THE DESIGN AND IMPLEMENTATION OF THE CONDITIONAL ACCESS SYSTEM FOR CABLE TV SUBSCRIPTION USING FIXED CONTROL WORD SCRAMBLE

WITCHA BURIRAK

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE (COMPUTER SCIENCE)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
2014

Research Project
entitled

THE DESIGN AND IMPLEMENTATION OF THE CONDITIONAL ACCESS SYSTEM FOR CABLE TV SUBSCRIPTION USING FIXED CONTROL WORD SCRAMBLE

……..……..……
Mr. Witcha Burirak
Candidate

……..……..……
Assoc.Prof. Damras Wongsawang,
Ph.D. (Information Engineering)
Major advisor

……..……..……
Asst.Prof. Chomtip Pornpanomchai,
Ph.D. (Computer Science)
Co-advisor

……..……..……
Prof. Banchong Mahaisavariya,
M.D., Dip Thai Board of Orthopedics
Dean
Faculty of Graduate Studies
Mahidol University

……..……..……
Asst.Prof. Sudsanguan Ngamsuriyaroj,
Ph.D. (Computer Science and Engineering)
Program Director
Master of Science Program in
Computer Science
Faculty of Information and
Communication Technology
Mahidol University

Research Project
entitled

THE DESIGN AND IMPLEMENTATION OF THE CONDITIONAL ACCESS SYSTEM FOR CABLE TV SUBSCRIPTION USING FIXED CONTROL WORD SCRAMBLE

was submitted to the Faculty of Graduate Studies, Mahidol University
for the degree of Master of Science (Computer Science)
on
December 29, 2014

……
Mr. Witcha Burirak
Candidate

……
Mr. Nawat Kamnoonwatana,
Ph.D. (Signal Processing)
Chair

……
Assoc.Prof. Damras Wongsawang,
Ph.D. (Information Engineering)
Member

……
Asst.Prof. Chomtip Pornpanomchai,
Ph.D. (Computer Science)
Member

……
Prof. Banchong Mahaisavariya,
M.D., Dip Thai Board of Orthopedics Dean
Faculty of Graduate Studies
Mahidol University

……
Assoc.Prof. Jarernsri L. Mitrpanont, Ph.D.
(Computer Science)
Dean
Faculty of Information and Communication Technology
Mahidol University

ACKNOWLEDGEMENTS

I would like to express the deepest appreciation to my Professor ASSOC. PROF. DR. Damras Wongsawang for the useful comments, and help through the learning and writing of this research. Moreover I would like to thank Mr. Samathorn Teankingkaeo for introducing me to this topic and support. Also, I like to thank my colleagues, who have shared their knowledge and idea to do experiment on the research.

Witcha Burirak

THE DESIGN AND IMPLEMENTATION OF THE CONDITIONAL ACCESS SYSTEM FOR CABLE TV SUBSCRIPTION USING FIXED CONTROL WORD SCRAMBLE

WITCHA BURIRAK 5338170 ITCS / M

M.Sc. (COMPUTER SCIENCE)

RESEARCH PROJECT ADVISORY COMMITTEE: DAMRAS WONGSAWANG, Ph.D., CHOMTIP PORNPANOMCHAI, Ph.D.

ABSTRACT

This research developed a Digital Video Broadcasting (DVB) Conditional Access system (CAS) that allows using fixed Control Word (CW). Actually, the CW used to scramble the video and audio channel is changed in seconds. The only complied Conditional Access Set-Top-Box (CAS-STB) can be used to watch the channel but the Basic Interoperable Scrambling System Set-Top-Box (CAS-STB) can not. In order to allow both CAS-STB and BISS-STB to be used to watch from the same encrypted channel, the CW within the Entitlement Control Message (ECM) should be modified.

This research project has developed the system called "Conditional Access System Using Fixed Control Word (CASFCW)". In CASFFCW, the signal encryption structure has been changed. We create the conditional access on cable TV signal by using a fixed key encryption system. The CASFCW has been examined and tested in the actual applications for many situations. There are five types of STB selected for the experiment in this research, 1) Set-Top-Box support only BISS brand PSI 2) Set-Top-Box support only Conditional Access System brand SUN Box (ABV-CAS) 3) STB support only Conditional Access System brand HUMAX (Irdeto-CAS) 4) STB support only Conditional Access System brand GMMz (Novel-CAS) and 5) Set-Top-Box support only BISS brand D-Khoom. The experimental results show that, the BISS-STB cannot be used to watch any channels that are encrypted by using any CAS. A channel is encrypted by ABV-CAS and allows only their STB to be used to watch the channel. The STB that support both BISS and Irdeto-CAS or Novel-CAS are not able to be used to watch the encrypted channel by ABV-CAS. Finally, for the channel encrypted by using CASFCW, both types of CAS-STB and BISS-STB allow people to watch the channel.

KEY WORDS: DIGITAL VIDEO ENCRYPTION/ CONDITIONAL ACCESS SYSTEM/ / FIXED CONTROL WORD SCRAMBLE/ DIGITAL VIDEO BROADCASTING

61 pages

การออกแบบและการทำให้เกิดผลของระบบการเข้าถึงแบบมีเงื่อนไขสำหรับโทรทัศน์แบบบอกรับเป็นสมาชิกโดยใช้การเข้ารหัสด้วยคำควบคุมแบบคงที่

THE DESIGN AND IMPLEMENTATION OF THE CONDITIONAL ACCESS SYSTEM FOR CABLE TV SUBSCRIPTION USING FIXED CONTROL WORD SCRAMBLE

วิชชา บุรีรักษ์ 5338170 ITCS/M

วท.ม. (วิทยาการคอมพิวเตอร์)

คณะกรรมการที่ปรึกษาโครงการวิจัย : ดำรัส วงศ์สว่าง, Ph.D. ชมทิพ พรพนมชัย, Ph.D.

บทคัดย่อ

วัตถุประสงค์ของงานวิจัยนี้เพื่อพัฒนาและออกแบบระบบการเข้าถึงแบบมีเงื่อนไข สำหรับโทรทัศน์แบบบอกรับเป็นสมาชิกโดยใช้การเข้ารหัสด้วยคำควบคุมแบบคงที่ ซึ่งอุปกรณ์รับสัญญานดาวเทียมที่รองรับการใช้งานระบบเข้ารหัสสัญญานแบบบอกรับเป็นสมาชิกด้วยคำควบคุมแบบไม่คงที่เท่านั้น ที่สามารถถอดรหัสและรับสัญญาณช่องรายการที่เข้ารหัสด้วยคำควบคุมแบบไม่คงที่ได้ แต่อุปกรณ์รับสัญญานดาวเทียมที่รองรับการใช้งานระบบเข้ารหัสสัญญานด้วยคำควบคุมแบบคงที่จะไม่สามารถถอดรหัสได้ เพื่อให้อุปกรณ์รับสัญญานดาวเทียมที่รอรับการใช้งานทั้งระบบเข้ารหัสด้วยคำควบคุมแบบไม่คงที่และคงที่ให้สามารถรับชมช่องรายการเดียวกันและเวลาเดียวกันได้นั้น การเข้ารหัสสัญญานวิดีโอและออดิโอแบบบอกรับเป็นสมาชิกควรใช้คำควบคุมแบบคงที่

งานวิจัยนี้ได้ทำการทดลองกับการเข้ารหัสสัญญาณทั้งแบบคงที่และไม่คงที่จำนวน 5 ช่องทีวี โดยใช้อุปกรณ์รับสัญญานดาวเทียมจำนวน 5 ชนิดคือ1) อุปกรณ์รับสัญญานดาวเทียมที่รองรับการเข้ารหัสคำควบคุมแบบคงที่ยี่ห้อพีเอสไอ และ ดีคุ้ม, 2) อุปกรณ์รับสัญญานดาวเทียมที่รองรับการเข้ารหัสคำควบคุมแบบไม่คงที่ยี่ห้อซันบล๊อก, ฮิวแม็ก และจีเอ็มเอ็ม หลังจากที่มีการทดสอบกับอุปกรณ์รับสัญญานดาวเทียมที่รองรับการเข้ารหัสด้วยคำควบคุมแบบคงที่จะไม่สามารถรับชมช่องการที่เข้ารหัสแบบบอกรับเป็นสมาชิกที่ใช้คำควบคุมที่ไม่คงที่ได้ และอุปกรณ์รับสัญญานดาวเทียมที่รองรับการเข้ารหัสบอกรับเป็นสมาชิกด้วยคำควบคุมแบบไม่คงที่นั้น จะไม่สามารถรับชมช่องการที่เข้ารหัสแบบคำควบคุมแบบคงที่ได้ ส่วนช่องรายการที่เข้ารหัสแบบบอกรับเป็นสมาชิกที่ใช้คำควมคุมแบบคงที่นั้น อุปกรณ์รับสัญญานดาวเทียมทั้งสองชนิดสามารถถอดรหัสและรับชมได้

61 หน้า

CONTENTS

CONTENTS (cont.)

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES (cont.)

LIST OF TERMS AND DEFINITIONS

AES	Advanced Encryption Standard
Access Criteria	(AC) CA system specific information needed by the ECMG to build an ECM
Array	An enumerated collection of identical entities (e.g., an array of bytes).
Bit	A binary digit having a value of 0 or 1.
BISS	Basic interoperable Scrambling System**,** the use of clear session word to scramble.
Block	The Sequence of binary bits and it is comprised of input, output, State, and Round Key.
Cipher	Series of transformations that converts plaintext to cipher text using the Cipher key.
Cipher text	Data output from the Cipher or input to the Inverse Cipher.
Inverse Cipher	Series of transformations that converts cipher text to plaintext using the Cipher key.
Plaintext	Data input to the Cipher or output from the Inverse Cipher.
Word	A group of 32 bits that is treated either as a single entity or as an array of4bytes
Crypto Period (CP)	Period when a particular Control Word is being used by the scrambler.ECM
Control Word (CW)	Data object used for scrambling.

LIST OF TERMS AND DEFINITIONS (cont.)

Broadcaster (Service provider)	An organization which assembles a sequence of events or services to be delivered to the viewer based upon a schedule.
CA_subsystem_ID	The CA_subsystem_ID is defined in this document to handle multiple connections to ECMGs with the same CA_system_ID value. The combination of CA_system_ID and CA_subsystem_ID is called Super_CAS_ID.
CA components	Those components brought by a CA provider for integration into a host head-end system.
Conditional Access (CA) system	A system to control subscriber access to broadcast services and events e.g. Videoguard, Eurocrypt.
Control Word Generator (CWG)	This component receives a CW request from the SCS and returns a CW.
Entitlement Control Message (ECM)	Private Conditional Access information which carries the control word in a secure manner and private entitlement information.
Entitlement Control Message Generator (ECMG)	This generator produces the ECM messages but does not support ECM repetition.

LIST OF TERMS AND DEFINITIONS (cont.)

Entitlement Management Message (EMM)	Private Conditional Access information which, for example, specifies the authorisation levels of subscribers or groups of subscribers for services or events.
Entitlement Management Message Generator (EMMG)	This generator produces the EMM messages and repeatedly plays them out at the appropriate times.
Generator	An component producing data.
Host head-end	A system which is composed of those components required before a CA provider can be introduced into the headend.
Multiplex (MUX)	A stream of all the digital data within a single physical channel carrying one or more services or events.
Proprietary	This term details the fact that the interface will be specified by the head-end provider, or by the CA provider. The interface can be commercially open but is not open within this specification. Its availability will be via commercial/technical agreement.
Packet Elementary Stream (PES)	The packet carry the elementary stream from video and audio encoder.
Service	A sequence of events under the control of a broadcaster which can be broadcast as part of a schedule.

LIST OF TERMS AND DEFINITIONS (cont.)

Service Information (SI)	Information that is transmitted in the transport stream to aid navigation and event selection.
Simulcrypt Synchroniser (SCS)	The logical component that acquires Control Words, ECMs and synchronises their playout for all the Conditional Access Systems connected.
Stream	An independent bi-directional data flow across a channel. Multiple streams may flow on a single channel. Stream_IDs (e.g. ECM_stream_ID, Data_stream_ID, ...) are used to tag messages belonging to a particular stream.
Transport Stream	A Transport Stream is a data structure. It is the basis of the ETSI Digital Video Broadcasting (DVB) standards.

CHAPTER I
INTRODUCTION

1.1 Digital TV encryption

The purpose of Digital Video Broadcasting (DVB) is to design global standards for the global delivery of digital television and data services to the home, The broadcasting may include High-definition Television (HDTV), multiple channel Standard-definition (SDTV) or new broadband multimedia contents and interactive services. At present, compression technology has been developed. One Satellite Transponder (36MHz) can contain more than 20 TV channels and these channels can be free-to-air or encrypted channels combining together in one Transponder. The Free-to-air channels can be done without security key. However, the encrypted channels have to be communicated with external parties in order to scramble their signals with a control word or encryption key in order to provide conditional access only for subscribers.

There are two systems of protection method that we introduce in this project, Conditional Access System (CAS) and Basic Interoperable Scrambling System (BISS). CAS is an application on Digital TV that can protect the content from piracy. The important function of CAS is to protect secret key or Control Word (CW). The secret key is always changed frequently in seconds. The CAS allows customer who has paid for fee subscription can access to the content. Another system is called “BISS”. It is used to protect the transmission to feed the content from one point to another. The secret key of BISS is fixed. However, BISS is popularly used for basic scramble of video and audio broadcasting via satellite in Thailand. They are using the fixed key to protect the Free-view channels but the security of BISS is less than CAS.

Condition Access System

There are two main functions of conditional access system (CAS). First, the CAS has to allow only subscribed user to view the encrypted contents. The system has to also prevent the unauthorized user to access the protected contents. The keys or control words (CWs) are used to protect the content and it is encrypted as called Entitlement Control Message (ECM).

