transmission. The ability of an IRD to descramble is conveyed to the receiver in the form of a key or covert digital number, and an encryption process is required to make this key secret.

In DVB, there are only a few packet types that must be transmitted without scrambling. Obviously, these include part of the service information (SI) stream such as the Program Association Table (PAT) and the Network Information Table (NIT). These data streams need to be transmitted without scrambling so that any DVB-compliant receiver can access this specific information.

The system to support DVB-CA requires a database, known as the subscriber management system (SMS), to manage the subscribers, their address, and program requirements. The program requirements are sent to the IRD using an appropriately structured message known as the entitlement management message (EMM). The CA system timing and synchronization, together with the current encryption key, are sent in

the entitlement control message (ECM). These terms apply to the system adopted by the DVB standard.

DVB uses two basic CA procedures: Simulcrypt and Multicrypt. An IRD implemented with Simulcrypt would only work on a network that is set up for this CA arrangement. In contrast, an IRD implemented with Multicrypt is able to work with a common interface (DVB-CI) to allow an open-system approach to normally proprietary CA system architecture. There are a number of different companies providing DVB-compatible CA systems (e.g., Nagravision, Irdeto, and Seca), so when DBS providers start a service, they have many options from which to choose. It is important to carefully consider the CA system when the transmission standard is not compatible with DVB-S. (Consider, for example, VideoGuard, which is used with DirecTV.)

The key used for the encryption process is usually transmitted over the satellite link along with the programming and other information. This is the most efficient and successful means of delivery of the electronic key. Users, identified by a smart card that also has a unique key, ask and pay for wanted programming via a terrestrial return channel using a voice-grade modem. Most smart card serial interfaces operate in the 9,600 – 38,400 –bps range. The key used to scramble the program changes over time. The serial communication between CI and the smart card occurs with a burst of data every few seconds.

Scrambling of the appropriate bit streams is performed at the uplink site. The MPEG-2 packets are encrypted by the usual techniques based on a common key known to both the scrambling and decryption devices. When a scrambled packet arrives, it is passed through the CI, which takes the key obtained from the smart card and uses it to turn the packet payload back into an MPEG-2 transport payload that can be processed by the rest of the system.

The standards like DVB and ATSC have defined CA protocols. These protocols specify the encryption of content and the transfer of CA control messages in the MPEG-2

transport stream (TS) (See Figure 2.11). The control messages themselves are proprietary for the CA system. The conditional access system includes several components, each performing specific tasks. These are:

- Entitlement Management Message Generator (EMM Generator) and auxiliary components
- Entitlement Control Message Generator (ECM Generator) and auxiliary components
- Security Server
- Control Word Generator

ECM

Entitlement ECM defines the program's access requirements, specifying the tiers required for subscription and the cost associated with the impulse purchase of the program. Encrypted program keys are delivered in the ECM stream [12]. The ECM consists of

- Control Word (CW) (which is the content encryption key)
- Content_Id
- Description of the rights required to access content

EMM

Entitlement Management Messages (EMM) define access rights for each individual decoder. The EMM stream is processed with the access control device, but the user processor is responsible for buffering EMM and feeding them via an interface to the access control device [12]. The EMM consists of

- Subscriber_Id
- Rights update

Security Server

Security Server provides the algorithm that is used to encrypt the CW and the content.

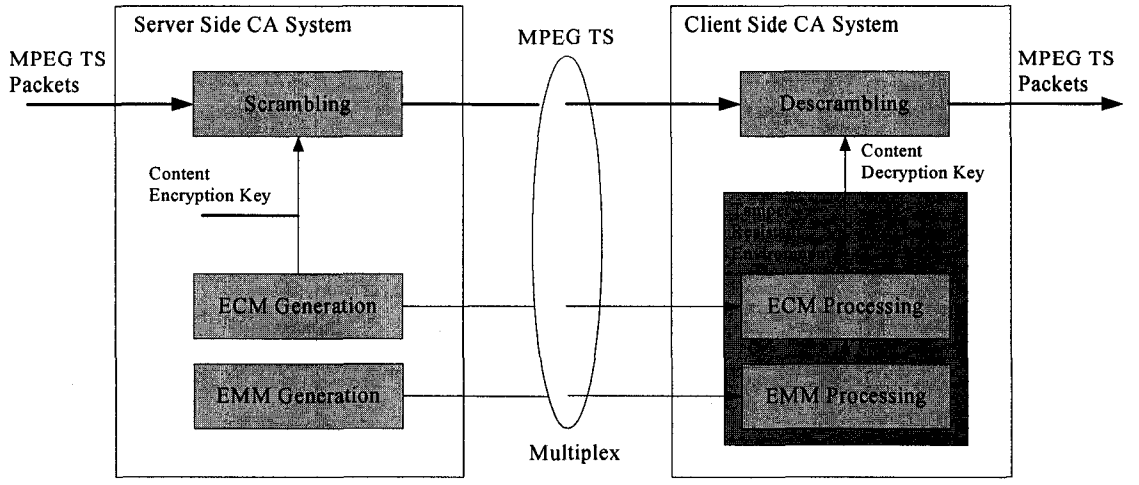


Figure 2.11 MPEG-2 CA Systems

2.4 Cryptology for Digital Video

Cryptography currently plays a major role in many information technology applications, especially in broadcasting systems. In cryptography, a message is called either plaintext or cleartext. The process of disguising a message in such a way as to hide its substance without changing its meaning is called encryption. An encrypted message is called ciphertext. The process of turning ciphertext back into plaintext is called decryption. [13]

To protect a message, a sender encrypts a plaintext into ciphertext. The ciphertext is transmitted over the data communications channel such as the Internet, broadcasting, or wireless. If the message is intercepted, the intruder only has access to the unintelligible ciphertext. Then, the receiver decrypts the ciphertext into its original plaintext format. The encryption and decryption concepts are illustrated in Figure 2.12.

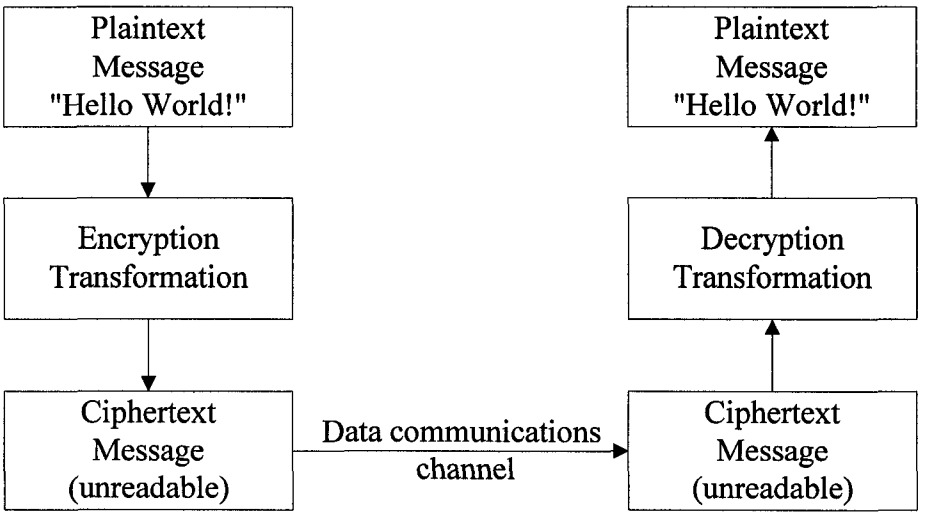


Figure 2.12 Message Encrypt and decrypt

The mathematical operators used to transmit message between plaintext and ciphertext are identified by cryptographic algorithms.

There are various techniques used to encrypt digital TV signals today. But they can be distinguished by two types of cryptographic algorithms. One is symmetric-key, also called private-key. Another is asymmetric-key or public-key.

2.4.1 Symmetric-key

Symmetric-key cryptography is characterized by the use of a single key to perform both the encrypting and decrypting of data. Classical examples are Caesar cypher, one-time pad, Enigma; current fast algorithms are 3DES, RC4, RC6, IDEA, Blowfish, Twofish, Mars, and so on. Most of them were used in SSL, SSH, AES, and PGP. Generally speaking, symmetric key encryption is fast and secure. But the problem is that, although symmetric-key encryption works well locally, it does not work very well across networks and broadcasting systems. The problem is that, for receivers to be able to decrypt the packets, they must use the key. This means that you must send them that key along with the message. The other problem is that you are sending the packets across an insecure channel. If it were secure, there would be no reason to encrypt the message in the first

place. This means that anyone who might be monitoring the network could steal the encrypted packets and the key necessary for decrypting them [14][15].

Here we just introduce the most common one, DES (Data Encryption Standard). DES encrypts and decrypts data in 64-bit blocks, using a 64-bit key (although the effective key strength is only 56 bits, as explained below). It takes a 64-bit block of plaintext as input and outputs a 64-bit block of ciphertext. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm, DES is both a block cipher and a product cipher.

DES has 16 rounds, meaning the main algorithm is repeated 16 times to produce the ciphertext. It has been found that the number of rounds is exponentially proportional to the amount of time required to find a key using a brute-force attack. So as the number of rounds increases, the security of the algorithm increases exponentially.

2.4.2 Asymmetric-Key

Asymmetric-key cryptography uses a pair of different cryptographic keys to encrypt and decrypt the plain text. Typically, the two keys are related mathematically; a message encrypted by the algorithm using one key can be decrypted by the same algorithm using the other. The most popular scheme is RSA. Other asymmetric algorithm are Elliptic Curves Cryptography (ECC) and Diffie-Hellman system. Public-key encryption, on the other hand, uses a pair of keys. It uses a public key that is sent along with the message and a private key, which is always in the possession of the recipient. The private key is based on a derivative of the public key, and only the two keys working together can decrypt the packets. Because the private key is never sent across the network, it remains secure. The down side of public-key encryption is that it tends to be very slow and resource-intensive. This makes it difficult to send large amounts of data using public-key encryption [14].

Comparing ECC and RSA, ECC is faster and the key is shorter. In this thesis, we mainly investigate elliptic curve cryptography to encrypt the digital TV signals. So here we only discuss elliptic curve cryptography.

- **Elliptic Curve**

An elliptic curve E over the field F is a smooth curve in the so-called "long Weierstrass form" [17]: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ (2.1)

The variables x and y can be complex, real, integers, polynomial base, optimal normal base, or any other kind of field element. In this report, we simulate an elliptic curve over an optimal normal basis.

Studies show that two kinds of elliptic curves can be chosen for cryptography [16]: supersingular elliptic curve (Equation 2.2) and non-supersingular elliptic curve (Equation 2.3).

$$y^2 + y = x^3 + a_4x + a_6 \quad (2.2)$$

$$y^2 + xy = x^3 + a_2x^2 + a_6 \quad (2.3)$$

Having some special characteristics, the supersingular elliptic curve is not suitable for cryptography. Because as long as the counterpart masters these characteristics, it will be easy for him/her to break the crypto-system. So in this thesis, we introduce a non-supersingular elliptic curve.