These same values of CWs are used to scramble the content. At the end user, they have to use the complied Set-Top-Box (STB) of CAS model. The only subscribed user can get the CWs from ECM and use it for descrambling the scrambled contents and decoding the pictures.

Basic Interoperable Scrambling System (BISS)

Normally, we use BISS in Digital satellite news gathering (DSNG) to protect our content and send to center for broadcasting to end users. The BISS is based on Digital Video Broadcasting – Common Scrambling Algorithm (DVB-CSA) specification standard and used of clear fixed key, it's called "session word". The BISS model is required to direct enter the session word or CW to transmitter and STB in order to protect the transmission from piracy. The CW that entered at transmitter must be the same value as STB.

There are three modes of operation,

1) Mode 0 is no scrambling
2) Mode 1 is used clear CW for scrambling signal
3) Mode E is used encrypted CW for scrambling signal.

The BISS system is designed and implemented based on BISS Mode1 also, most of the STB in Thailand use them as function for basic descramble.

Motivation

Now, there are two encryption types in the STB which exist in the field and market.

1) BISS uses basic scrambling in the satellite STB in Thailand. There are many models of BISS-STB available in the market and it is cheaper than Conditional Access-Set-Top-Box (CAS-STB).

2) The price of CAS-STB may be higher than basic BISS-STB but it is embedded the CA software that can decrypt the condition access message. The STB is more secured and they are able to support the cycling CW.

It would be better if one channel can be descramble by using both BISS-STB and CA STB. The content can be delivered to customer easily without uplink two channels for BISS-STB and CAS-STB. The content provider can do CA during the period of time and activate the BISS key when the program is required less of security.

Problem Statement

Bit-rate in the satellite Transponder is limited. There is about 40 Mbit/sec in one Transponder and costly. In DVB-CSA standard, there is no mention about fixed CW in the process. There is no scrambler in the market having function of BISS and CA setting in the same TV channel or service. We categorize the problems into two cases.

1) Many channels are required to encrypt with BISS but some brands of STB support only CAS-STB. We can save the cost and equipment if we can do the BISS and CAS in the same channel, otherwise the duplicated content have to uplink.

2) Some period of time, channels have to be encrypted by BISS in order to allow all STBs in the field can receive a special program, for example World Cup, football EURO and etc. However, normally the same channels are encrypted by CAS because the content is allowed only subscribers who paid for the content.

Objectives

According to the problem statement, this project is focused on the following objectives.

1) To study the process of DVB-CSA and BISS, which part of the process can do together in order to allow the BISS and CAS to work together in the same time and same TV channel.

2) To design the system which allows the BISS and the CAS to work together in the same TV channel.

3) To analyze and evaluate the system of BISS and CAS working together and finding the impact when implementing the system in actual applications.

Scope of the project

This project is focused on designing, implementing and experiments the system of BISS and CAS working together in same TVchannel.

1) Designing the system

The system need to be designed complying to the DVB-CAS specification standard, otherwise the system may get unexpected problem due to the CAS is designed on proprietary for each CAS vendor.

2) Implementation

- The system is implemented with one CAS only even though implementing of multi-CASs is the same concept. The details of CAS system cannot be declared in this document due to the CAS security is not allowed to publish.
- BISS mode 1 is focused on designing, implementing and experiments even though implementing of BISS mode-E is the same concept.

3) Experiment and results

- The experiment is conducted in the Lab. Some details of the results cannot be published due to the security of reason.
- There are five channels of video and audio in the experiments.

1.2 Research Project Organization

The research document consists of sixth chapters including the following chapters.

Chapter I: Introduction

This chapter introduces Digital TV and video encryption, motivation, problem statement, objectives and scope of the project.

Chapter II: Literature Review and Related Work

This chapter describes about the DVB standards and techniques which are used in the research.

Chapter III: Methodology and System Design

This chapter describes the concepts and approaches of that using in the research and also presents about system design.

Chapter IV: Implementation

This chapter presents how to implement our research according to our system design.

Chapter V: Experimental Results

This chapter describes about the results of experiments. The system will be tested under various situations. The results of the experiments will be recorded, analyzed and evaluated.

Chapter VI: Conclusions and Suggestions

This chapter presents the conclusion of the research, and also some further development to improve the system is suggested.

CHAPTER II
LITERATURE REVIEW AND RELATED WORK

This chapter describes an overview of conditional access system and current researches related to TV scrambling standard. In section 2.1, we explain the problem found with incompatible STB. In section 2.2, we explain about the related theories used in our research. Finally in section 2.3, we present the related works and commercial products currently available in market.

2.1 Problems Found with incompatible Set-Top-Box

The main problem found is inability to descrambling TV channels when using incompatible Set-Top-Box (STB). Actually, receiving the encrypted TV channel involves both parties' head-end and receiving side. The STB software has to be able to support encryption methods on the Head-end. A TVchannel on the Head-end can be encrypted either by Conditional Access System (CAS) or Basic Interoperable Scrambling System (BISS). There are a lot of STBs supporting CAS only and some other STBs supporting BISS only. In this research, we propose to use fixed key to encrypt the TV channel in order to allow both BISS-STB and CAS-STB to decrypt the TV channels as show in figure 2.1.

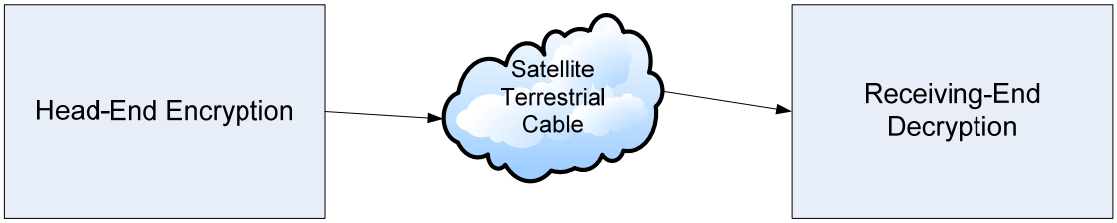

Figure 2.1 VDO broadcasting system

2.2 Related Theories

This section reviews the related theories and basic knowledge in the Digital Video Broadcast (DVB), Head-end implementation of DVB in Common Scrambling Algorithm. These theories supports for scrambling and conditional Access (CA) within digital broadcasting system. Moreover, we also discuss about available products related to our research.

2.2.1 Head-End Implementation of Simulcrypt

This section is to introduce of encryption for digital television signals used DVB in CSA standard. The DVB-CSA is an ETSI (European Telecommunications and Standards Institute) specified the algorithm of security the MPEG2 transport streams signal. In the standard of DVB-CSA, A TV channel can be encrypted by many CAS vendors using the common CW as show in Figure 2.2. The CAS is separated from the head-end component and there are different functions. The free-to-air channels is not required the CAS to integrate in the head-end system.

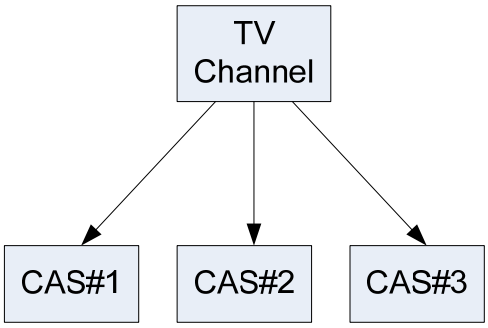

Figure 2.2 Basic simulcrypt concepts

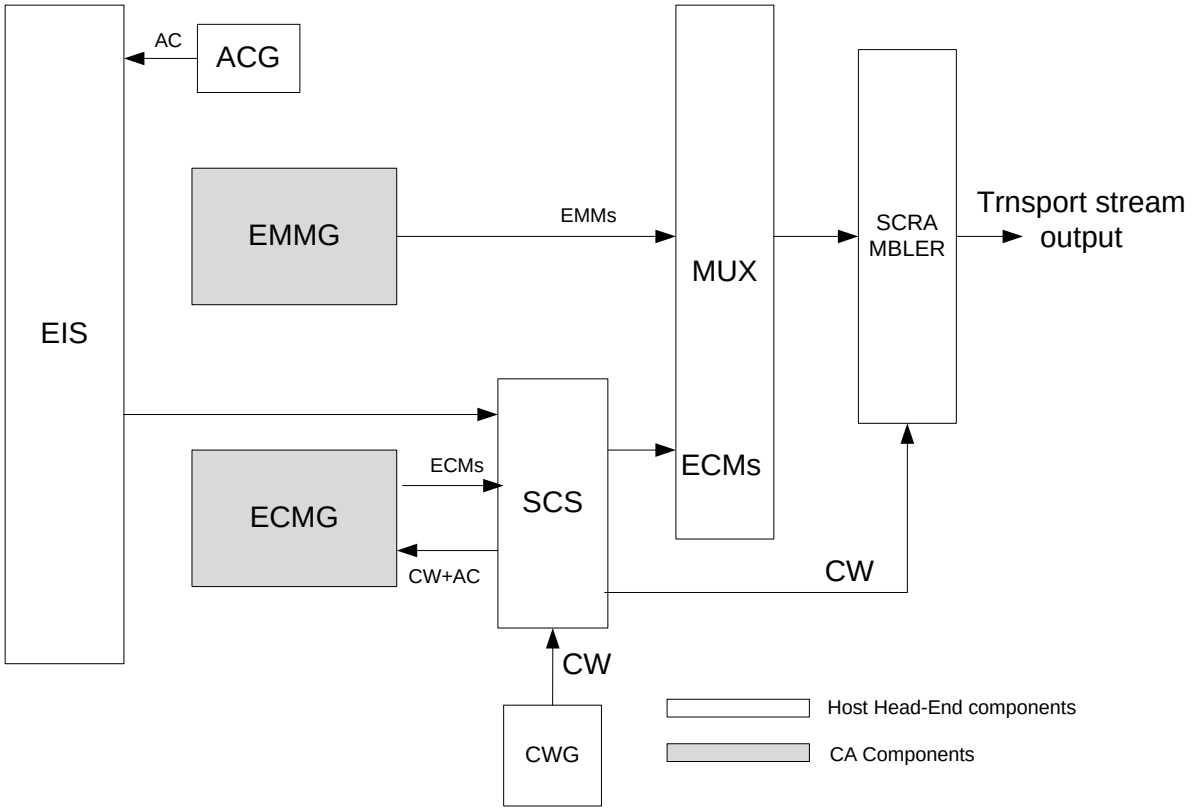

Figure 2.3 Head-End component of Simulcrypt

In the Figure 2.3, there are two areas divided in different function on Head-End Component of Simulcrypt system.

1) Conditional Access (CA) Components.
2) Host head-end components.

In the CA components, there are two components related in the system, Entitlement Control Message Generator (ECMG) and Entitlement Management Massage Generator (EMMG). These two massages are proprietary information of each Conditional Access System (CAS).

The host head-end components are required to be ready in the system before Simulcrypt CA components are introduced. Normally, all Host Head-end components are combined in the same unit equipment. The Simulcrypt CA component is apart from Host Head-end components. This proprietary equipment is provided by CAS vendor.

The description of each Component

1) Event Information Scheduler (EIS)

EIS is responsible for managing all schedule information, all the configuration and CA information. The ECMG need this component to get any needed information in order to generate the correct ECM. The Entitle Control Message Generator (ECMG) will receive the CWs and access criteria from Simulcrypt Synchronizer (SCS), the ECM will be generated or error message to let SCS know what is happening in connection.

2) Simulcrypt Synchronizer (SCS)

The main function of Simulcrypt Synchronizer is to establish TCP connection with ECMGs and create one channel per connection. The streams are created within channel and generate the ECM stream id values in order to get the control words from the CWG. The CWs are submitted to ECMGs on the related streams with the CA specific information, the ECMs is replied by ECMGs and send them back to SCS. The ECMs are synchronized with their Crypto periods and channel parameter in order to send ECMs back to multiplexer (MUX). The function of MUX is to request the repetition time values from ECMG for repeating the ECM according the repetition time periods. Finally, the CW is submitted to the scrambler to be used for specified Crypto period.

3) EMM Generator (EMMG)

The message will be encrypted and send to MUX directly by using either TCP or UDP connection. This message contains authorization information of each STB, private information and text message and etc. In additional, some CAS vendors use this massage for sending their encrypted keys to STBs.

4) ECMG and SCS interface

There are two messages of communication between ECMG and SCS.

(1) Channel messages

a. Channel setup

The TCP connection is established and channel setup message sent to setup the channel. The Super CAS id parameter within the message is to identify the ECMG to which CA system.

b. Channel test

The channel test message is sent by either ECMG or SCS to check whether the TCP connection is still alive and channel is in the error.

c. Channel status

It can be message response to a channel setup or channel test

d. Channel close

This message is sent by SCS to identify the channel is going to be closed.

e. Channel error

This message is shown that there is a recoverable channel level error happened.

(2) Stream messages

a. Stream setup

The SCS is sending the stream setup message to setup a stream when the channel is created.

b. Stream test

The stream test is used for requesting a stream status message to give the ECM channel id and ECM stream id.

c. Stream status

It can be replay to the stream setup message or the stream test message.

d. Stream close request

The SCS will be sent the ECM Stream id within the Stream close request message to identify which of stream in the channel need to be closed.

e. Stream close response

The ECMG will send the ECM stream id within the stream close response message to show which of the stream need to be closed.

f. Stream error

The stream error message can be sent by ECMG or SCS at any time to show that an unrecoverable stream level error happened.

g. CW provision

The CW provision message is sent by SCS to ECMG for requesting an ECM. The control words are also carried within this message.

h. ECM response

The ECM datagram will be computed and replied to the CW provision message.

In this interface, the ECMG is configured as server and the SCS is the client. The mapping between Super CAS ids and IP address as well as port numbers of ECMGs are basic information build in the SCS. The SCS will open a new stream with the appropriate ECMG when EIS requests a new ECM stream for a given Super CAS id value. The new ECM id will be defined by head-end when a new stream is created into a transport stream.

5) Entitlement management massage generator (EMMG) and Multiplexer (MUX)

The Channel setup message is sent to MUX by EMMG to open the channel. EMMG will close the TCP connection when the channel could not be opened by the MUX.

The EMMG sends a stream setup message to the MUX for establishing the stream, once the channel and stream have been correctly created, EMM will be transferred as TS packets. The EMMG and the MUX are talking to allocate the EMM bandwidth and also, the EMMG will talk to request the optimal bandwidth for the stream.

6) Scrambling control field

There are two types of packet headers in the MPEG-2 system specification, TS packet header and packet elementary stream (PES) packet header. The table of scrambling control field in the TS packet header is shown in Table 2.1.

Table 2.1 Transport scrambling control values

Bit values	Description
00	No scrambling of TS packet payload (MPEG-2 compliant)
01	Reserved for future in DVB use
10	TS packet scrambled with Even key
11	TS packet scrambled with Odd key

The first scrambling control bit implies whether the packet payload is scrambled or not and the second bit imply to use Even key or Odd key in scrambling. The bit value "01" will not be occurred in this case because it is reserved for future in DVB use. The TS packet payload may not be scrambled at the TS, but scrambling data might be defined at PES. The PES scrambling control is similar to Transport scrambling control as Table 2.2.

Table 2.2 PES scrambling control values

Bit values	Description
00	No scrambling of PES packet payload (MPEG-2 compliant)
01	Reserved for future in DVB use
10	PES packet scrambled with Even key
11	PES packet scrambled with Odd key

2.2.2 DVB scrambling Algorithm

The CSA version 1&2 was designed and approved by the Steering Board of the DVB Project in May 1994 to minimize the likelihood of piracy attack in payload of a Transport Stream (TS) packet. They use a 64 bit key (control word) to scramble data block size of 8 bytes.

DVB scrambling Algorithm version3

It is designed of reducing the likelihood of piracy attack. They are using a 128-bit key (control word) to encrypt the data blocks of size over 16 bytes. A descrambler is required in the order of 100k gates in hardware. Its algorithm is used on

two block ciphers which is a variation of the “Advanced Encryption Standard”, AES128.

The DVB common scrambling algorithm is introduced as a cascade of two different a block cipher and a stream cipher. The ciphers uses the same 64-bit key K, they are called the common key. In the encryption process a m-byte packet is first separated into blocks (DBi) of 8 bytes each. Probably, the length of the packet is not a multiple of 8 bytes. The sequences of 8-byte blocks are encrypted in reverse order with the cipher-block chaining (CBC) mode of operation as show in Figure 2.4. The initialization vector (IV) is always set to zero. The last output of chain (IB0) is set as a nonce for the stream cipher. The first m of 8 bytes for key-stream generated by the stream cipher are operated in XOR to the encrypted blocks (IBi) i≥1 followed by the residue to generate the scrambled blocks SBi. The descrambling process shows in Figure 2.5 and uses the same methods as scrambling process.

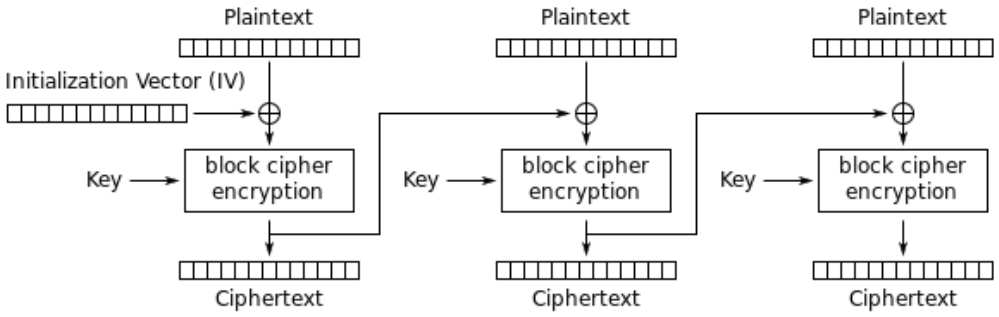

Figure 2.4 Cipher-block chaining CBC
(Source: http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation)

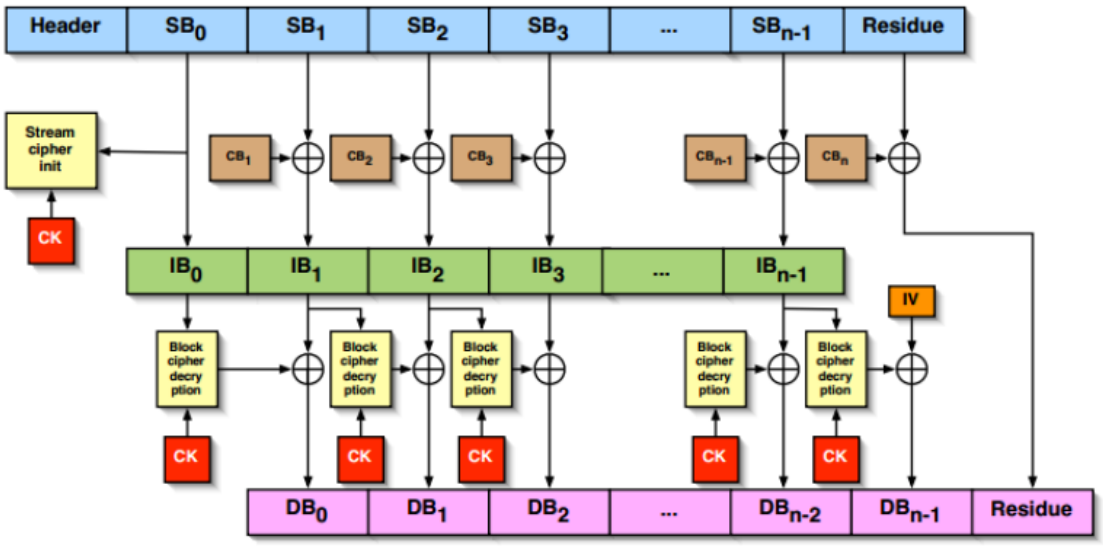

Figure 2.5 The descrambling process of Common Scrambling Algorithms
(Source: Broadcast Encryption, Joseph Tsun Kiet Man)

2.2.3 Basic Interoperable Scrambling System (BISS)

Digital Satellite News Gathering (DSNG) is often used in satellite transmission. It is used for sending the breaking news or special event news from remote location back to center studio for broadcasting. Normally, the content is really confidential and they do not want the other to know the content before broadcasting time, therefore the content need to be protected by scrambling the digital content with the fixed session word (SW) before sending out the content.

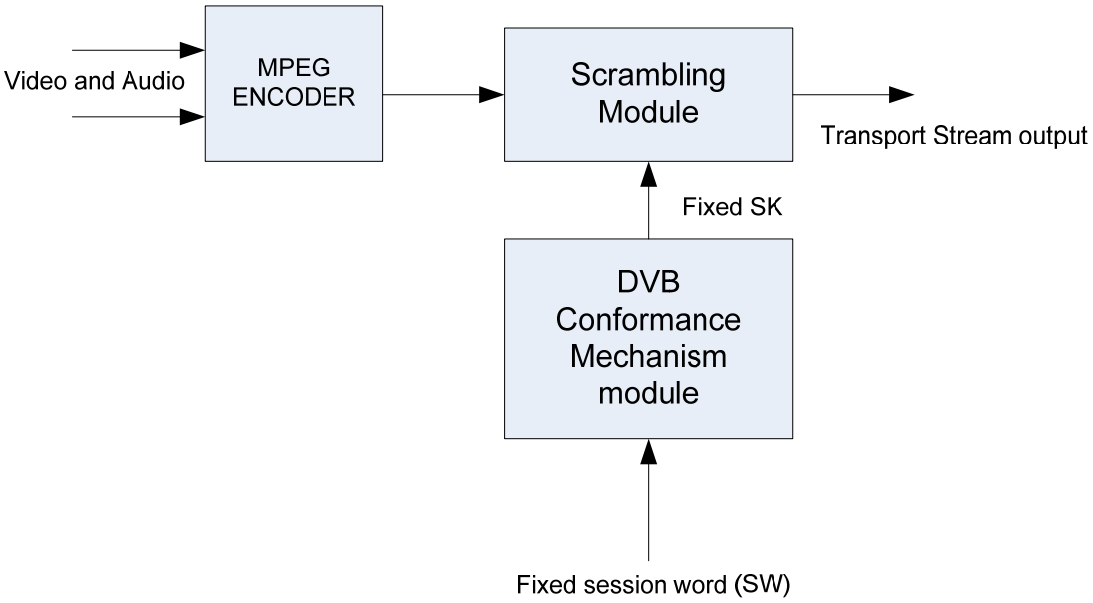

Figure 2.6 Basic Interoperable Scrambling System (BISS)

Basic requirement

The system at the head-end is required entering the same fixed session word into transmitter and receiver directly in order to protect the transmission, only people who know the session word (key) will be able to receive the transmission.

Mode of Operation

There are four modes of operations in BISS.

Mode 0: No scrambling

Mode 1: All components are scrambled by a fixed Control Word.

Mode 2: The single CW sequence is used to scramble for all components.

Mode 3: Each component might be scrambled by a different CW sequence.

Mode 0

This mode can be done by scrambler; the Transport Scrambling Control in the Transport Packets shall be set to “00”.

Mode 1

The session word (SW) needs to be entered to scrambler directly, and it will be transformed into session keys (SK) within the scrambler module. The session word and session key are the same meaning with control word that is specified in the DVB common scrambling specification standard. The SW 96-bit word will be transformed into SK 128 –bit, the mapping of SW 96-bit and SK 128 –bit is given in Table 2.3.

Table 2.3 Mapping of SW 96-bit and SK 128 –bit

96 –bit CW	128 bit CW
SW(1)	SK(1)
SW(2)	SK(2)
SW(3)	SK(3)
SW(4)	SK (4)
SW(5)	SK (5)
SW(6)	SK (6)
N/A	First digit of note a
N/A	Second digit of note a
SW(7)	SK (9)
SW(8)	SK (10)
SW(9)	SK (11)
SW(10)	SK (12)
SW(11)	SK (13)
SW(12)	SK (14)
N/A	First digit of note b
N/A	Second digit of note b

a. SW(1), SW(2) + SW(3), SW(4)+ SW(5), SW(6)

b. SW(7), SW(8) + SW(9), SW(10)+ SW(11), SW(12)

BISS Mode 2 and 3

The variable CW is used in this mode and must be generated in advance and stored locally in the scrambler. The next CW will be fixed from the sequence CWs

in the scrambling Module. The scrambler will use Crypto-Period to set the duration of current CW or next CW. The CWs are encrypted and transmitted within the ECM stream. Figure 2.7 shows overview of BISS mode 2 and 3.

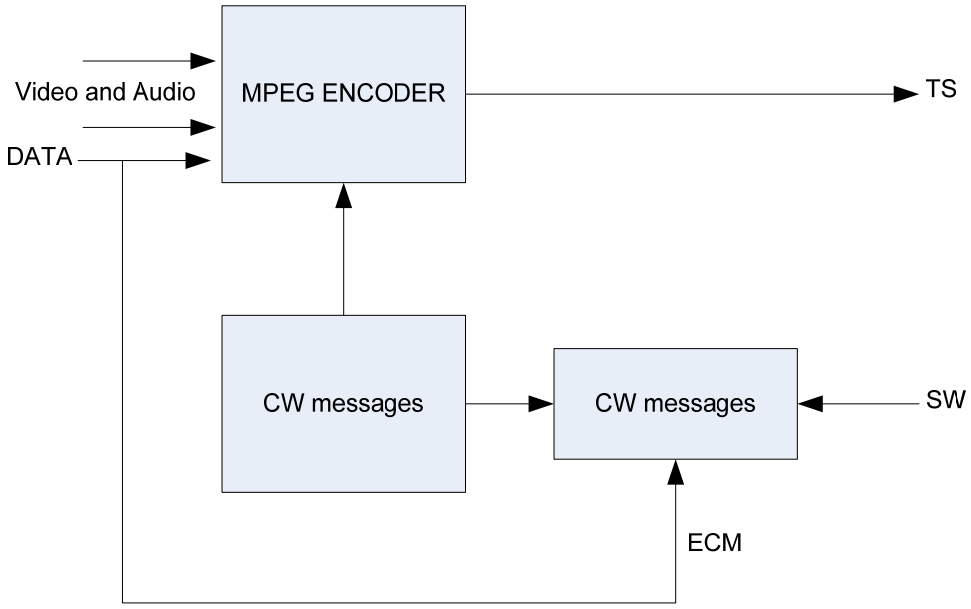

Figure 2.7 Overview of BISS mode 2 and 3

The CWs are encrypted by using DES in ABC EDE 3DES mode, and CA descriptor will be in the program map table (PMT) as programme level that used for identifying the ECM stream for the CW sequence. In the Mode3, CA descriptor will be in the PMT under each component for identifying the ECM stream for the CW sequence of that component.

The transport scrambling control bits of transport stream packet should be set to “11” or “10”, it depend on which key is being used (even or odd).

Entitlement Control Message

In this Mode, there will be CA descriptor presenting in the PMT, and also ECMs are generated and they are encrypted by using 3DES.

2.3 Related works and products

At the present, we cannot find any research to implement the BISS and CAS in the same TV channel. In the other word, the solution may be done at the STBs. The STBs have to be developed to support both BISS and CAS functions. Currently, there are a lot of models and brands of STBs in the field, but all of them could not be upgraded to support both BISS and CAS.