Two factors are very important in deciding the security level of the crypto-system: bit size and elliptic curve. Normally the longer the bit size is, the more difficult it is to break the keys, but also the more costly the crypto-system will be.

To select an elliptic curve, the first step is to decide the coefficients in Equation 2.3. For this equation to be valid, a_6 must never be 0; however, a_2 can be 0. So according to whether a_2 is zero or not, the non-supersingular elliptic curve can be divided into two forms: "Form 0" (Equation 2.4) and "Form 1" (Equation 2.3). During the simulation, the

users can choose to simulate either one of the elliptic curves, and a_2 as well as a_6 are generated randomly.

$$y^2 + xy = x^3 + a_6 \qquad (2.4)$$

➢ **Mathematics for the Elliptic Curve**

Scientists define addition, multiplication, and reverse over elliptic curves. These definitions have different implementations among real number, polynomial, and optimal normal basis. Details of these definitions can be found in reference [16]. Here we only discuss multiplication.

$$Q = kP \qquad (2.5)$$

where Q and P are points on an elliptic curve, and k is a integer. Equation 2.5 means we add P to itself k times. For example, we want to compute $15P$. We can expand this as:

$$15P = P + 2(P + 2(P + 2P)) \qquad (2.6)$$

Since $15 = 1111_2$, starting the chain with 0, the most significant bit is set so we add P. Then double the result (2*) and add P, repeating until all bits are done. This expansion requires 3 doubling operations and 3 sums, a total of 6 operations instead of 15.

➢ **Public Key and Private Key**

In the ECCS, we need an elliptic curve E and a base point G (a point over E) for the public and private key pair. Both the elliptic curve coefficients and the base point are randomly generated. The procedure to generate a public key and private key pair can be stated as following:

1) Choose a random number K as the private key.

2) Obtain the corresponding public key by equation P = KG, where P is the public key, K is the private key, and G is the base point.

➢ **Functional Mechanism of an ECCS**

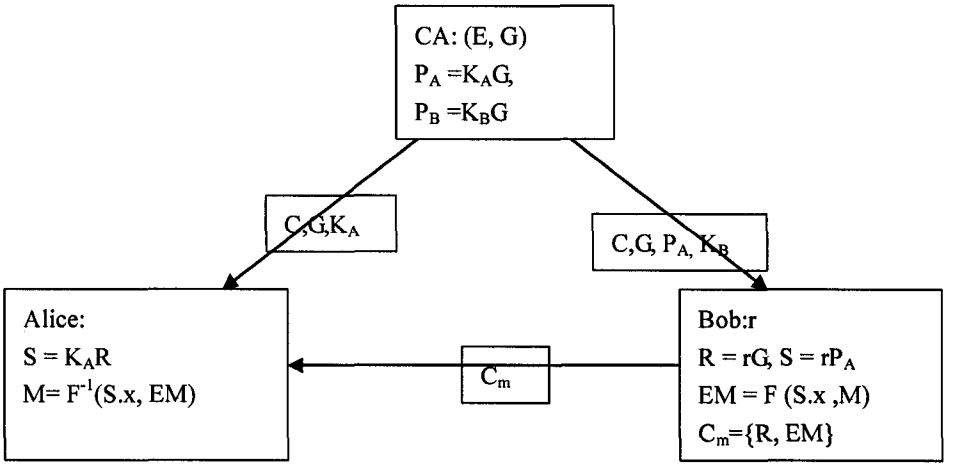


Figure 2.13 An Elliptic Curve Crypto-System

An ECCS functional model is given in Figure 2.13. A CA here refers to a certificate agent. Alice and Bob are the partners that would like to communicate with each other. For simplicity, we only need to illustrate how Bob transmits a message to Alice.

Before communication, each user client needs to buy a certificate from the certificate agent. A certificate in this report includes an elliptic curve E, a base point G, a private key K, and a public key P. Analog to Diffie-Hellman key exchange protocol, in this system the two communication partners need to exchange public keys and calculate some shared secrets.

➢ Data Encryption

To transmit the message to Alice, Bob needs to do the following work:

1) Obtain Alice's public key P_A from the certificate agent.

2) Generate a random one-time key r.

3) Hide the one-time key into one hidden point R over the elliptic curve E using the base point G. The relationship between them are as follows:

$$R = rG \qquad (2.5)$$

4) Using the one-time key r and Alice's public key P_A to calculate the shared secret:

$$S = r P_A \qquad (2.6)$$

5) Using X component of S to encrypt the message M into EM, a mask generation function is used for the message encryption.

6) Transfer the cipher text C_m to Alice. The cipher text C_m includes two parts: the hidden point R and the encoded message EM.

➢ Data Decryption

Upon receiving the ciphertext C_m, Alice will do the following tasks to decrypt the message M.

1) Calculate the shared secret S by the following equation:

$$S = KR \qquad (2.7)$$

2) Use the X component of the shared secret to decode EM to M.

Since $S = KR = KrG = rKG = r\ P_A$, then we know that both Alice and Bob can get the same shared secret so that we can get the message M correctly.

Chapter 3

Commercial Satellite Encryption System

3.1 Introduction

As mentioned before, there are several different encryption systems used in Pay-TV, such as Irdeto, VIAccess, Nagravision, Conax, SECA, Cryptoworks, and Betacrypt etc.

- The Irdeto system offers Irdeto Pisys, Irdeto M-Crypt, Irdeto CypherCast - different products for various implementations. They use different encryption/decryption algorithms such as 3DES, Blowfish (56 / 128 bit), and 128-bit AES Rijndael encryption.

- Nagravision uses the IDEA algorithm with a 128-bit key, reputed to be the most secure on the market and used in encryption modules and smart cards.

- Betacrypt 2 offers a set of revolutionary security functions such as 128-bit key length and adaptive security mechanisms.

- The VIAccess system uses DES algorithms.

Most encryption systems use symmetric-key cryptography.

3.2 Irdeto

Figure 3.1 shows a cursory draft of the Irdeto system.

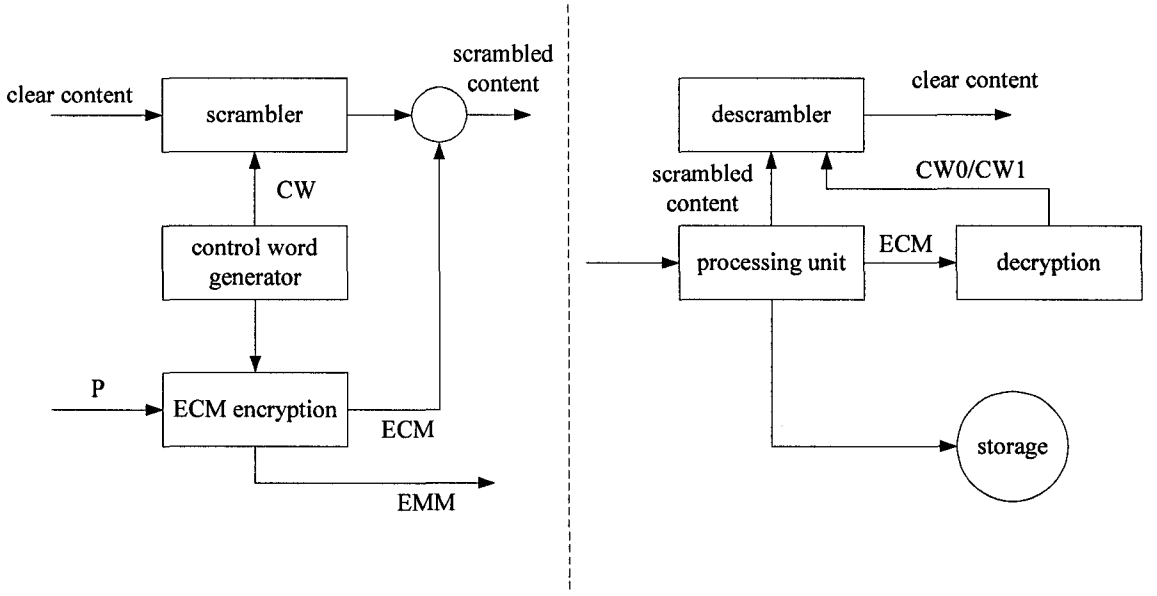


Figure 3.1 Irdeto System [19]

The IRDETO system is mainly composed of the following modules:

- ✓ **Conditional Access (CA)**

  The CA system provides the features to control the subscribers' access to the services. A Subscriber Management System passes on to the Integrated Receiver Decoder (IRD) SmartCard the Entitlement Management Messages (EMM), which includes the subscriber control information and commands. The control information and commands have the key R, which the IRD need to descramble the content.

- ✓ **Network Management System**

  The Network Management System controls the digital play-out and integrates the system and conditional access information carried within the MPEG-2 data stream. The system also generates Program-Specific Information (PSI) and Service Information (SI) tables according to DVB standards. The Network Management System provides multiplexer and encoder management to guarantee that each service can be played with its correct information.

- ✓ **Conditional Access Module**

  The Conditional Access Module is capable of processing MPEG-2 data at 54 Mb/s; it descrambles the MPEG-2/DVB data stream and filters off ECMs and EMMs under the control of the SmartCard. Then it gets the control words to descramble the content.

- ✓ **SmartCard**

  A SmartCard is used together with the CA Module in the IRD to control access to television programs and services broadcast in scrambled form. It processes the information on viewing and access rights. [18]

3.3 Nagravision

Nagravision offers licenses using the IDEA™ algorithm with a 128 bit key used in encryption modules and SmartCards.

Figure 3.2 shows how a CAM (Conditional Access Module)/SmartCard combination handles a Nagravision encrypted satellite signal.