2.3.1 Common interface

The solution is based on interface between a module and a host. Each module defines proprietary functions of each CAS specification. This solution is to allow user to use module either CAS or BISS solutions depending on type of encryption on a TV channel.

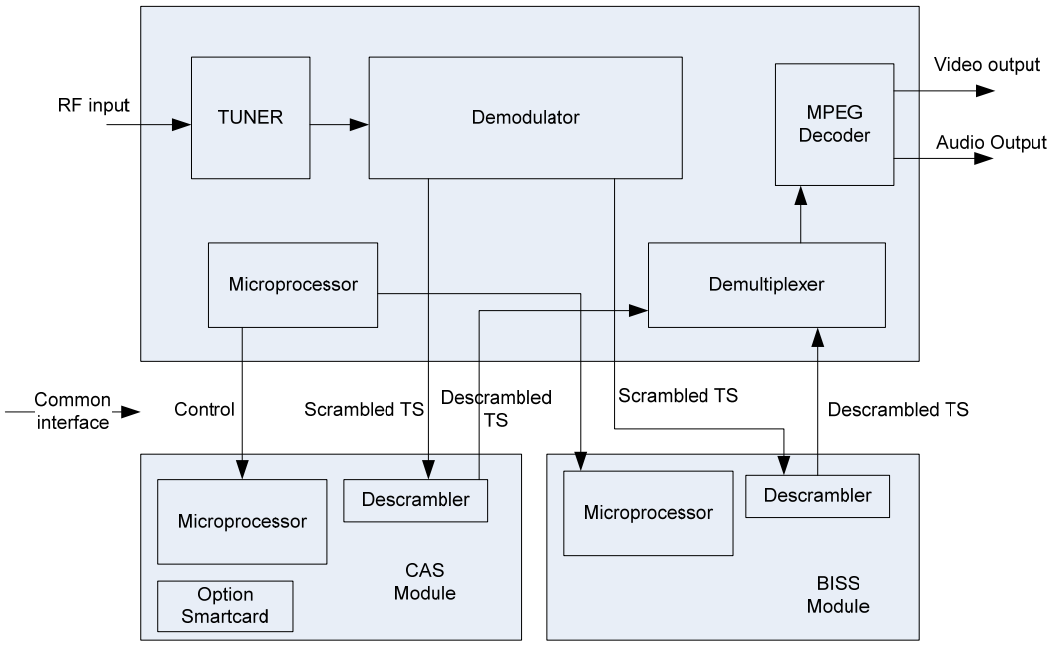

Figure 2.8 Common interface modules in connection with host

Figure 2.8 shows the diagram how the common interface works. The radio signal (RF) is demodulated into scrambled transport stream. The channels encrypted by BISS are sent to BISS module for descramble. After that, the channels will be sent back to

demultiplexer and decoder to get the video and audio signal. However, the encrypted channels by CAS need the CAS module to perform the descramble signal.

Available products

1) Harmonic ProView 7100 is multi format integrated receiver-decoder (IRD) and others specifications listed as the following

Figure 2.9 Hamonic Pro view 7100
http://www.harmonicinc.com/product/proview-7100

- MPEG2 and MPEG4 decoding
- Four TS descramblers with four integrated DVB-CI slots
- HD-SDI, SD-SDI, HDMI and analog video outputs

2) BISS CI module is inserted into the DVB-CI slots to be used for descrambling the BISS encrypted channels.

Figure 2.10 Aston BISS CI modules
http://www.aston-france.com/modules/biss-professionnel.php

CHAPTER III
METHODOLOGY AND SYSTEM DESIGN

This chapter describes the methodology and system design of the Conditional access system for cable TV subscription using fixed control word scramble. The first section discusses about design of the system and second section explains all methods related to our system.

3.1 The system architecture overview

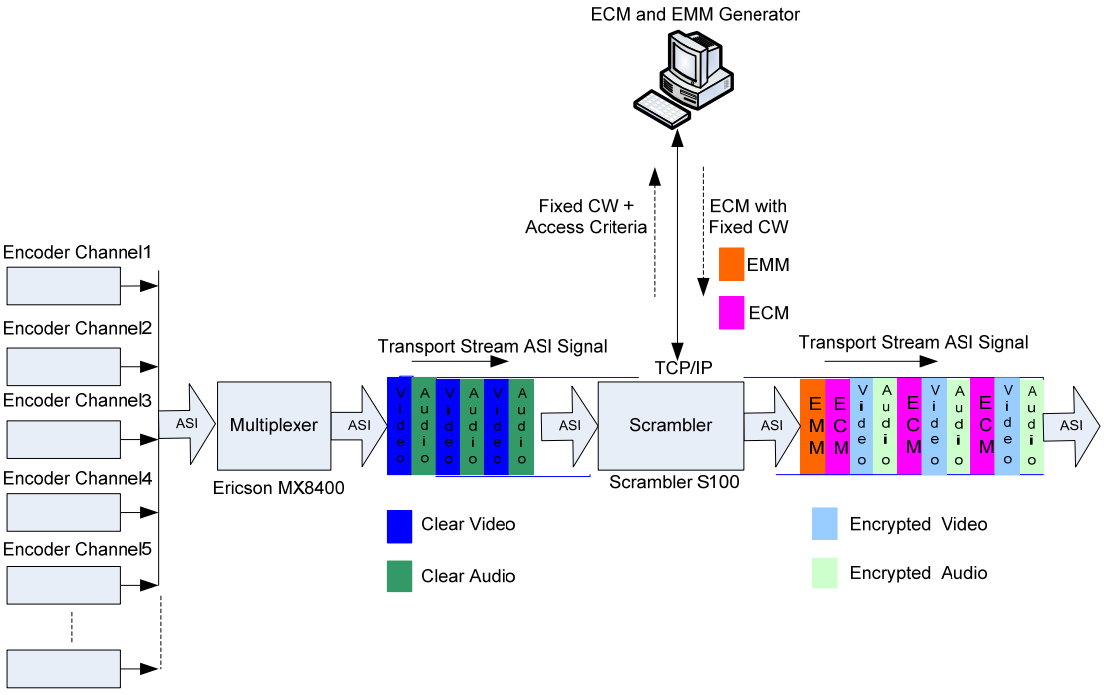

Figure 3.1 System Architecture Overview

The system called Conditional Access System for cable TV subscription using Fixed Control Word scramble (CASFCW) is designed Figure 3.1 shows the

system architecture of CASFCW. There are TV channels encoded with MPEG-2, all channels stream are multiplexed into Transport stream (TS) signal by using Multiplexer. All TV channels in the TS are Free-to-air (not encrypted), the fixed 16 characters CW need to be prepared and configured in the Scrambler S100. The Scrambler sends the fixed 16 characters CW to CAS system for asking the ECMs, the ECMs is sent back to Scrambler according to fixed 16 characters CW as well as EMM. The number of ECM is based on the number of encrypted channels in the TS; the ECM is located under all encrypted channels. The Scrambler gets the ECMs and EMM from CAS and injects them into payload in the TS. Finally, the TV channels in TS are encrypted with fixed 16 characters CW.

The TS output of Scrambler S100 is sent to Modulator in order to convert the baseband TS signal into RF signal for sending to Satellite. The end users need STB to receive the satellite signal and also is required the DVB-S qualification. The implementation of this project is based on DVB standard and all equipment is also complied to the DVB standard as show in Fig 3.1

3.2 Structure chart of the system

In this section, we discuss about the related theories of the CASFCW system. The system is divided into four processes, Establishing connection process, Reading Transport stream process, Acquiring ECM and EMM process and Creating fixed CW process. Figure 3.2 shows the structure chart of CASFCW.

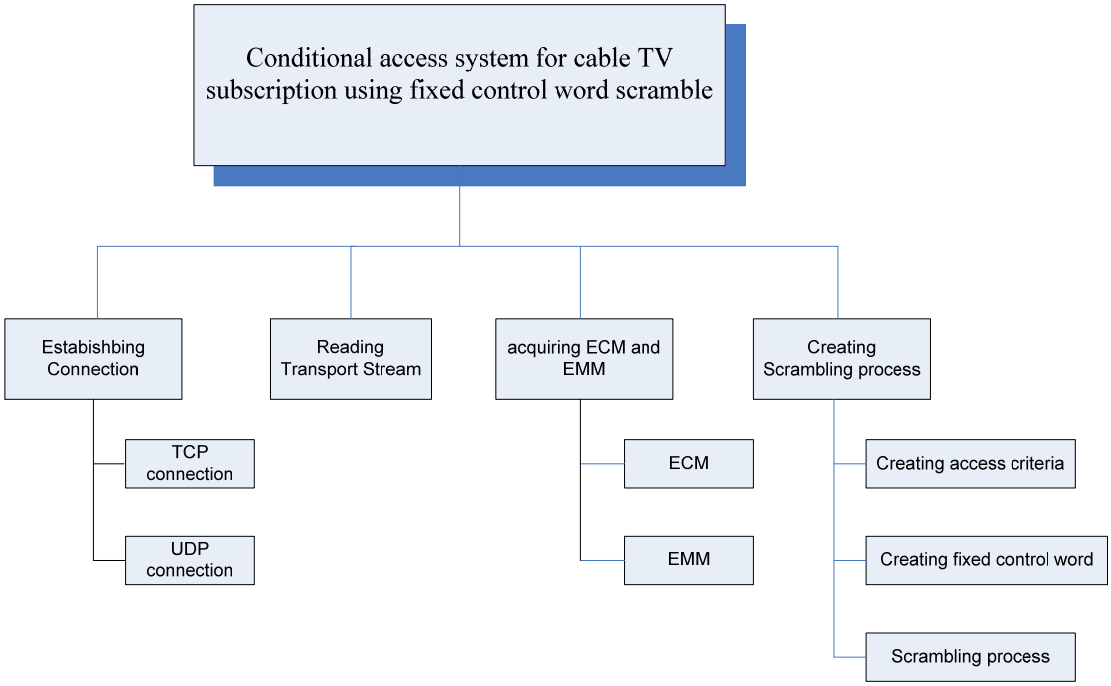

Figure 3.2 The CASFCW system Structure Chart

3.2.1 Establishing connection process

Connection between CAS and Scrambler is based on TCP and UDP depending on type of message. The ECM message requires for TCP connection only because of ECM containing important CWs. In term of EMM, the connection can be either TCP or UDP depend on delay time of connection between CAS and Scrambler.

3.2.1.1 TCP connection

The ECMs are the keys of Conditional Access System, they cannot be lost, otherwise the some periodic of video will be black out. In order to get the ECMs correctly, reliability of connection must be high. The TCP connection is introduced to use for communication between ECM generator and SCS.

TCP is connection oriented, the connection have to be established before sending the data and stopped the connection after ending the data. In this case, CW is sent on reliable connection. The process is shown as Figure 3.3

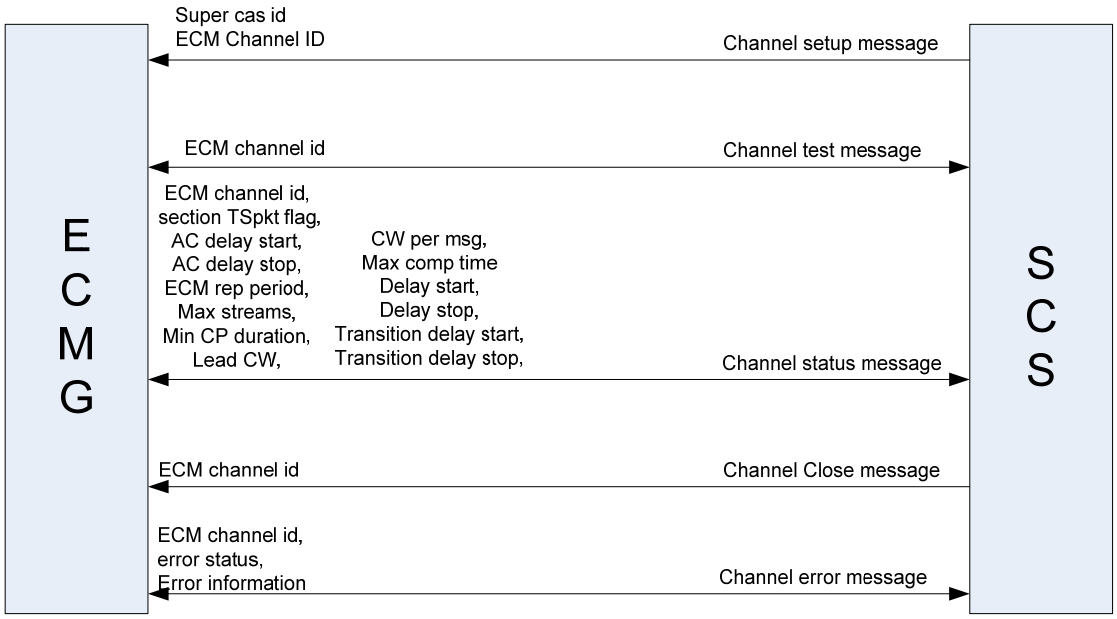

Figure 3.3 TCP connections between ECMG and SCS

3.2.1.2 UDP connection

UDP is user datagram protocol and based on connectionless. The data is sent as datagram and may not be reliable without ordering of the data. In this case, EMMs are used UDP to send the EMM data to the Set-top-boxes periodically. If some STBs are missing to receive the EMMs data, they can wait for a while to receive the EMMs data in next sending period. The diagram in Figure 3.4 shows for the process of an EMMs sending format.

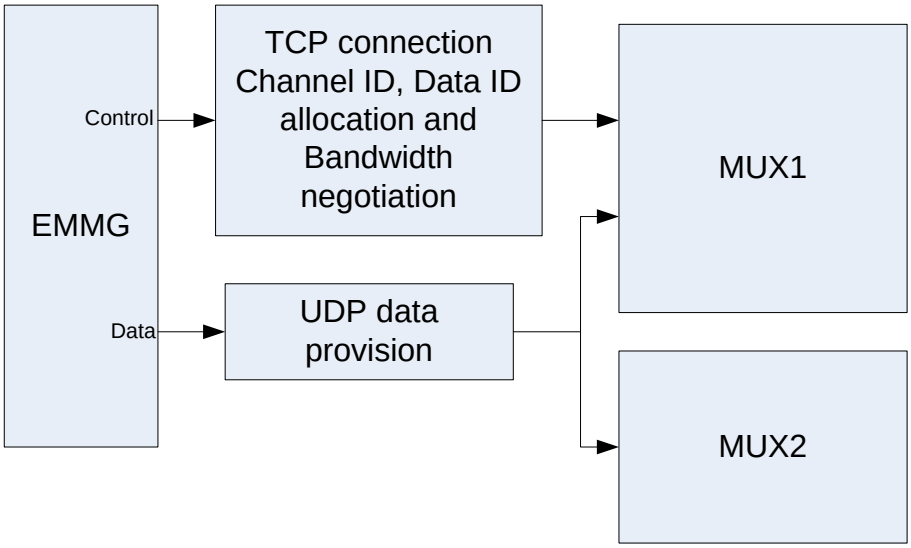

Figure 3.4 EMM sending process

3.2.2 Reading transport stream process

This section, we discuss about the Transport stream (TS) that needs to be imported into the system. The process shown in Figure 3.5 describes about MPEG systems standard. The elementary streams are obtained by compressing and coding the video and audio signal. The main propose of compression is to reduce the number of bits that is required to represent the video image and audio. The compression streams can be sent over lower bit-rate than uncompressed streams and there are many formats of compression methods e.g. MPEG-1, MPEG-2, and MPEG-4 H.264 etc.

The TS consists of all video and audio components that are compressed and coded according to the MPEG standard as called elementary stream. It also includes DVB table for further using in the STB. All elementary streams of all TV channels will be multiplexed together in a transport stream and The MPEG transport stream is a standard for transmission as shown in Figure 3.5.

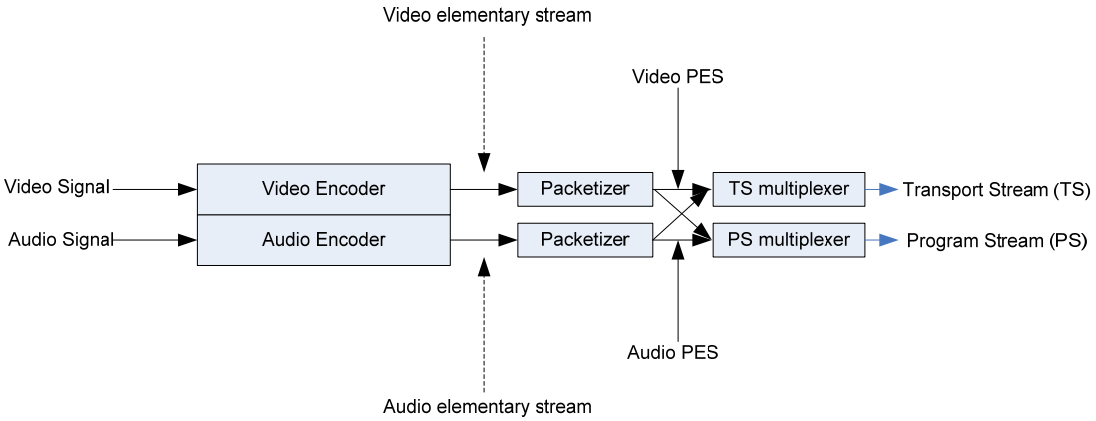

Figure 3.5 Overview of MPEG system standards.

MPEG Transport stream (TS) Packet

The multiple program channels of digital video channels are combined as Transport streams. The MPEG Transport stream is used the fixed length packet size of 188 bytes with 4-byte header and the payload of the Transport stream packet is 184 bytes. The details are shown in Figure 3.6

This format is for transmission and storage in environments where the errors may be occurred, so we need to add some error checking in the packet before sending out in order to recovery the loss packet while they are being transmitted.

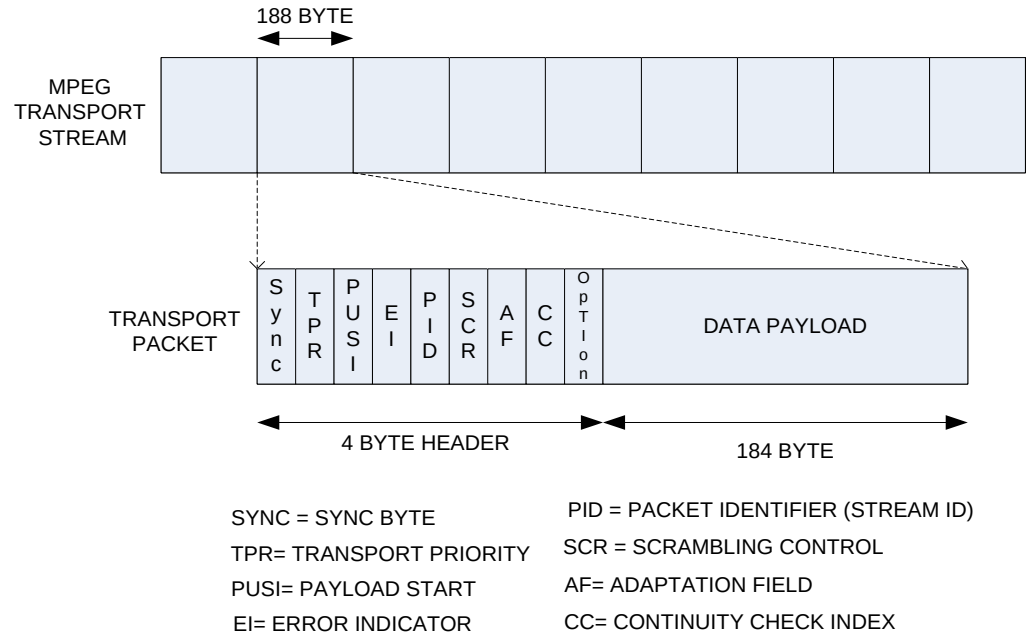

Figure 3.6 MPEG Transport Stream Packets

3.2.3 Acquiring ECM and EMM process.

3.2.3.1 Acquiring ECM

The Head-end interface specifications such as ECMG SCSs, are based on a connection-oriented communications paradigm (i.e. channel/streams). Alternatively, all these interfaces can be implemented using a transaction-based communications paradigm using the Simulcrypt Integrated Management Framework SIMF.

When a new ECM stream is created in a transport stream, a new ECM id shall be assigned to it by the head-end, according to the operational context (ECM stream creation or ECMG replacement). The value of the ECM id parameter remains unmodified as long as the ECM stream exists. The combination {« ECM » type + Super CAS id + ECM id} identifies uniquely this new ECM stream in the whole system.

The stream setup message is used for sending the ECM channel id, ECM stream id, ECM id and Nominal CP duration to ECMG to setup the stream. Once the stream test message is ready, the ECM stream id and ECM id are

sent. The stream status message is implied to be ready of sending the CW and stream close request message and stream close response message are indicated which stream in the channel need to be closed. The stream error message is used for showing which stream sending is not completed. The access criteria and CW value are carried with this message sending to ECMG to compute the ECM datagram. Once the ECM is generated then it is sent back to SCS again, as show in Figure 3.7

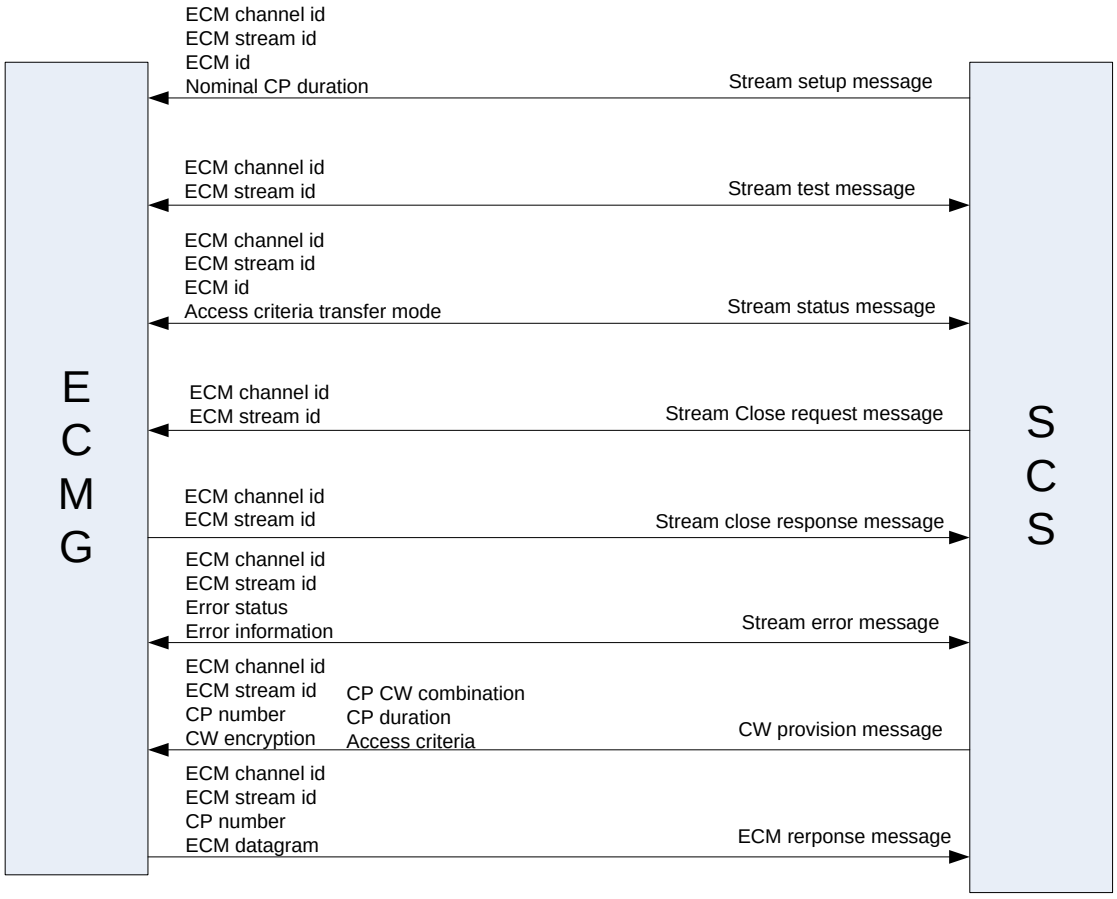

Figure 3.7 Process of acquiring the ECM

3.2.3.2 Acquiring EMM

The data message is used by the EMMG to send, on a given data ID the Data channel ID and data stream ID are optional parameters. The client ID/data ID pair shall identify in a unique manner an EMM/Private Data stream across the system. For example, if two EMMGs send an EMM stream with the same data ID

to the same multiplexer port, the multiplexer shall be able to distinguish between the two streams by looking at the client ID field in the data provision message.

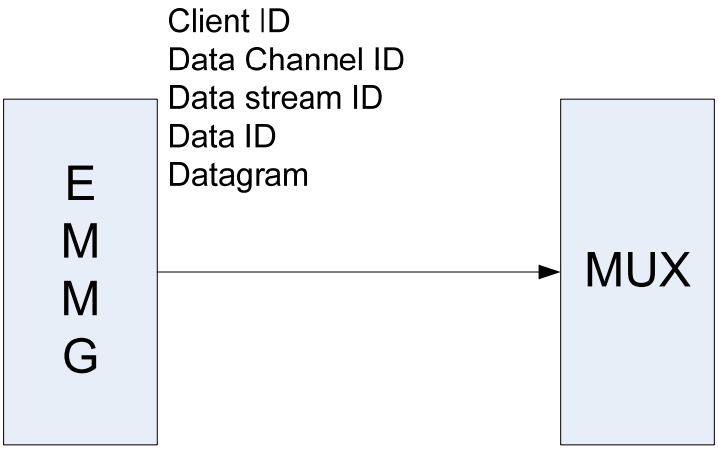

Figure 3.8 Process of acquiring the EMM

3.2.4 Creating scrambling process

In the creating of scrambling process, it is divided into three processes, creating access criteria process, creating fixed control word process and scrambling process. The details are explained as follows.

3.2.4.1 Creating access criteria process

The Access criteria is the specific information that required by ECMG to generate the ECMs. According to the DVB Simulcrypt standard, the access criteria is transmitted to SCS in the format that is understandable to the corresponding ECMG, so that ECMs can be generated properly. Figure 3.9 shows the flow of this process.

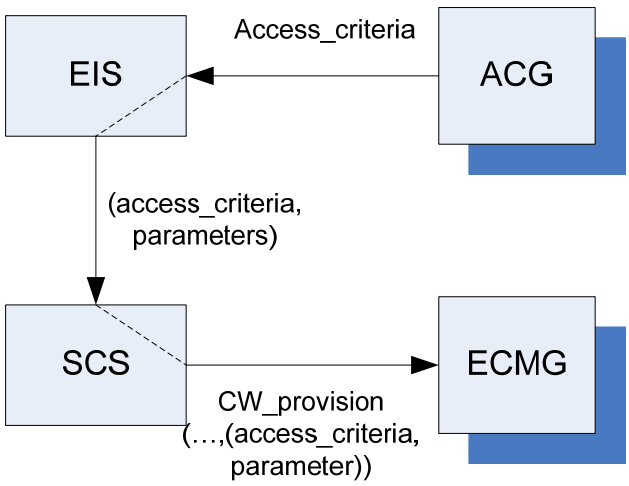

Figure 3.9 Access criteria creating process

3.2.4.2 Creating fixed control word

The bits in binary numbers or sequences are numbered from the left, according to engineering notation. Bit 0 is on the right and is the least significant one; the bit on the left is the most significant one. Here is an example of engineering notation for an n-bit number:

$$b_{(n-1)}\, b_{(n-2)} \ldots b_1 b_0$$

The 64-bit CW is derived from the SW according to the DVB-CSA specification.