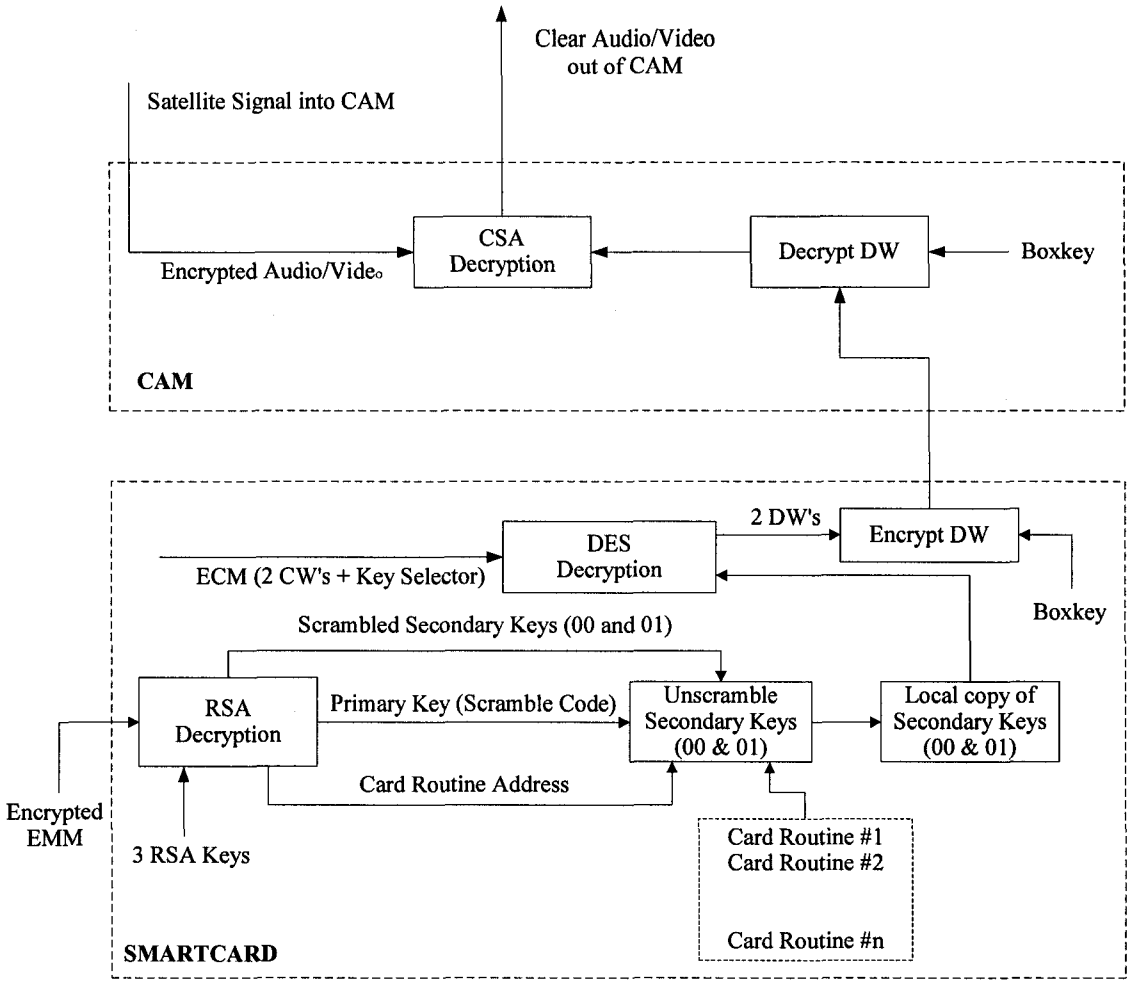


Figure 3.2 Nagravision CA

The satellite signal is fed to the CAM from the receiver; the CAM then applies the CSA decryption algorithm to decrypt the audio/video and passes the clear audio/video signal back to the receiver. CSA is an abbreviation for **Common Scrambling Algorithm**, which is employed in almost every scrambled digital-TV-channel so far. Those MPEG-streams are encrypted with this algorithm, which needs an eight-byte seed for initialization (up until now, only six bytes are used), in order to be able to descramble the encrypted TV signal.

In order for the CSA decryption algorithm to work, a pair of DW (decryptoworks) encryption keys (the seeds in CSA) is required, and this pair is passed to the CAM from the SmartCard.

The satellite signal contains periodic ECMs, each of which specifies a pair of CW (cryptoworks) keys and a key selector. A CW pair is used to generate a DW pair, which in turn is used by the CAM to clear a stream of audio/video. ECMs are therefore passed to the SmartCard from the CAM, whereupon the SmartCard decrypts the CW pairs using the DES decryption algorithm and, in doing so, generates the DW pairs required by the CAM.

In order for the DES decryption algorithm to work, a secondary key (00 or 01) is required. The secondary key used by the DES decryption algorithm on a given DW pair is determined by the key selector associated with that DW pair. Also, since the SmartCard needs to be married to the CAM, then prior to passing the DW pairs to the CAM, the SmartCard encrypts them with a boxkey. At the CAM side, the DW pairs are decrypted using the same boxkey, and the DW pairs are then used by the CSA algorithm to clear the audio/video. If the boxkeys in the SmartCard and CAM are not the same, then the DW pairs decrypted by the CAM will not be the same, as the DW pairs encrypted by the SmartCard and the CSA algorithm will not therefore be able to clear the audio/video.

The satellite signal also contains periodic EMMs, some of which contain key updates. SmartCards containing AU files decrypt EMMs using the RSA decryption algorithm. In order for the EMM decryption algorithm to work, a set of three RSA keys is required, which are programmed onto the SmartCard (note: there are different RSA key sets for different SmartCard types). When an EMM containing a valid key update is decrypted, the SmartCard is then able to read a primary key (which is clear) and a pair of secondary keys (00 and 01), which are scrambled. The SmartCard then unscrambles the secondary keys (00 and 01) using the primary key (which is a scramble code routine) and a routine, which is already programmed on the SmartCard.

The EMM specifies the address of the card routine, which is used to unscramble the secondary keys (00 and 01). Smartcards are programmed with all the card routines (both past and future) necessary to be able to unscramble the secondary keys (00 and 01).

Once the SmartCard has managed to unscramble the secondary keys (00 and 01), it then stores these keys locally so that the SmartCard does not need to repeat the time-consuming process of deriving them from the EMM the next time the receiver is powered up. These stored secondary keys (00 and 01) are then used by the DES decryption algorithm to decrypt the CW contained in the ECM and, in doing so, generate the DW's needed by the CAM. [20]

3.4 VIAccess

VIAccess is a modification of Eurocrypt M. In this modification, the key has eight bytes, whereas EC-M has only seven. If the eighth byte is zero, then VIAccess works exactly like EC-M. If the eighth byte is nonzero, then this will trigger several different small modifications. One of these modifications is in DES routine. Seven key bytes are used in DES, but the eighth byte is used in the special core function in every DES round. This modification is done just before expansion E, and it alters the fifth data byte, which is the first of the right-hand four data bytes to be used in the DES-round. Therefore, it affects S-boxes 1, 2, 3 and 8. The modification is done only with this byte for expansion E, and the original byte remains the same.

In this modification the eighth key byte is multiplied with the data byte to get a 16-bit word. Then the data byte is added to this word (upper eight-bit byte is incremented if there was a carry with the lower byte). Then the eighth key byte is added to the word in the same way. Then the upper byte is subtracted from the lower byte. If there is a carry in this subtract, then the result is incremented by one. Then this result byte is used instead of the original byte in expansion E.

Another modification in the DES routine is the permutation table used after xoring the bytes of the expanded data with the modified keys data. The new permutation table is

32	15	4	9
25	24	20	1
5	31	11	18
13	2	27	30
28	19	7	21
3	29	26	14
10	23	8	17

Table 3-1 VIAccess DES Key Table

Key

If the eighth keybyte is nonzero, then the first seven keybytes are rotated left by two bytes. This means key (k1 k2 k3 k4 k5 k6 k7 k8) -> key (k3 k4 k5 k6 k7 k1 k2 k8). This modified key is used in the DES routine, but in the hash routine we have to use the non-modified key.

Hash

All hash algorithms work as the do in EC-M when this DES modification is done.

CA 88 and CA 18 message processing:

If the eighth key byte is even, then this is the last modification, but if it is odd, then there is still one very complicated data modification. First there is one constant, which is 5Ah if the eighth key byte is odd, and its lower byte is equal to zero. If the eighth byte is odd, its lower byte is not equal to zero, then this constant is A5h.

We have to calculate the hash like we do in encryption, but the encrypted words included in the data field have to be processed with the k constant to build the real encrypted word.

The bytes of the sanded CW are first ANDed with the constant and then XORed with the encrypted data bytes. The resulting bytes are then stored in the real encrypted word,

which is used as input data for DES. Of course, DES is done with necessary modifications. The non-modified bytes of the CW are still used to continue the hash processing. After DES, the resulting bytes are ready for the CA C0 message or other uses in CA 18 messages. [23]

3.5 Signal Pirating Problem

Various pirate technologies currently completely compromise satellite TV signals. Auto roll on some pirate technologies has made frequent key changes ineffective against signal compromise.

Some pirate technologies (e.g., Syndrome) can retrieve the new keys automatically from the satellite stream (auto roll). Keys are distributed through pirate Web sites (e.g., www.dishnewbies.com, www.satellites.co.uk/) for technologies that do not auto roll.

If you search on the Internet, you will be able to find a batch of Web sites that offer the keys for all Pay-TV programs on satellite, including all the systems that I mentioned above. Obviously, all those encryption systems are not very "secure." The major weakness in those encryption systems is that symmetric key cryptography does not work very well across Internet, because keys are shared by many users. The following is a sample procedure of signal stealing (SmartCard-based):

- Use the JTAG facility of the receiver to read the ID number of the receiver.
- Buy a SmartCard emulator from a vendor.
- Enter the ID number of the receiver and the SmartCard number for basic program subscription from the service provider into the emulator.

Plug the emulator into the SmartCard receptacle of the Set-Top Box (STB), and the emulator will then generate the appropriate number for the STB to generate the key for all the programs.

JTAG is a standard test interface defined by the Joint Test Action Group and supported on many late-model digital receivers for factory test purposes. Operating using a six-wire interface and a personal computer, the JTAG interface was originally intended to provide a means to test and debug embedded hardware and software. In the satellite TV world, JTAG is most often used to obtain read-write access to nonvolatile memory within a digital receiver; initially, programs such as Wall and JKeys were used to read box keys from receivers with embedded CAM but JTAG has since proven its legitimate worth to satellite TV fans as a repair tool to fix receivers where the firmware (in flash memory) has been corrupted.

The *Sombrero de Patel* is another device used to obtain direct memory access to a receiver without physically removing memory chips from the board to place them in sockets or read them with a specialized device programmer. The device consists of a standard PLCC integrated circuit socket which has been turned upside-down in order to be placed directly over a microprocessor already permanently soldered to a printed circuit board in a receiver. The socket makes electrical contact with all of the microprocessor's pins and is interfaced to one or more microcontrollers, which use direct memory access to pause the receiver's microprocessor and read or write directly to the memory. The term *sombrero* is used for this hack, as the novel use of an inverted IC socket somewhat resembles a hat being placed upon the main processor. [21]

Chapter 4

ECC in Real Time for Digital Television Broadcast

As we discussed in Chapter 4, the most current commercial satellite encryption systems use symmetric-key cryptography. The symmetric key is stored in the SmartCard for distribution. Those systems have one common feature: the symmetric-key can be copied easily by unauthorized persons. To avoid those weak points, we proposed a public-key cryptograph technology-based security system for DVB, which is ECC in a real-time system.

To avoid this, the public-key cryptography technique is used in the Set-Top Box to ensure that it will only read the subscription information from a SmartCard with the same serial number as its own during a boot-up process. Otherwise, the Set-Top Box will not boot up.

4.1 Proposed Methodology Introduction

The proposed security system for DVB consists of three parts: the broadcast center encryption part, the set-top box (STB) decryption part and the SmartCard-based key part.