3.2.4.3 Scrambling process

The PES packet header and an Adaptation field are not scrambled. The scramble of the first part of the PES packet payload is exactly the same as a TS packet with a similar size payload. The remaining part of the PES packet payload is divided in the blocks of 184 bytes and each block is scrambled exactly the same as a TS packet payload of 184 bytes. When the length of the PES packet is not a multiple of 184 bytes packet, the last part of PES payload is scrambled exactly same as

a TS packet with a similar size payload. Mappings of scrambled PES packets into TS packets show in Figure 3.10.

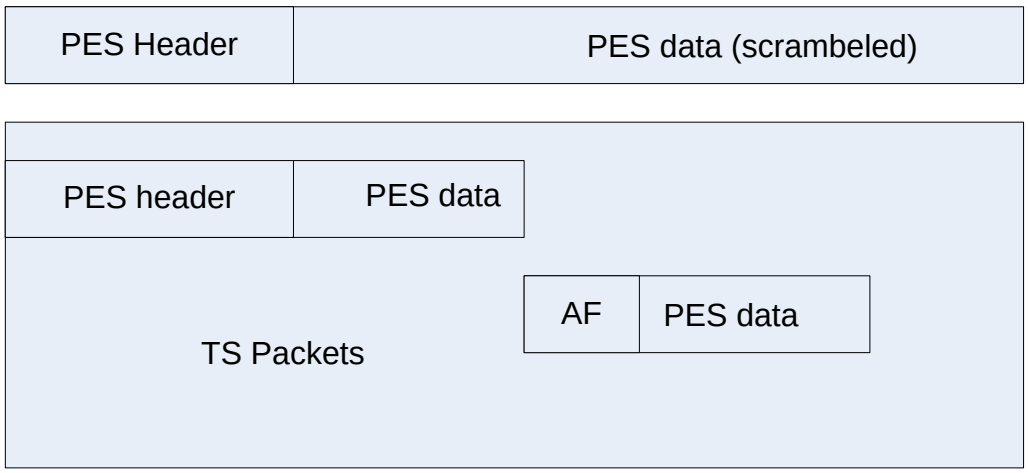

Figure 3.10 Mapping of scrambled PES packets into TS packets

CHAPTER IV
IMPLEMENTATION

In this chapter, we present the implementation, experiments. The system architecture and configuration are described. Finally, we show how the experiments and their result are conducted. The figure shows how the system works,

4.1 Equipment Configuration Specification

We present the hardware and software needed for implementation are described as the following as well as their configuration in the experiments.

4.1.1 Hardware

The Hardware tools for implementing the CASFCW consist of two types of equipment currently available. The detail of each equipment is described as the following:

Compunicate Scrambler S100

Scrambler S100 is a product from Compunicate Technologies INC. It is designed based on DVB Common Scrambling Algorithm Standard and mainly used for digital TV program scrambling. The main function of the unit is to use for scrambling the MPEG transport stream and it also supports the service level and component level scrambling.

Figure 4.1 Compunicate Scrambler S100

- RAM : 64MB
- Software version: V1.22
- H/W version: 3.5
- Software: FW

Ericson Multiplexer 8400

Ericson Multiplexer 8400 is used to combine the multiple input streams into single or multiple output streams. The input stream can be Video, Audio or data MPEG stream.

Figure 4.2 Ericson Multiplexer 8400

- RAM: 64MB
- Software version: 5.26
- H/W version: 12.3
- Computer HP360 G
- CPU: Pentium 4
- RAM: 128GB
- Harddisk: 500GB

4.1.2 Software

- Windows 7 Ultimate
- Ncompass version: 1.5.3

4.2 System Implementation

The processes of system implementation are described as shown in Figure 4.3.

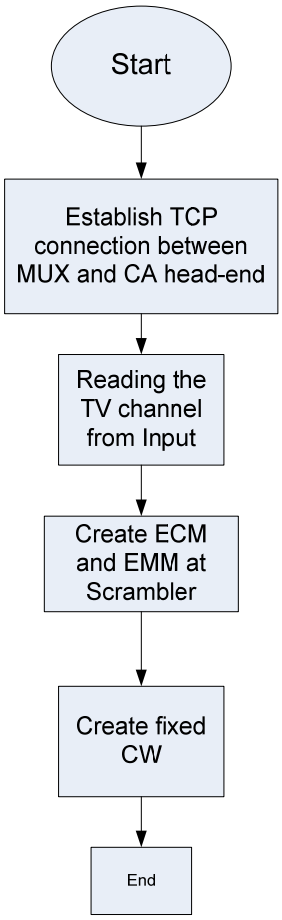

Figure 4.3 The design and implementation of the Conditional Access System for Cable TV Subscription using Fixed Control word.

The diagram shows overview of system implementation, consisting of four steps. The first step is to establish the TCP connection for communication between CAS and Scrambler. The ECMs and EMM are sent via connection-oriented protocol as called “TCP” because they need the reliable connection to carry the important Control word within the ECM. The second step performs reading the transport stream TV channels. All TV channels will be read and stored in the memory. The third step is to create the ECM and EMM packet within the scrambler. The last step is to configure

the fixed control word (CW) that will send out in order to acquire the ECM from the CAS.

4.3 Configuration of each step

This section is described each step configuration of implementation process.

4.3.1 Establish TCP connection between CAS and Scrambler

The connection between CAS and Scrambler need to setup at scrambler as TCP/IP. This reliable connection is used for sending the necessary fixed Control word (CW) from Scrambler to CAS and acquiring the ECM from CAS. Figure 4.4 shows how to establish TCP connection configuration.

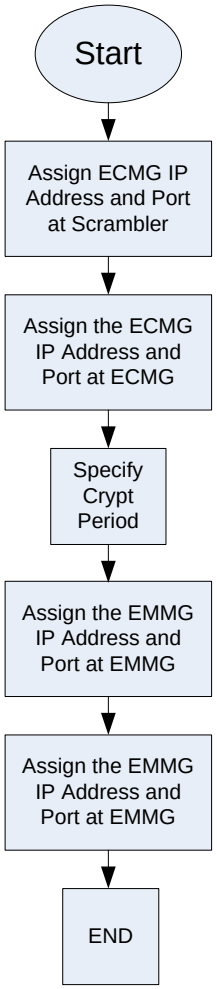

Figure 4.4 Diagram of TCP connections between CAS and Scrambler.

Table 4.1 Parameters and configuration of ECM and EMM

Parameter	Value
Ecmg_IP Address	192.168.12.5
Ecmg_IP Port	4350
Emmg_TCP port	4640
Emmg_UDP port	0
Crypto Period (sec)	15

Table 4.2 Parameters and configuration of EMM port and EMM BW

Parameter	Value
Emm input method	TCP
Emm_Pid	32(20H)
Emm Bandwidth(kbit)	500
Emm_channel_ID	0
Emm_stream_ID	0
Emm_data_ID	0
Emm_private_Data	

4.3.2 Reading the TV channels stream

The TV channels stream have to be loaded and stored in the scrambler in order to make sure that all incoming services are ready to perform the encryption. If some services are loaded incorrectly, they have to be performed loading again. Figure 4.5 shows diagram of reading the TV channels stream and Table 4.3 shows parameters of reading the TV channels stream.

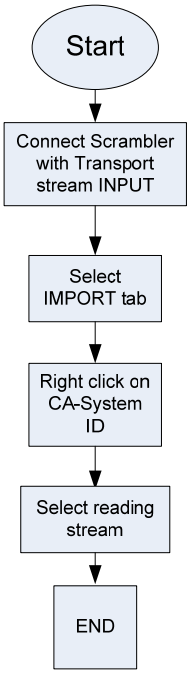

Figure 4.5 Diagram of reading the TV channels stream

Table 4.3 Parameter of reading the TV channels stream

Service ID	PMT ID
201	441
202	442
203	443
204	444
205	445

4.3.3 Acquiring an ECM and EMM from CAS

The ECM will be generated by CAS according to the parameter sending from scrambler. The CAS needs some parameters from scrambler to generate the ECM and EMM correctly. The following parameters are needed to configure at scrambler.

- Stream ID
- CA System ID
- Channel ID

Figure 4.6 and Table 4.4 shows the acquiring an ECM and EMM from CAS and CA system ID values respectively.

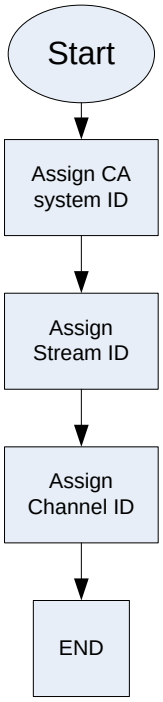

Figure 4.6 Diagram of acquiring an ECM and EMM from CAS

Table 4.4 Parameter of CA system ID values

CA System_ID	Value
System_ID	1556(614H)
SubSystem_ID	0(0H)

Table 4.5 Output programs Encrypt setup

Output Program	Value
Output Program No.	201
Program_CA	stream_1
Stream Information	Pid:550(226H)
stream type	ISO/IEC 13818-2 Video
Pid_CA	None

4.3.4 Creating fixed Control word (CW)

The CWs are generated by scrambler and manually enter via the provided GUI. The CW character is based on 16 Hex numbers and need to select the difficult

numbers to prevent the piracy. Normally, the access criteria (AC) numbers have to be provided without configuring on fixed CW. In this case, we need to configure both AC and fixed CW in order to allow the scrambler to send the fixed CW to CAS for acquiring ECM. Figure 4.7 shows how to creating fixed Control word and Table 4.6 shows the configuration of fixed Control word and Access Criteria.

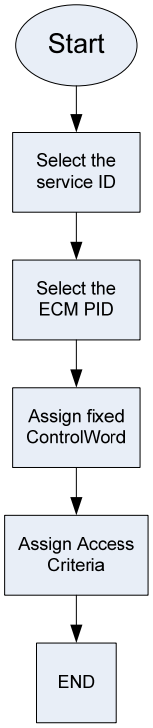

Figure 4.7 Diagram of creating fixed Control word

Table 4.6 Configuration of fixed Control word and Access Criteria

ECM Parameter	Value
ECM_streams	Stream1
Ecm_Pid	1341(53dH)
ECM_AC Data	900100060001000200C9
Ecm_Private_Data	
Ecm_Fixed CW	67 52 86 3F BD 55 AA BC

4.4 Analysis of MPEG Transport Stream and network traffic connetion.

The analysis of transport stream is done by using “MPEG Analyzer Textronix MTS 4000” Dektec Transport Stream DTA-2160 and Ether real V 0.9.8. The details of each Analyzer to use for this research are described as the following.

- Tektronix MTS4000 is the MPEG Analyzer Instrument that complies with the standard for MPEG stream analysis and interoperability testing. The purpose of this instrument is to analyze and find the root cause of problem in the Transport stream. The specification is listed as the following.

CPU: Intel i7 860 Quad-core CPU

Memmory: 4GB

- Dektec monitoring is also the MPEG Analyzer but it has more different function from Tektronix MTS4000. It is capable to show the keys that are being used (Odd or Even) for scrambling the MPEG packet. Its specification is shown below.

CPU: Pentium 4 CPU 3 GHz

Memory: 992 MB

Hardisk: 80GB

Dektec card: DTA-2160

- Ethereal is the Network Analyzer. It is able to capture the traffic in the network. In this case, the Ethernet protocol and packet frame can be shown or monitored for analysis of the connection between CAS and scrambler.

4.4.1 The analysis of MPEG transport stream.

There are two bits in the header of each Transport Stream Packet as called Scrambling Control. They will be used to indicate to the status of scrambling control packet as show in Table 4.7.

Table 4.7 Transport_scrambling_control values

Bit values	Description
00	No scrambling of TS packet payload (MPEG-2 compliant)
01	Reserved for future in DVB use
10	TS packet scrambled with Even key
11	TS packet scrambled with Odd key

4.4.2 The analysis of communication between CAS and Scrambler.

The communication between CAS and Scrambler is based on TCP/IP protocol. The TCP is used to communicate between CAS and Scrambler. Figure 4.8 shows the steps of sending the fixed Control word (CW).

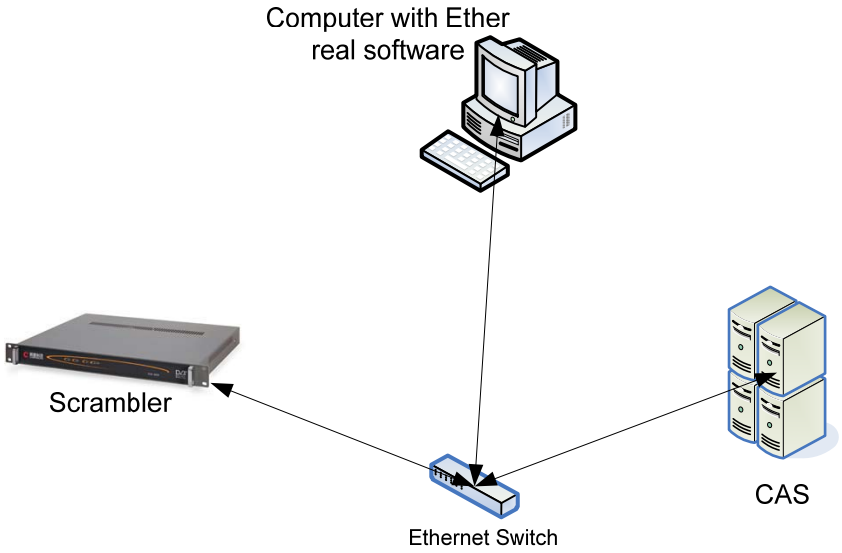

Figure 4.8 How to analysis the communication between CAS and Scrambler.

4.4.2.1 Creating the ECM Channel.

In the first step of communication, the TCP is created to use for communication. The ECM channel with ID is created for sending the ECM as shown in Figure 4.9.

ECM channel ID: 1

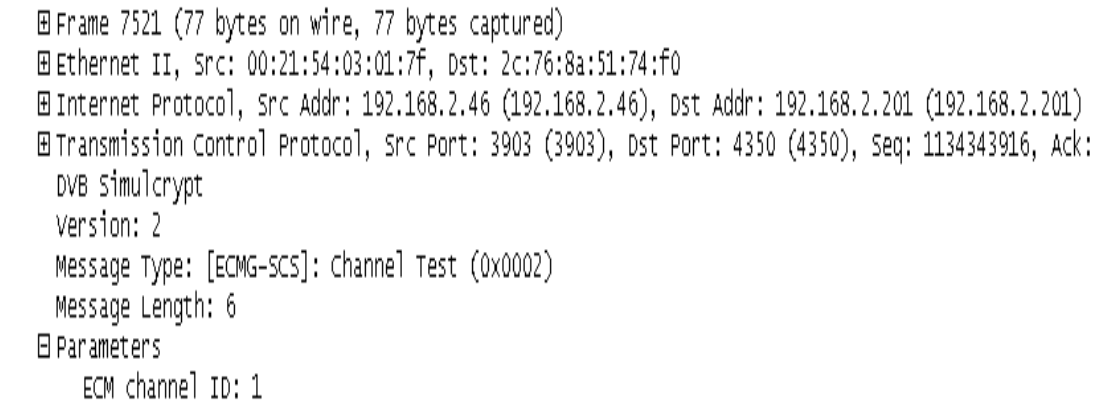

Figure 4.9 message of creating the ECM channel

4.4.2.2 Generating parameters for ECM broadcasting.

The Scrambler receives the parameters from CAS to be used for ECM broadcasting. The ECM need to be broadcasted in milliseconds in order to make sure that every STBs are received. The following shows sample parameters used for ECM broadcasting. Figure 4.10 shows message of necessary parameters of scrambler.

Delay start: 600

Delay stop: 0

ECM repetition period: 300

Minimum crypto period duration: 150

Number of Control word require in advance: 1

Number of control word required: 2

Maximum computation time: 14000

```
⊞ Frame 7522 (128 bytes on wire, 128 bytes captured)
⊞ Ethernet II, Src: 2c:76:8a:51:74:f0, Dst: 00:21:54:03:01:7f
⊞ Internet Protocol, Src Addr: 192.168.2.201 (192.168.2.201), Dst Addr: 192.168.2.46 (192.168.2.46)
⊞ Transmission Control Protocol, Src Port: 4350 (4350), Dst Port: 3903 (3903), Seq: 1016813443, Ack:
  DVB Simulcrypt
  Version: 2
  Message Type: [ECMG-SCS]: Channel Status (0x0003)
  Message Length: 57
⊟ Parameters
    ECM channel ID: 1
    Section/TS packet flag: MPEG-2 Packet (1)
    Delay start: 600
    Delay stop: 0
    ECM repetition period: 300
    Maximum number of streams: 0
    Minimum crypto period duration: 150
    Number of control word required in advance: 1
    Number of control word required: 2
    Maximum computation time: 14000
```

Figure 4.10 Message of necessary parameters of scrambler

4.4.2.3 Sending the fixed Control word (CW) to CAS for asking the ECM stream.

The fixed control words are sent to CAS to acquire the ECM according to the Access Criteria. There are many TVs channels in the transport stream. The access criteria is use to identify which channel will be encrypted. The two fixed control words are sent to CAS at the same time as shows in Figure 4.11.

Control word period number 44754: 7895B5C25AE7A1E2

Control word period number 44755: 7895B5C25AE7A1E2

Network ID: 1

Transport ID: 2

Service ID : 201

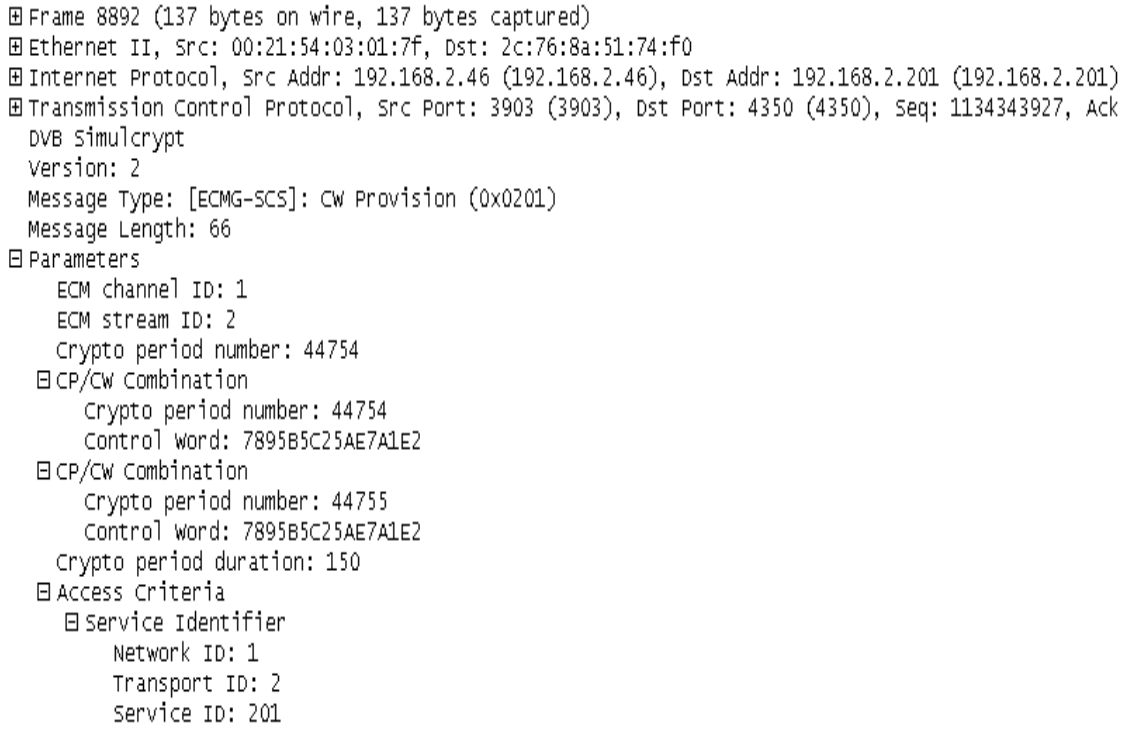

Figure 4.11 Message of fixed control word values

4.4.2.4 The ECM data is sent back to Scrambler.

As soon as CAS received the control word, it will ask the keys from encryptor and uses that key to encrypt the control cord. The encrypted control cord will be sent back to scrambler to inject into the transport stream. Figure 4.12 shows the message of an ECM datagram.

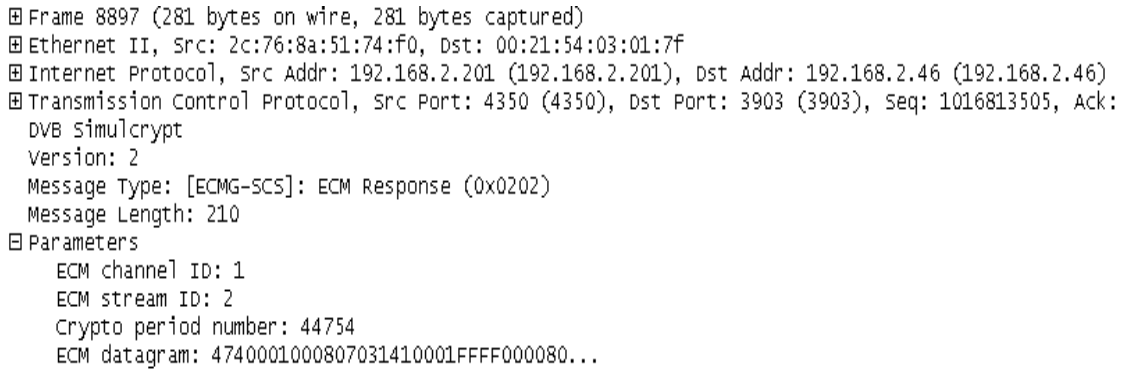

Figure 4.12 Message of an ECM datagram

4.4.2.5 The two fixed Control word of next Crypto Period .

The control words have to remain still the same value until requesting the change value of control word from User. Figure 4.13 shows the control cord value at any period time. The values of CW do not change even the crypto period duration or crypto period numbers are changed.

CW period number 44755: 7895B5C25AE7A1E2

CW period number 44756: 7895B5C25AE7A1E2

Network ID: 1

Transport ID: 2

Service ID : 201

```
⊞ Frame 13235 (137 bytes on wire, 137 bytes captured)
⊞ Ethernet II, Src: 00:21:54:03:01:7f, Dst: 2c:76:8a:51:74:f0
⊞ Internet Protocol, Src Addr: 192.168.2.46 (192.168.2.46), Dst Addr: 192.168.2.201 (192.168.2.201)
⊞ Transmission Control Protocol, Src Port: 3903 (3903), Dst Port: 4350 (4350), Seq: 1134344435, Ack:
  DVB Simulcrypt
  Version: 2
  Message Type: [ECMG-SCS]: CW Provision (0x0201)
  Message Length: 66
⊟ Parameters
    ECM channel ID: 1
    ECM stream ID: 2
    Crypto period number: 44755
  ⊟ CP/CW Combination
      Crypto period number: 44755
      Control Word: 7895B5C25AE7A1E2
  ⊟ CP/CW Combination
      Crypto period number: 44756
      Control Word: 7895B5C25AE7A1E2
    Crypto period duration: 150
  ⊟ Access Criteria
    ⊟ Service Identifier
        Network ID: 1
        Transport ID: 2
        Service ID: 201
```

Figure 4.13 Message of necessary parameters of Scrambler

CHAPTER V
EXPERIMENTAL RESULTS

In this chapter, we present the experimental results of the system. The experiments are conducted on 5 different brands of STBs, PSI S-X, SUN BOX, GMMz, HUMAX and D-khoom. They receive the loop back L-band signal from Modulator. Five signal channels are created and encoded by using MPEG-2 coding and multiplexed into single DVB transport stream. The transport stream signal is transmitted to external scrambler for encryption process. The external scrambler use fixed CW to scramble with video and audio data stream within the transport stream. The fixed CW is sent to ECM and EMM generator to encrypt with private key from conditional access system. Finally, the encrypted video/audio signals are modulated and up-converted to L-band signal.

5.1 Equipment to perform experiment.

5.1.1 Set-Top-Box (STB), it is device consisting of a set of electronic device to perform de-modulation, de-Multiplexing, de- scrambling and decoding and connects to TV set. We focus on STBs that supporting DVB-S and use five different brands of STBs to do experiments and each one is also different CAS supported as shown in Table 5.1

Table 5.1 STB models

STB Model	Specification	Encryption Type	Picture
PSI S-X	-Satellite L Band Input -MPEG-2 -DVB-S1 -Composite Video Output -Audio (L/R)	BISS	
SUN BOX	-Satellite L Band Input -MPEG-2 -DVB-S1 -Composite Video Output -Audio (L/R)	ABV CAS	
HUMAX IR-H100S	-Satellite L Band Input -MPEG-2 -DVB-S1 -Composite Video Output -Audio (L/R)	Irdeto CAS	
GMMz	-Satellite L Band Input -MPEG-2 -DVB-S1 -Composite Video Output -Audio (L/R)	Novel	
D-Khoom	-Satellite L Band Input -MPEG-2 -DVB-S1 -Composite Video Output -Audio (L/R)	BISS	

There are three different CAS brands (ABV, Irdeto and Novel) supporting in each sample STB and another brand is supported scrambling standard as called BISS. Different CAS has different method and algorithm to encrypt the ECM data. The STB that supporting BISS function can directly enter the BISS key to the unit. However, in term of creating the ECMs, our solution is not to change any process in creating of all ECMs but we only focus on how to fix the CW values inside the ECM. Therefore, all processes within the STBs are still certified the standards.