Figure 4.1 shows a proposed Direct Broadcast Satellite System. In this system, the programming sources part is not included. The Direct Broadcast Satellite system was discussed in Chapter 2. The most important parts of the system are the Broadcast Center and the receiver or Set-Top Box.

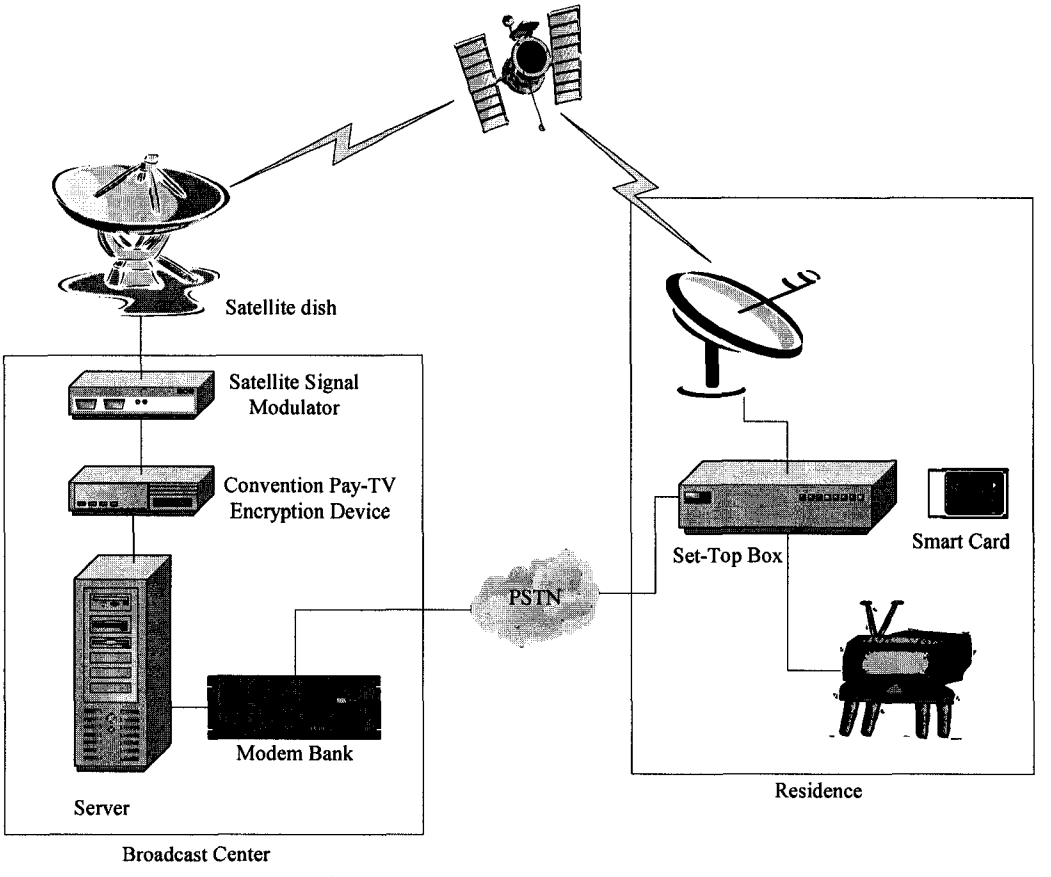


Figure 4.1 Proposed Systems

The Broadcast Center broadcasts an encrypted Pay-TV program to a set of subscribers via a satellite. Each subscriber has a Set-Top Box, which receives and decrypts the encrypted Pay-TV program if the subscriber is entitled to the TV program.

4.1.1 Broadcast Center

The Broadcast Center includes a lot of aspects, which we already discussed in Chapter 2. The main functions of the Broadcast Center is to generate Control Word to encrypt video/audio signals and the CA information, packetized to the MPEG transport stream, and use the terrestrial uplink transmitter to the stream to a satellite. In our proposed method, we focus on part of CA – how to manage keys.

All the various public and private keys such as public and private keys A and B used in authentication of SmartCards and encryption/decryption of Pay-TV signals are stored in the memory of the Broadcast Center. Public Key B and Private Key B are used to encrypt and decrypt the Pay-TV signal. Public Key A and Private Key A are used to encrypt and decrypt the user profile and the serial number of the STB. The Private Key is transmitted in ECM (Entitlement Control Message Stream):

Broadcast Center	Public Key A	Public Key B
	Private Key A	Private Key B

Table 4-1 Broadcast Center Key Storage

The Control Word is auto exchanged. The Keys can be auto upgraded.

4.1.2 Set-Top Box (STB)

Unlike a traditional STB, the proposed STB uses different algorithms to authenticate and to decrypt Pay-TV signals. The STB store encrypted private keys and the serial number of the STB. The STB only reads from the SmartCard with the same serial number, thus providing a secure way to authenticate whether a SmartCard contains the authorized information to operate the STB.

Set-Top Box	Encrypted Private Key A Serial Number of STB

Table 4-2 STB Key Storage

Differences between the traditional STB and the proposed STB also include the encryption/decryption of Pay-TV signals using more computational public-key cryptography techniques and the secure update of user profile and private keys in the proposed STB using a PSTN channel. In this system, we use ECC public-key cryptography.

4.1.3 SmartCard

To prevent people from copying the SmartCard, only the encrypted user profile and the serial number of the STB are stored in the SmartCard. Because of the fact that the user profile and the serial number are encrypted by Public Key A, only the Private Key A stored in the memory of the STB can be used to decrypt the information.

SmartCard	Encrypted User Profile using Public Key A (User profile contains information on subscription, serial number of the STB and Private Key B)

Table 4-3 SmartCard Key Storage

4.2 Proposed Methodology

Now we discuss the details of this proposed methodology and show how it works efficiently to prevent signal pirating.

4.2.1 Boot-Up Set-Top Box

First, in this system, during the Set-Top boot up, the Set-Top authenticates the SmartCard. If the SmartCard is not an authenticated one, then the Set-Top will shut down. The flowchart showing the authentication sequence between the STB and the SmartCard during a boot up of the STB is shown in Figure 4.2.

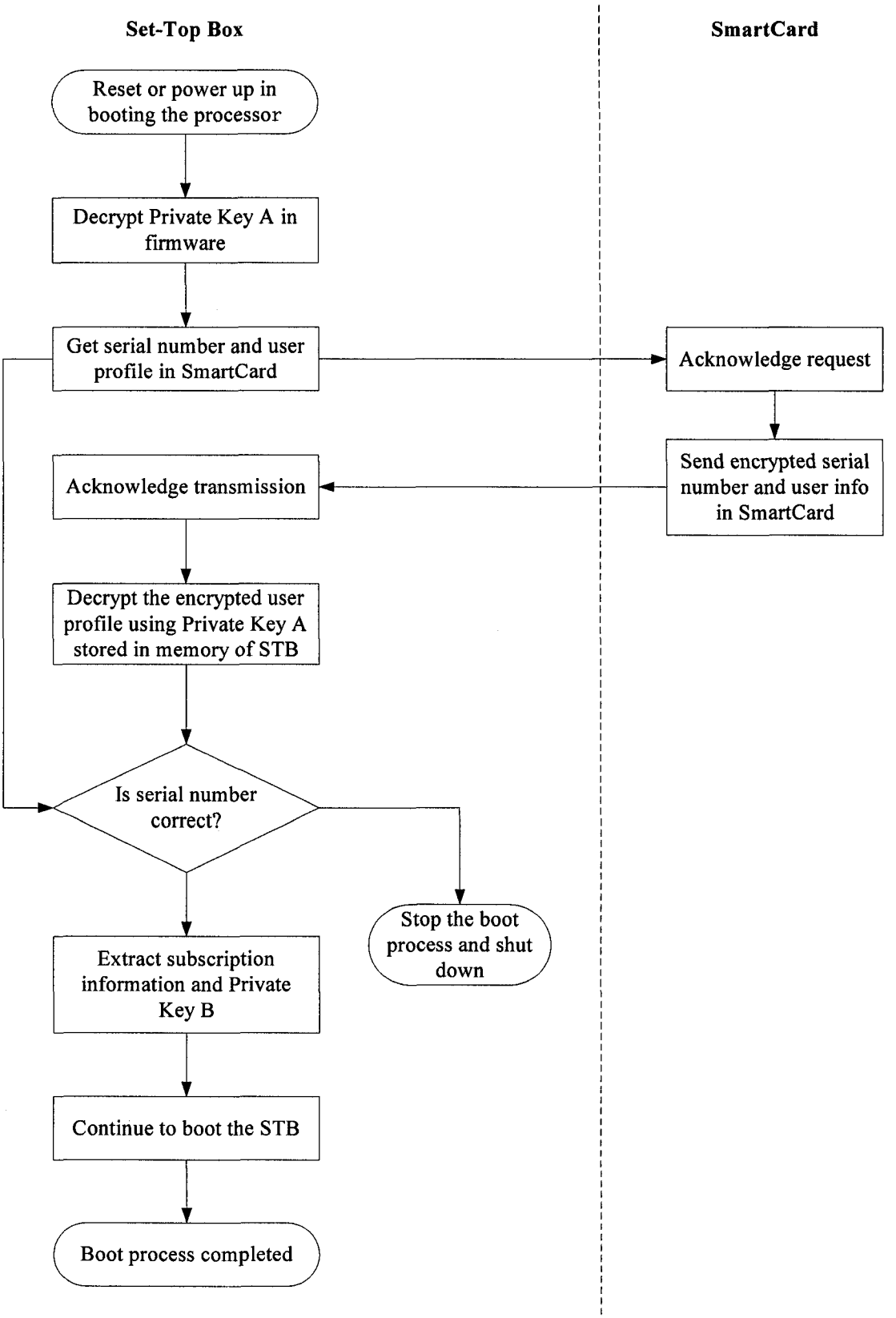


Figure 4.2 Boot-Up the STB

The STB enters the boot-up sequence as soon as the STB is switched on. To make it difficult to copy Private Key A stored in the memory of the STB, it is advisable to encrypt Private Key A. To extract Private Key A, the STB executes a piece of boot-up firmware to decrypted Private Key A and stores the key in its random access memory so that it can be used later.

The STB then reads from the SmartCard the encrypted user profile and decrypts the encrypted user profile using Private Key A. The STB compares the extracted serial number from the SmartCard with the serial number stored in its flash memory. If the two numbers are the same, then the SmartCard is authenticated in order to be correct, and the boot-up process continues. Otherwise, the STB immediately terminates the boot-up process, making it inactive.

Once the SmartCard is authenticated correctly, the STB continues to extract and stores the decrypted information in the random access memory of the STB. The decrypted user profile contains information such as the length of subscription, type of subscription, and Private Key B.

4.2.2 Update user profile

Second part, this system can auto upgrade the keys. The Broadcast Conter will send an update message to Set-Top box using the EMM (Entitlement Management Message) Stream. Then the Set-Top box will process the update. During the process, the Broadcast Conter will check if this Set-Top box is authenticated again.

Figure 4.3 shows the process.

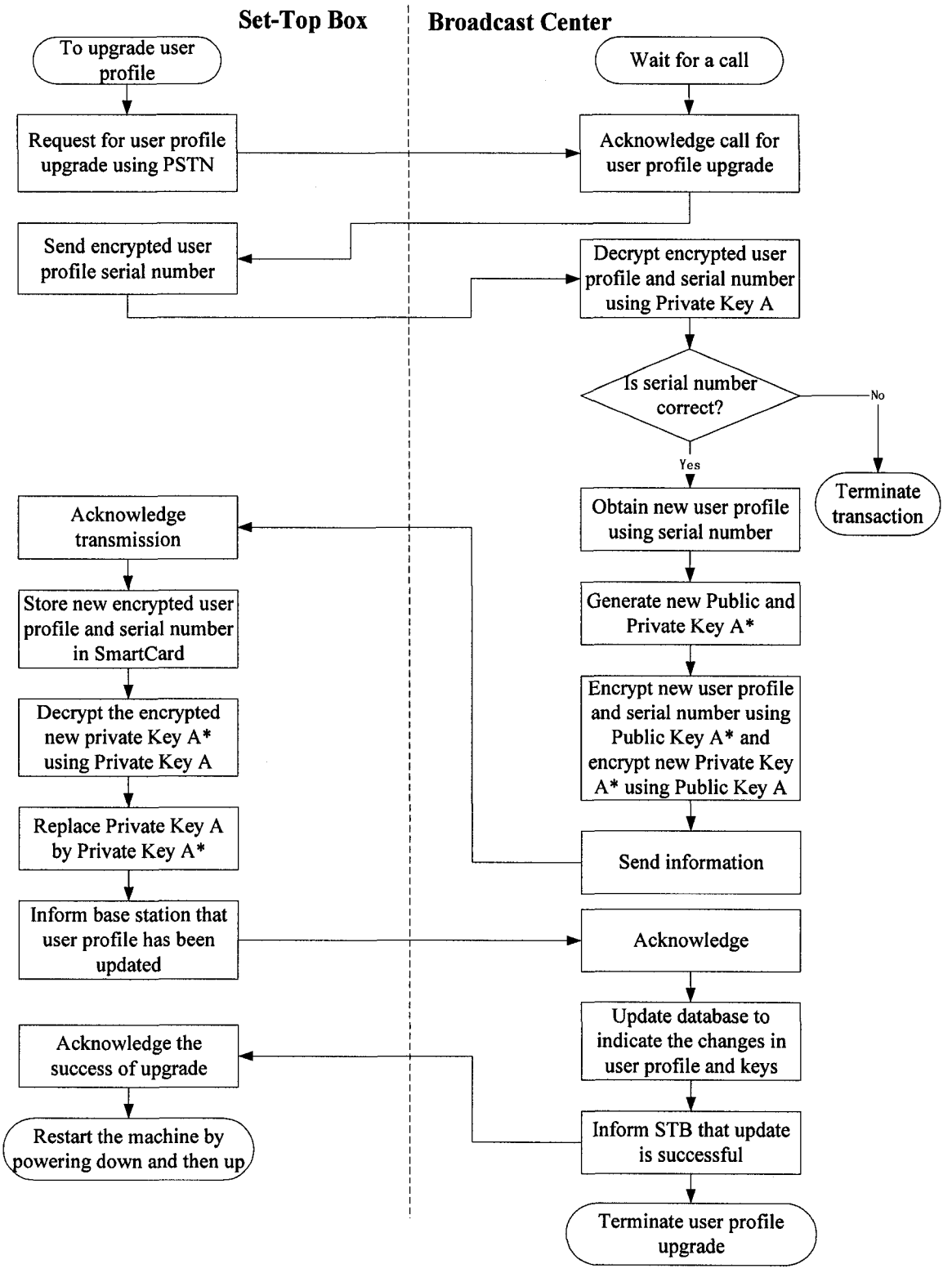


Figure 4.3 Update User Profile

When an STB gets the EMM from the Broadcast Center, the STB will check if it needs to be updated. If so, then the STB requests a new user profile from the Broadcast Center through PSTN.

It first sends the encrypted old user profile to the server, as shown in Figure 4.3. To avoid a fake call, the server in the Broadcast Center decrypts the encrypted old user profile using its own private key A and compares the serial number with the serial number stored in its database. If the serial numbers are not the same, then the call is disconnected. If both serial numbers are the same, then the server proceeds to fetch new user profile, generates new private and public keys A*, and associates and stores the new keys with the serial number in its database. The server then encrypts the new user profile with Public Key A* and Private Key A* with the old public key A. It then sends the encrypted information to STB.

After the STB receives the encrypted information, it stores the new encrypted user profile in the SmartCard. It decrypts the new private key A* with its own private key A. It then replaces the private key A with the new private key A* in its memory, and then powers down. When the STB powers up, it will follow the same power-up sequence shown in Figure 4.2.

4.2.3 Encryption and Decryption of Digital Signals

The third part is also the main part of this system - encryption and decryption of the signal. In this thesis, we consider two different ways to do encryption and decryption. Figure 4.4 shows the data flow. We have three different methods: two methods combine two symmetric-key and asymmetric-key cryptographic algorithms together; one only uses asymmetric-key. But in all methods, the asymmetric-key is the primary method.

In Chapter 3, we mentioned several cryptographic algorithms. But in this thesis, encryption/decryption cryptography is based on fast ECC encryption/decryption protocol.

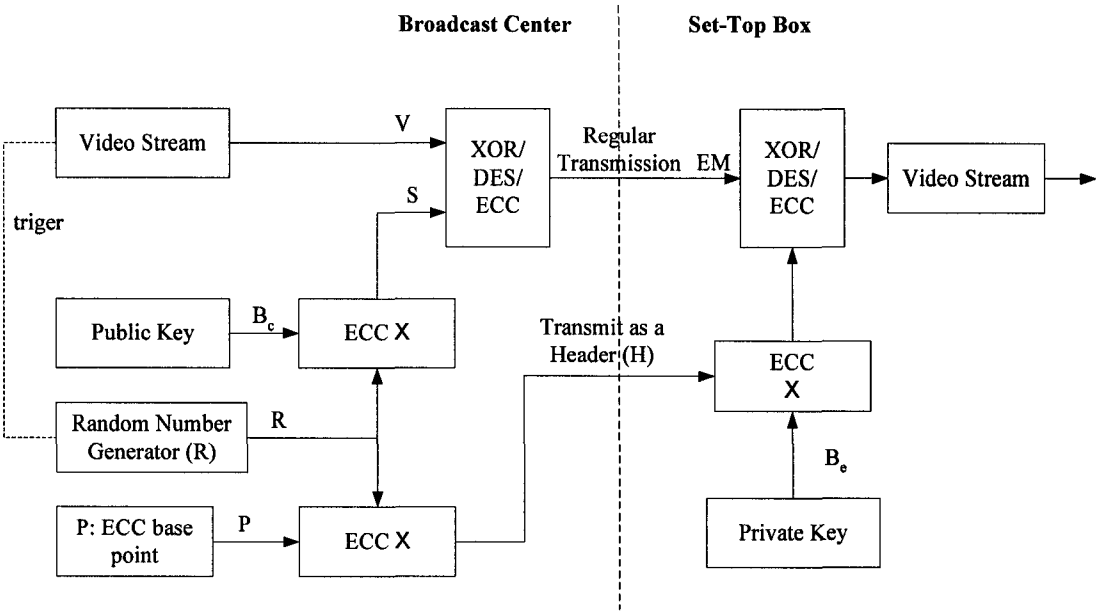


Figure 4.4 Proposed Methods

In the Broadcast Center, there is a random number generator to generate random number R (also called Control Word). P is a base point on an elliptic curve. Hide the one-time key R into one hidden point P over the elliptic curve using the base point P.

$$H = R \times P \tag{4.1}$$

H will be delivered in the ECM stream.

Using the one-time key R and the public key B_c to get the shared secret:

$$S = R \times B_c \tag{4.2}$$

The video streams are encrypted by the X component of S. To archive this, we have proposed two ways (XOR 4.3 and ECC 4.4) to encrypt the video stream and also test the traditional method DES (4.4).

a) XOR: S key stream XOR with video stream V.

$$EM = S \oplus V \tag{4.3}$$

b) DES:

$$EM = DES(S.x, V) \tag{4.4}$$

c) ECC:

$$EM = F(S.x, V) \tag{4.5}$$

Then broadcast using regular transmissions to broadcast EM.

In the Set-top Box side, we need to get the shared secret S. In order to get the S, first the STB gets the encrypted Control Word H, then it uses Private Key B_e to multiply H.

$$B_e \times H$$

Because $H = R \times P$, then it will be

$$B_e \times R \times P$$

As we know $B_e \times P = B_c$, so we get shared secret S.

$$\begin{aligned} S &= B_e \times H \\ &= B_e \times R \times P \\ &= B_c \times R \end{aligned} \qquad (4.6)$$

Equation 4.6 is the same as equation 4.2.

After we get S, we use the associated method (XOR/DES/ECC) to decrypt EM and get video stream V.

In this system, the random number R is changed depending on the video stream.

Chapter 5

Simulation Results

Computer simulation of the proposed encryption system is constructed to test the computation time needed to encrypt/decrypt the video content to verify whether the algorithm is suitable to be used in real-time video signal encryption and decryption. The robustness of algorithms has been also examined in simulation to know if the proposed methods are practical.

The simulation program has two parts. One is the encryption part, another one is the decryption part. The three cryptograph methods XOR, DES and ECC have been developed for video stream encryption/decryption based on equations 4.3, 4.4, and 4.5.

5.1 Assumptions

In the computer simulation process, we do not have a satellite for transmission. So we could not have transport streams as input or output for the computer simulation program. Based on the above reasons, we make the following assumptions:

- Use disk write/read as satellite transmission

- Delay (disk speed)
- Use MPEG files as the Broadcast Center video program
- Use encrypted files as a signal from the satellite
- Use the JPEG file to display the system error rate

5.2 Encryption Part

The program flow chart is shown in Figure 5.1. In the simulation program, the three cryptography algorithms have been deployed to encrypt the video stream:

- Symmetric-key cryptography: XOR and DES
- Asymmetric-key cryptography: ECC

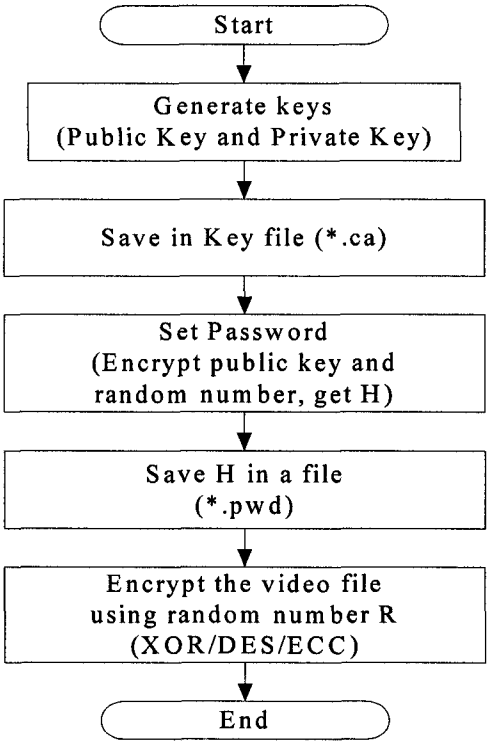


Figure 5.1 Encryption Program Flow Chart

To encrypt the data, use the void CEncryptDlg::OnEncrypt() function (part of the function).

```
void CEncryptDlg::OnEncrypt()
{
	if(myDial.DoModal()==IDOK)
	{
		FILE *fpR;
		FILE *fpW;
		CString PlainFile=myDial.GetPathName();
		fpR=fopen(PlainFile,"r+b");

		CString sEncryptFile=sUserName +".ecc";

		fpW=fopen(sEncryptFile,"w+b");
		if(fpW==NULL) return;

		long NamRead;
		long NamWrite;
		char TempFile[1024];
		while(!feof(fpR))
		{
			//Reading the file
			int iTempLen=1000;
			NamRead=fread(TempFile,sizeof(char),iTempLen,fpR);

			//XOR
			int i;
			int j=0;
			for(i=0;i<NamRead;i++)
				{
					TempFile[i]=TempFile[i]^Random[j];
					j++;
					if(j==40)
					{
						j=0;
					}
				}

			//Write the Encrypted File
			NamWrite=fwrite(TempFile,sizeof(char),NamRead,fpW);
			m_Progress.StepIt();
		}
	}
}
```

5.3 Decryption Part

The decryption part also has three ways to decryption the data, as shown by the flow chart below.

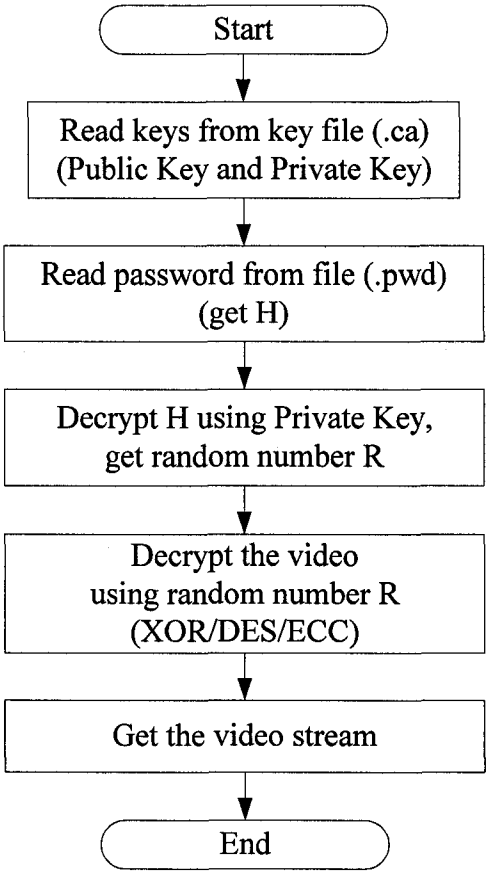


Figure 5.2 Decryption Part Flow Chart

Decrypt data using function void CDecryptDlg::OnDecrypt() (part of the function).

```
void CDecryptDlg::OnDecrypt()
{
	if(myDial.DoModal()==IDOK)
	{
		FILE *fpR;
		FILE *fpW;
		CString CipherFile=myDial.GetPathName();
		fpR=fopen(CipherFile,"r+b");

		CString sDecryptFile=sUserName +".txt";

		fpW=fopen(sDecryptFile,"w+b");
		if(fpW==NULL) return;

		long NamRead;
		long NamWrite;
		char TempFile[1026];
		while(!feof(fpR))
		{
			//Reading the file
			int iTempLen=1024;
			NamRead=fread(TempFile,sizeof(char),iTempLen,fpR);

			int i;
			int j=0;
			char *d, *k;
			k=cRandom;
			d=TempFile;
			for(i=0;i<NamRead;i=i+8)
				{
					d=TempFile+i;
					dedes(d,k);
				}

			//Write the Encrypted File
			NamWrite=fwrite(TempFile,sizeof(char),NamRead,fpW);

			m_Progress.StepIt();
		}
	}
}
```

5.4 Simulation Result

5.4.1 Simulation Platform

Operation system: Window XP

CPU: Intel P4/1.5G, 2.66GHz

RAM: 992MB RAM

5.4.2 Simulation Results and Analysis

As mentioned in Chapter 2, for the encryption/decryption module, the input and output are TS (Transport Stream). But for the simulation, we base on the assumptions above. So we have a time delay for reading files and writing files. Figures 5.3 and 5.5 show how the simulation program counts encryption/decryption time.

❖ **Encryption**

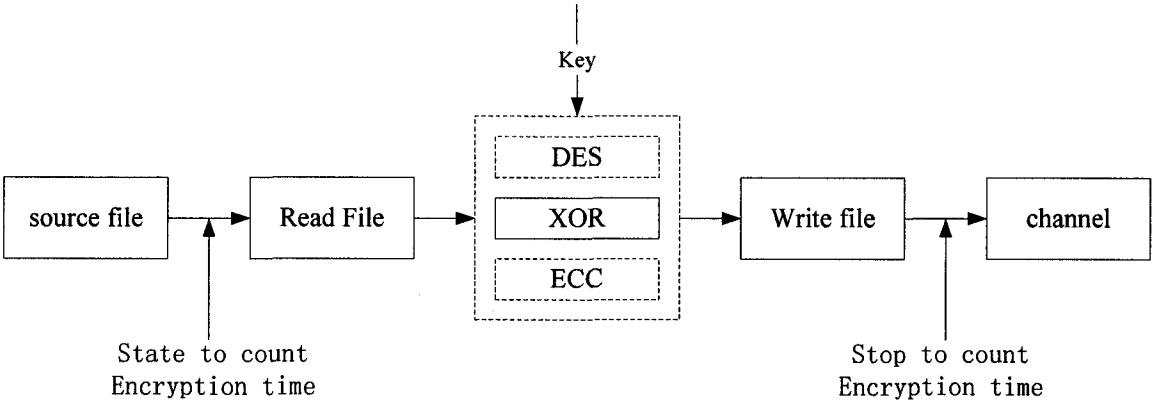


Figure 5.3 How to Count the Encryption Time

Table 5-1 shows the encryption time for various video data using three different algorithms.

Encryption algorithm	File Size 1.06M	File Size 2.05M	File Size 2.95M	File Size 4.07M	File Size 5.05M	File Size 5.98M	File Size 7.11M	File Size 8.17M	File Size 9.12M	File Size 10.05M
XOR Encryption Time (ms)	15.27	26.66	37.41	53.84	65.13	79.52	94.12	109.38	118.97	133.36
DES Encryption Time (ms)	13,224.09	25,493.11	36,591.65	50,327.33	62,104.07	73,964.66	87,889.75	101,113.84	112,431.40	124,291.99
ECC Encryption Time (ms)	33,991.21	65,131.36	94,073.71	129,469.37	161,255.28	190,003.77	225,721.62	259,712.83	290,724.65	319,473.14

Table 5-1. Encryption Time for Different Sizes of Video Files

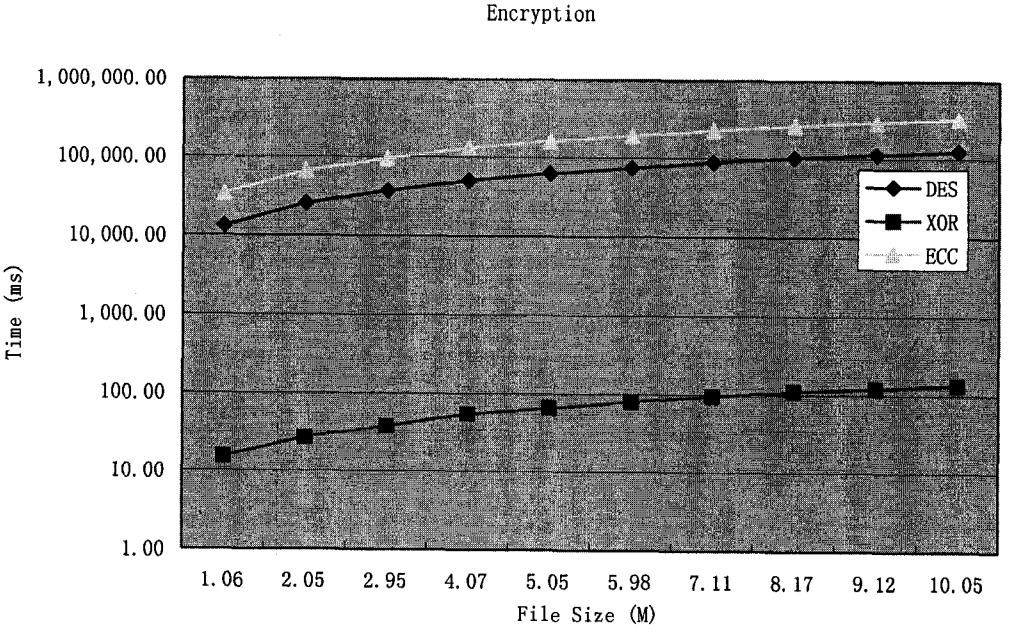


Figure 5.4 Encryption Time Chart

Figure 5.4 shows the encryption time. From this chart, we know that the proposed algorithm XOR needs less time to encrypt data. The DES and ECC take much more time, almost 1,000 times more. All three methods take the linear time, based on the video stream file size.

❖ **Decryption**

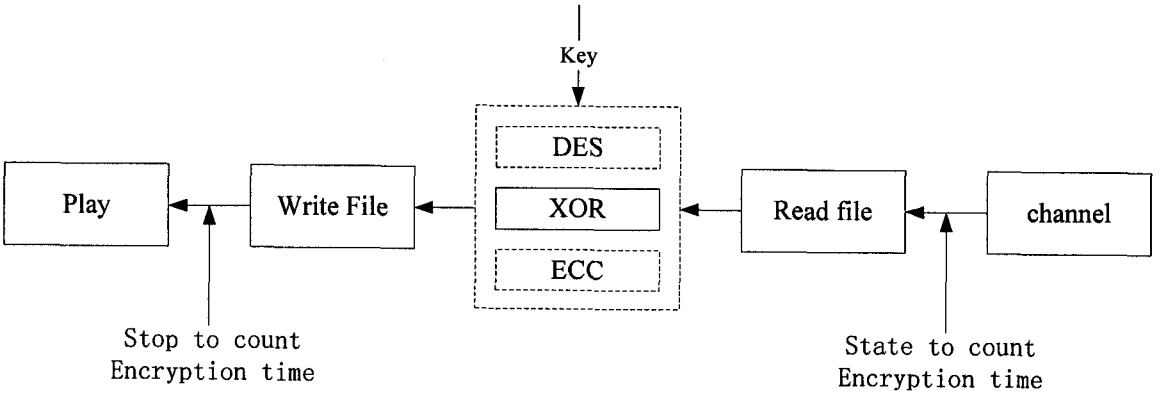


Figure 5.5 How to Count the Decryption Time

Table 5-2 shows the decryption time for various video data using three different algorithms.

Decryption algorithm	File Size 1.06M	File Size 2.05M	File Size 2.95M	File Size 4.07M	File Size 5.05M	File Size 5.98M	File Size 7.11M	File Size 8.17M	File Size 9.12M	File Size 10.05M
XOR Decryption Time (ms)	13.68	26.02	42.10	54.43	66.49	79.05	91.49	105.17	120.92	133.48
DES Decryption Time (ms)	13,464.44	26,058.36	37,422.32	51,459.80	63,425.37	75,934.98	92,216.86	103,681.30	114,885.17	127,394.78
ECC Decryption Time (ms)	16,586.53	30,647.71	46,422.38	63,118.97	77,866.95	92,841.72	110,066.46	126,652.99	140,985.92	155,960.69

Table 5-2. Decryption for Different Sizes of Video Streams

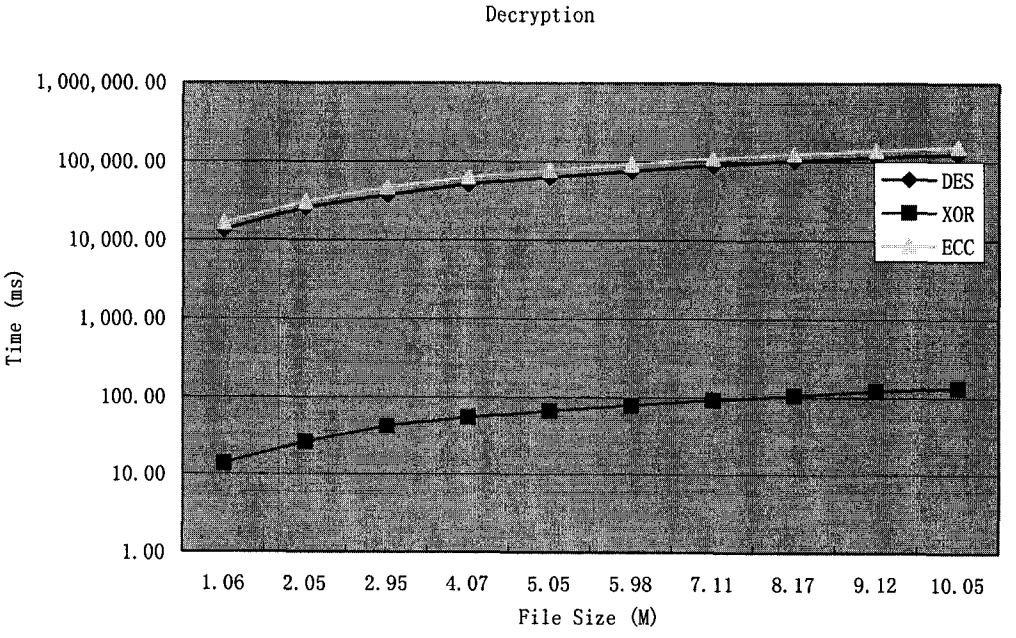


Figure 5.6 Decryption Time

Figure 5.6 shows the decryption time. From this chart we know proposed algorithm XOR needs less time to decrypt data. The DES and ECC take much more time, almost 1000 times more. The decryption time is linear, based on the video size for all three methods.

For digital TV, the transmission speed required for any MPEG 2 broadcast varies according to the nature of the video material. Here we list just some of them:

Type of video service data rate

- Movies (VHS quality) 1.152 Mb/s
- News/entertainment 3.456 Mb/s
- Live sports events 4.608 Mb/s
- 16:9 Wide-screen TV 5.760 Mb/s
- Studio-quality broadcast TV 8.064 Mb/s
- High-definition TV 14.00 Mb/s

Audio or data services data rate

- Monaural sound 0.128 Mb/s
- Stereo sound (L + R) 0.512 Mb/s
- Digital data 9.6 kb/s

Figures 5.7 and 5.8 show the encryption/decryption rate using different algorithms, and also compare them to the standard MPEG 2 transmission speed. From the chart, it is obvious that the proposed algorithm (XOR) has the highest rate, higher then the standard MPEG 2 transmission rate. The algorithms DES and ECC are lower then the standard MPEG 2 transmission rate.

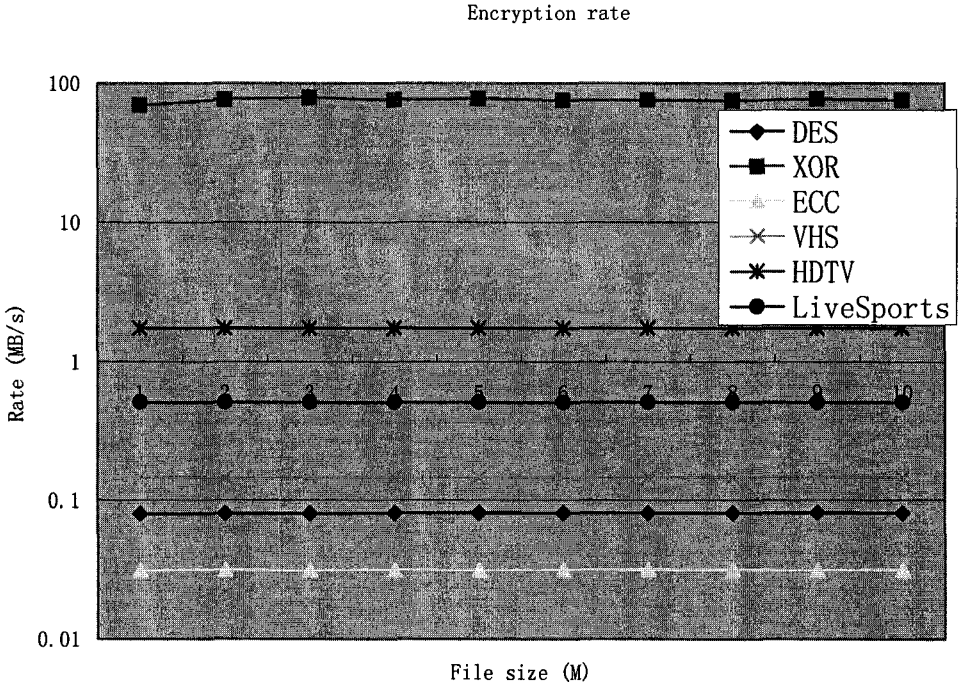


Figure 5.7 Encryption Rate

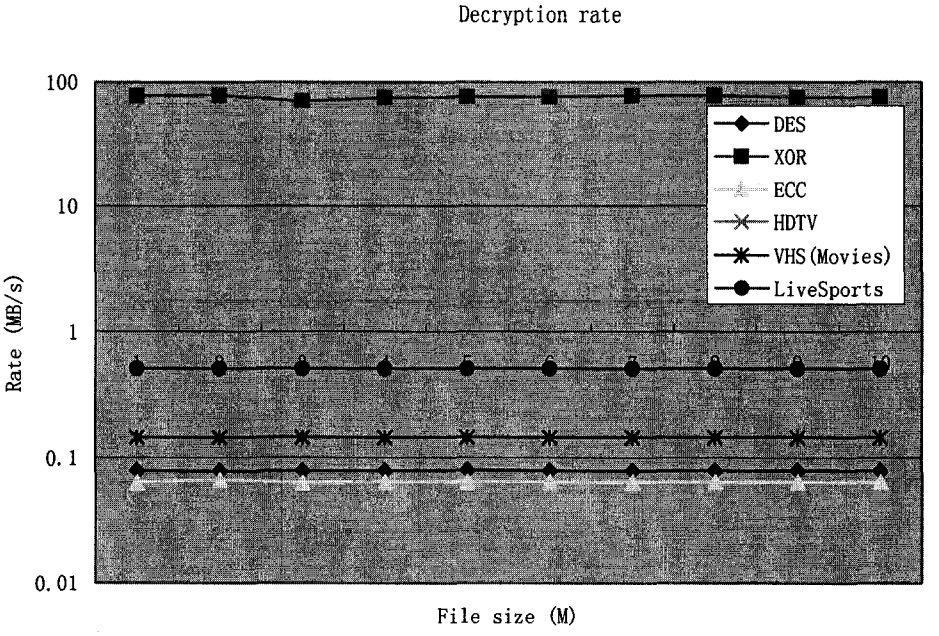


Figure 5.8 Decryption Rate

5.5 JPEG File Display Error Rate

Also for digital satellite broadcast, we need consider system errors. Figure 5.9 explains how to simulate a system noise to a system.

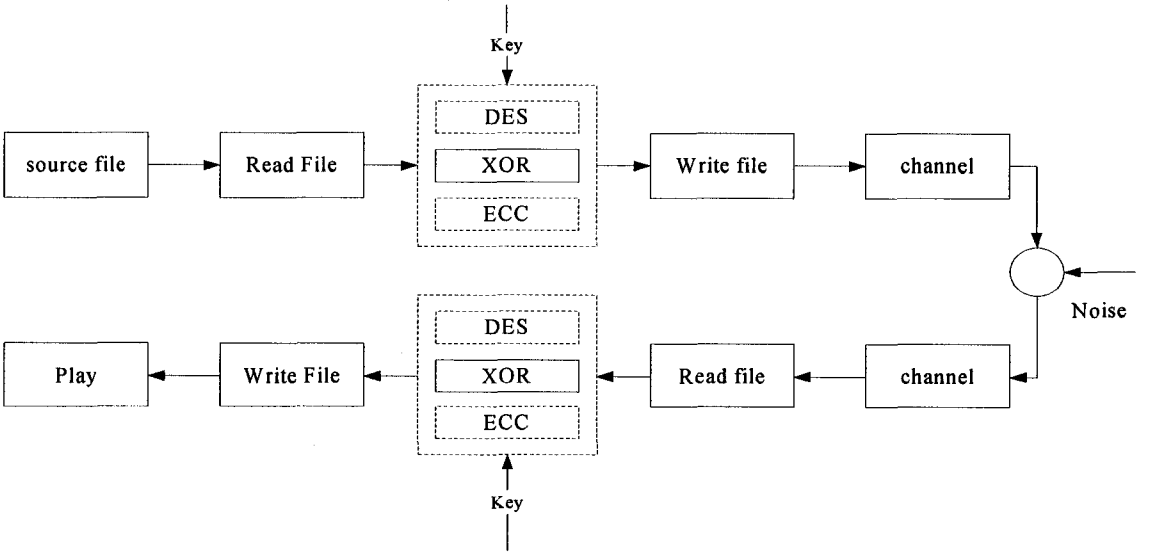


Figure 5.9 System Errors

Proposed algorithm XOR is a kind of data stream algorithm to encrypt/decrypt. When the input data stream has errors, after decryption, the system does not amplify the error. For the algorithm ECC, it is the same idea. However, the algorithm DES is a kind of block algorithm; it does amplify the error. Figure 5.10 displays the error rate. In the simulation program, we use 64 bits as a block.

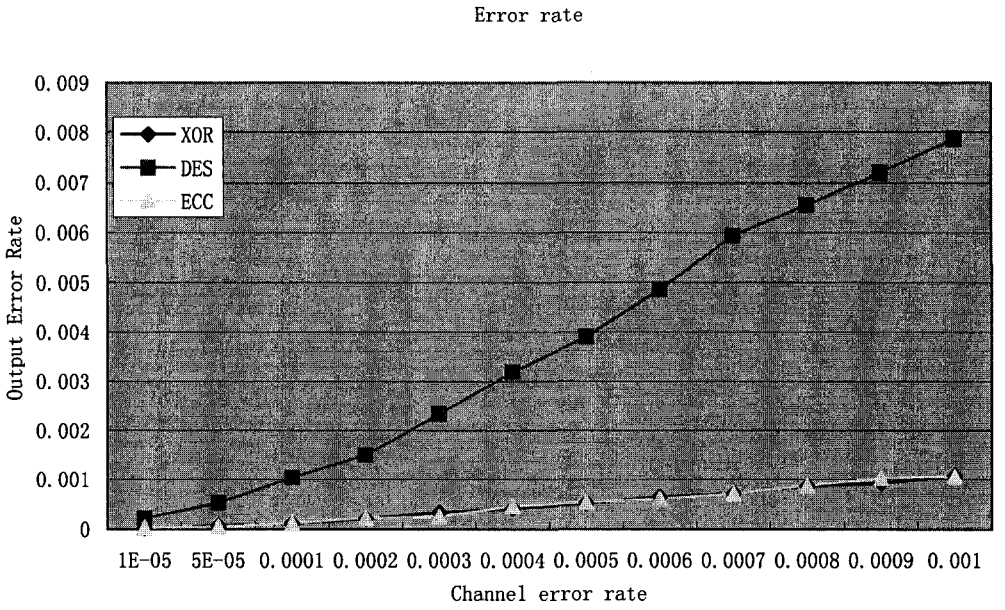


Figure 5.10 Error Rate

Figure 5.11 Normal

Figure 5.12 Error Rate 0.001 (XOR)

Figure5.13 Error Rate 0.001 (DES)

Figure 5.14 Error Rate 0.001 (ECC)

Figures 5.11-5.13 display how the system error affects the image quality. It very obvious that XOR and ECC will not amplify the error, but DES does.

Based on all the simulation results, the two proposed methods XOR and ECC have the good robustness performance (error rate is not increased by algorithms). It implies that they are suitable for digital satellite broadcast applications. The method XOR could be applied in high data rate real-time video applications, although it is a relatively low security method. For video applications with high security needs, ECC is a practical method, although it uses large amounts of computing power. ECC is still possible to implement to reach real-time requirements with a fast signal process such as DSP technology. The algorithm DES does not have good performance in both computing and robustness based on our simulation. In other words, the two new proposed methods (XOR and ECC) could solve the security problems that the digital satellite broadcast applications currently have.

Chapter 6

Conclusion and Future Work

6.1 Conclusions

In this thesis, we investigated various encryption/decryption systems in Pay-TV. Three prevailing systems, Irdeto, Nagravision, and VIAaccess, were discussed and compared. The proposed systems were presented and compared with current methods. Based on the computer simulation, some conclusions are made:

1. The simulation results show that it is possible to encrypt/decrypt broadcast video in real time using public-key techniques.

2. In addition to the ECC encryption algorithm, we proposed to store all the appropriate keys stored in different parts of the STB, and only the smart card associated with the STB will be able to retrieve them. In this case, stealing Pay-TV signals by just copying the content of a SmartCard will not work at all.

3. The main problem with the current Pay-TV encryption systems is that the sender and the receiver share the same key, and the key is delivered though an unsecured channel. Therefore, we proposed to use a public key to avoid this problem. ECC is used to encrypt the key because ECC is more difficult to break.

4. The current Pay-TV encryption systems did not change the key. With the propose system, the random number R is changed very frequently, depending on the video stream.

5. In the proposed system, update Private Key B using the PSTN channel to avoid using an unsecured channel.

6.2 Future Works

Implementation of this algorithm in the embedded system will be considered. The expected result is that this proposed algorithm should be able to handle real-time encryption/decryption of broadcast video signals.

A security management system will be developed to enhance the proposed method so that the solution can be deployed in the real system.

Also, a solution will need to be found to upgrade the current system.

Stream encryption technology is very popular now. There are several methods we could investigate (for instance, XOR256, HC-256, or RC4). Perhaps we can find more effective methods that have high-leave security and that are also fast enough for real-time encryption/decryption of broadcast video signals.

Reference:

1. *Jorge Matos Gómez*, "Satellite Broadcast Systems Engineering," © 2002 Artech House, INC.

2. *Sastri L. Kota, Kaveh Pahlavan, Pentti Leppanen*, "Broadband Satellite Communications for Internet Access," © 2004 by Kluwer Academic Publishers.

3. *Rudolf F. Graf and William Sheets*, "Video Scrambling & Descrambling for Satellite & Cable TV Second Edition," © 1998 by Rudolf F. Graf and William Sheets.

4. *Bruce R. Elbert*, "The satellite communication applications handbook" 2004, © by Boston: Artech House.

5. *Book, Connie Ledoux*, "Digital television: DTV and the consumer," Ames, Iowa : Blackwell, 2004.

6. CableWorld LTD. "Pay-TV encrypting solutions in digital Cable TV headends," CW-4000 Digital TV Handend, 2002. http://www.cableworld.hu/content/Pay-TV-a.pdf, access time: January, 2006

7. *Jorge Matos Gomez*, "Satellite Broadcast Systems Engineering," Chapter1 and Chapter4, ARTECH HOUSE, INC., 2002.

8. *Bruce R.Elbert*, "The Satellite Communications Applications Handbook," Chapter 5 ARTECH HOUSE, INC., 1997

9. Digital Broadcasting Systems for Television, Sound and Data Services; Framing Structure, Channel Coding and Modulation for 11/12 GHz Satellite Services, European Telecommunication Standard ETS 300 421, ETSI Secretariat, Sophia Anatipolis—Valbonne, France: European Telecommunications Standards Institute.

10. *Ronald de Bruin, Jan Smits*. "Digital Video Broadcasting: Technology, Standards, and Regulations," ARTECH HOUSE, INC. 1999.

11. ISO/IEC, "Coding of moving pictures and associated audio—Part 1: Systems," IS 13818-1, 1994

12. Bitcentral—Innovators in digital broadcasting, Glossary—E—ECM, EMM, http://www.bitcentral.com/bcweb/glossary.asp?glossaryletter=e EAR European Academic Research Network. A network using BITNET technology connecting universities and research labs in Europe. Access time: March, 2006

13. *John barkley*, "Cryptography Overview," 1994 Oct. 7. http://csrc.nist.gov/publications/nistpubs/800-7/node207.html#figcryptconcepts. Access time: April, 2006

14. *Brien M. Posey*, MCSE, "Understand The Differences Between Public Key And Symmetric Key Encryption," http://www.brienposey.com/kb/general_security.asp, 2002, Posey Enterprises. Access time: February, 2006

15. *Jerome Burke, John McDonald, Todd Austin*, "Architectural Support for Fast Symmetric-Key Cryptography" Advanced Computer Architecture Laboratory

University of Michigan, available at http://www.ee.princeton.edu/~rblee/ELE572Papers/ArchFastSymmetricKey-austin.pdf. Access time: March, 2006

16. *Michael Rosing*, "Implementing Elliptic Curve Cryptography," 1998, Manning Publications.

17. *J.H. Silverman*, "The Arithmetic of Elliptic Curve" (New York: Springer-Verlag, 1985)

18. Irdeto system http://isat.info/eng/share/index.php?db=share&category=CAS&mode=view&sp=0&id=178 Access time: May, 2006

19. Irdeto system http://gauss.ffii.org/PatentView/EP1111923#head-e46dd58e56820ecb452aec4b9a2914c8f483c2ec Access time: April, 2006

20. Pirate website for keys http://www.satellites.co.uk Access time: May, 2006

21. Pirate decryption http://en.wikipedia.org/wiki/Pirate_decryption Access time: June, 2006

22. *Michael O. Kolawole,* "Satellite Communication Engineering" New York: Marcel Dekker, c2002

23. Viaccess http://www.viaccessfree.org/start_en.html Access time: June, 2006

24. *N.Koblitz*, "Elliptic Curve Cryptosystems," Mathematics of Computations (1987):203-209

25. *V.S.Miller* "Use of Elliptic Curves in Cryptography," in CRYPTO '85 (New York:Springer-Verlag,1986),417-426.

26. *William Stallings*, "Cryptography and Network Security: Principles and Practice," 1998, Prentice Hall.

27. Certicom securing innovation
http://www.certicom.com/resources/ecc_tutorial/ecc_tut_1_0.html
Access time: June 2006

28. *Michael Rosing*, "Implementing Elliptic Curve Cryptography," 1998, Manning Publications.

29. *J.H. Silverman*, "The Arithmetic of Elliptic Curve" (New York: Springer-Verlag, 1985)

30. *Jerry C. Whitaker*, Editor-in-Chief, "The ATSC DTV System"

31. ATSC Standard: "Modulation And Coding Requirements For Digital TV (DTV) Applications Over Satellite," Doc. A/80, Advanced Television Systems Committee, Washington, D.C., July 17, 1999.

32. ATSC Standard: "Direct-to-Home Satellite Broadcast Standard," Doc. A/81, Advanced Television Systems Committee, Washington, D.C., 2003.

33. ATSC Standard: "Conditional Access System for Terrestrial Broadcast, Revision A," Doc. A/70a, Advanced Television Systems Committee, Washington, D.C., July 22, 2004.

34. ATSC Standard: "ATSC Digital Television Standard (A/53) Revision E," Doc. A/53e, Advanced Television Systems Committee, Washington, D.C., December 27, 2005.

35. *Holzner, Steven*, "Advanced Visual C++ 5," New York : M&T Books, c1997.

36. *Eckel, Bruce*, "Thinking in C++," Upper Saddle River, N.J. : Prentice Hall, c2000-