5.1.2 Network Protocol Analyzer

We use Ether-real software in the research. This software is installed on the personal computer and connected to switch hub to receive the broadcast TCP packet for our analyzing. We can see the details of CWs values that generated by scrambler before getting ECMs from ECM generator. The solution of our research is to fix CWs values. The values must not be changed in anytime until we do it manually. This software use for monitoring and analysis the CWs values sent from external scrambler or multiplexer. We use Ether-real version 0.9.8 as show the details in Figure 5.1

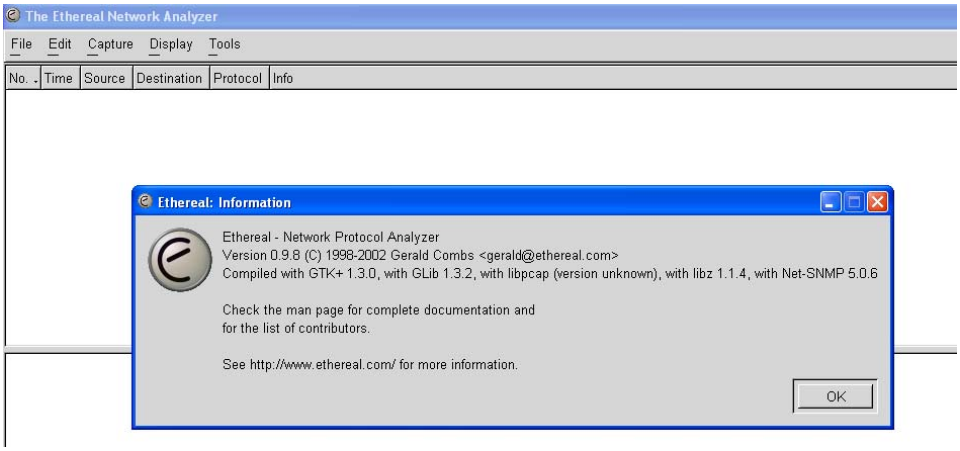

Figure 5.1 Ether real network protocol Analyzer

5.1.3 MPEG Analyzer

This equipment is used for analyzing the transport stream packet in order to see inside the ECM packet and header of each TS packet. Actually, there is a

scrambling control bit to identify which key (ODD/EVEN) being used for scrambling the transport stream. This key should be corresponding with the table ID within TS header of the ECM. Figure 5.2 shows physical of MPEG analyzer.

Figure 5.2 MPEG Analyzer

5.2 Channel configuration

There are five TV channels to setup in the experiment and different encryption type has done on each channel. Table 5.2 shows a list of five channels and types of their encryption.

Table 5.2 CAS configuration in each channel

Channel Name	Type of encryption
Channel1	Irdeto CAS only
Channel2	ABV CAS only
Channel3	Novel CAS only
Channel4	BISS only
Channel5	BISS and Irdeto encryption (our solution)

5.3 Solutions

In this section, we discuss about the solutions of our experimental and its results. There are three solutions of experiments.

5.3.1 Fixing Control Word (CW) in the Multiplexer

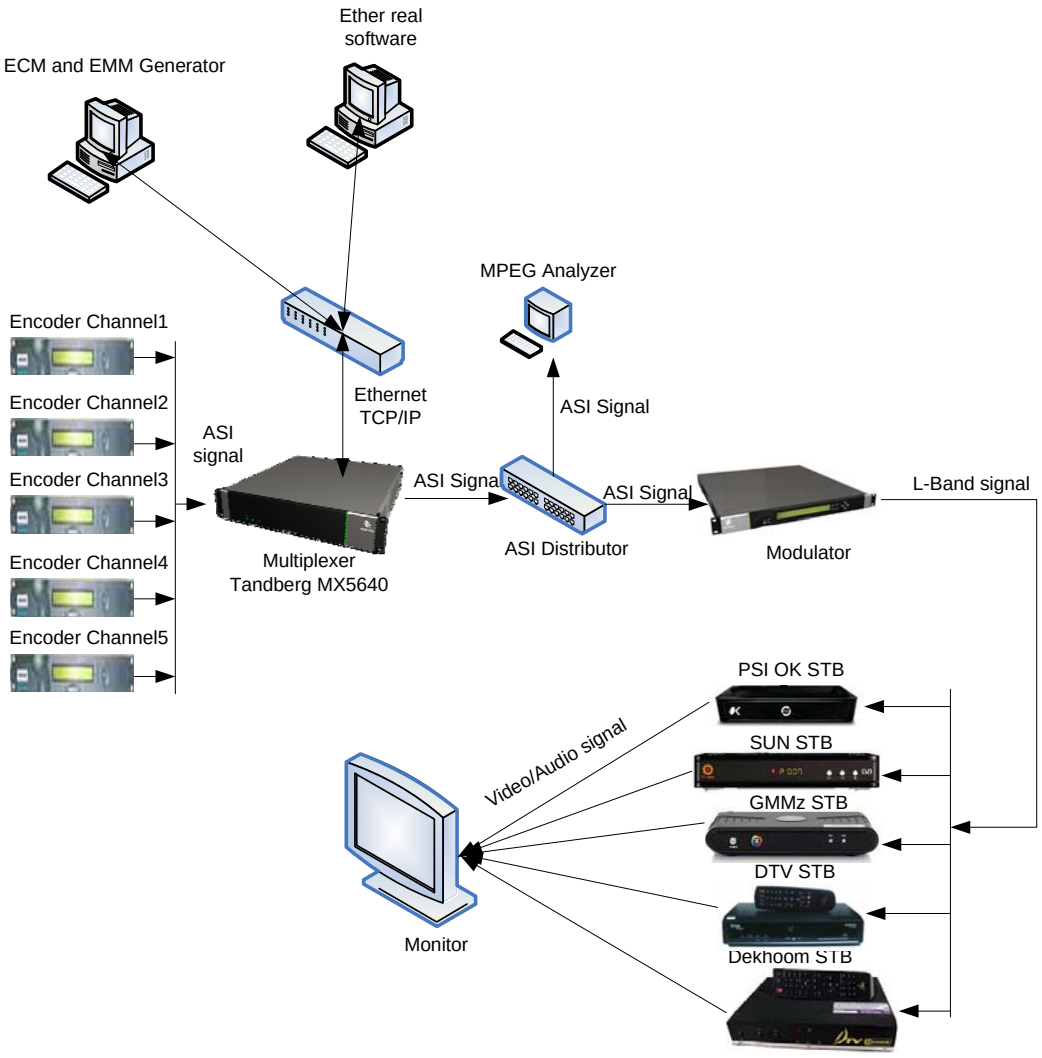

Figure 5.3 Fixed CW by Using MX5640 Multiplexer

In the Figure 5.3, we use Multiplexer MX5640 to implement and perform fixing CW. The DVB Common Scrambling Algorithm (DVB-CSA) Software is embedded in the Multiplexer and connects to the CAS by using TCP/IP connection.

At the beginning of the process, there are five Tandberg encoders connecting to Multiplexer. All five channels are encoded and transmitted to Multiplexer as Program Elementary Stream (PES). The Multiplexer receives all five PES streams and multiplexed them together in one Transport Stream. The Multiplexer and Conditional Access System (CAS) are negotiating together on TCP/IP connection in order to have the Entitlement Control Message (ECM).

This experiment is focused on each value of Crypto Period (CP) setting. Actually, Control Word (CW) value is randomly changed according to CP setting in the Multiplexer and the CP can be set manually. The ECM is replied from the CAS as soon as they get CW from Multiplexer. From the results of experiment, we monitor the CW value for each TV channel. The Network analyzer software is able to monitor all CW values between CAS and Multiplexer. The results of CW values are shows in table 5.3.

Table 5.3 Relation of CP duration and CW values in Multiplexer.

CP duration setting	**10Sec**	**15 Sec**	**1 hour**	**3 hour**	**4 hour**	**5 hour**
CW Values for each channel	Change in every 10 Sec	Change in every 15 Sec	Change in every 1 hour	Change in every 3 hour	Change in every 3.26 hour	Change in every 3.14 hour
Channel1	HUMAX	HUMAX	HUMAX	HUMAX	HUMAX	HUMAX
Channel2	SUN BOX	SUN BOX	SUN BOX	SUN BOX	SUN BOX	SUN BOX
Channel3	GMMz	GMMz	GMMz	GMMz	GMMz	GMMz
Channel4	PSI S-X D-khoom	PSI S-X D-khoom	PSI S-X D-khoom	PSI S-X D-khoom	PSI S-X D-khoom	PSI S-X D-khoom
Channel5	HUMAX	HUMAX	PSI S-X HUMAX D-khoom	PSI S-X HUMAX D-khoom	PSI S-X HUMAX D-khoom	PSI S-X HUMAX D-khoom

5.3.2 Encryption by external Scrambler and scrambling with fixed CW by Multiplexer.

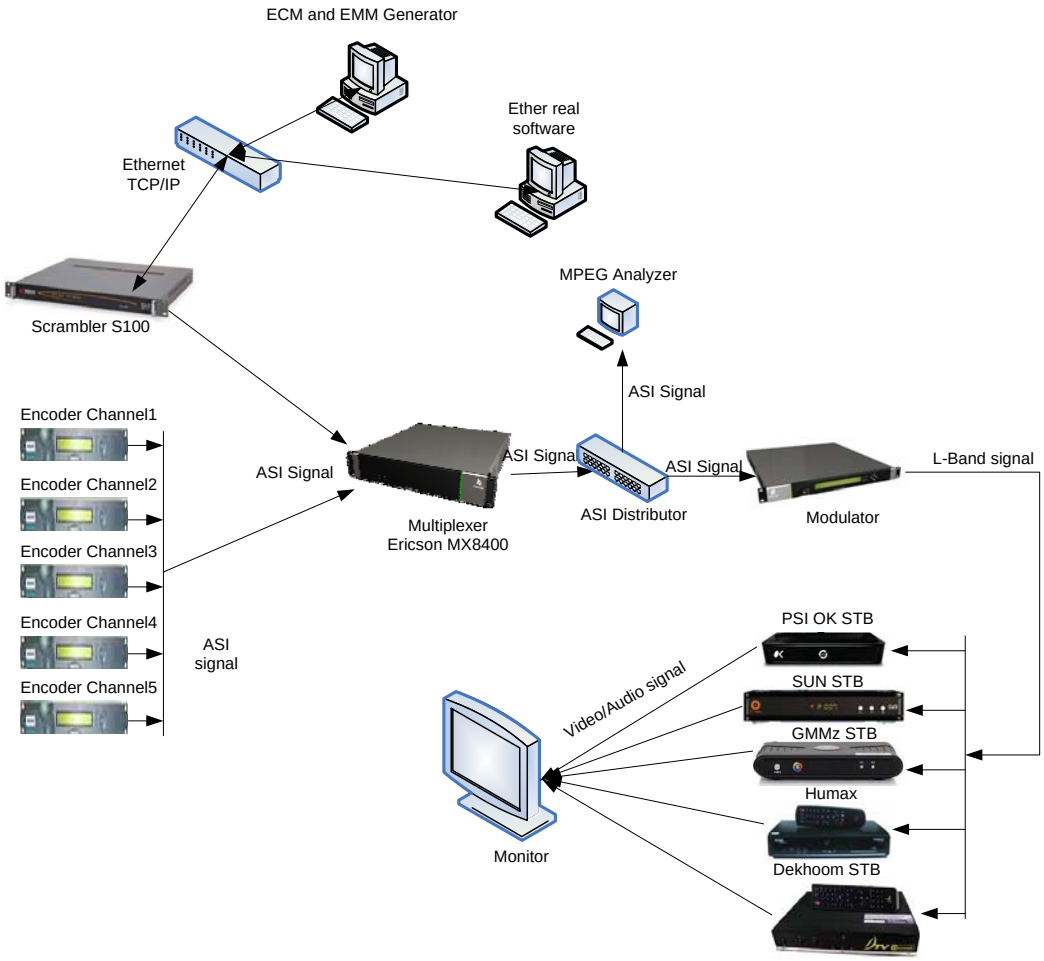

Figure 5.4 Fixed Control Word (CW) by external Scrambler but before Multiplexering

In this solution as shown in Figure 5.4, there are five encoded channels. Channel1-channel3 are multiplexed and encrypted by Multiplexer. Channel4 is scrambled by Multiplexer as BISS and channel5 is implemented with our solution as BISS&CA. The external scrambler (S100) is connected to CAS in order to get ECMs and they are fed to Multiplexer. In the Multiplexer, channel5 is scrambled by using BISS and combined the incoming ECM under channel5. The Network analyzer software is running to monitor the CWs values and also there is a MPEG Analyzer to verify and analyze all PID parameters in the Transport stream packet. The encrypted

Video and Audio packets are sent to Modulator for converting to L-band frequency in order to check the Video and audio component by using five brands of STBs.

The table ID in the each ECM channel is analyzed and checked what table ID number is being used. The table ID number can be 80 or 81. Furthermore, two bits of Scrambling Control Bit (SCB) in each TS packet have to be recorded what bits status are shown. It can be “10” or “11”.

All STBs are accepted to receive the L-Band frequency and give the output for each TV channel as results shown in Table 5.4. Table 5.4 shows the results of our experiments.

Table 5.4 Table ID and Scrambling Control Bits values with 15 seconds CP duration.

Channel Name	Type of encryption	CW on Scrambler	CW on Ether-real	Table ID in ECM TS on TS Analyzer	Scrambling control bits on TS Analyzer
Channel1	Irdeto CAS	N/A	Changing every 15 Second	changing “80” and “81” every 15 second	changing “10” and “11” every 15 second
Channel2	ABV CAS	N/A	Changing every 15 Second	changing “80” and “81” every 15 second	changing “10” and “11” every 15 second
Channel3	Novel CAS	N/A	Changing every 15 Second	changing “80” and “81” every 15 second	changing “10” and “11” every 15 second
Channel4	BISS	7895B5C25 AE7A1E2	7895B5C25 AE7A1E2	Fixed at “80”	Fixed at “10”
Channel5	BISS & Irdeto CAS	7895B5C25 AE7A1E2	7895B5C25 AE7A1E2	changing “80” and “81” every 15 second	Fixed at “10”

Table 5.5 The results of decryption in each channel.

Channel Name	Type of encryption	PSI S-X	SUN BOX	HUMAX IR-H100S	GMMz	D-Khoom
Channel1	Irdeto CAS	X	X	Y	X	X
Channel2	ABV CAS	X	Y	X	X	X
Channel3	Novel CAS	X	X	X	Y	X
Channel4	BISS	Y	X	X	X	Y
Channel5	BISS and Irdeto CAS	Y	X	Y, tableID=80 N, tableId=81	X	Y

X= cannot descramble and Y= Show Video and Audio

5.3.3 Encryption with fixed Control Word (CW) by external Scrambler.

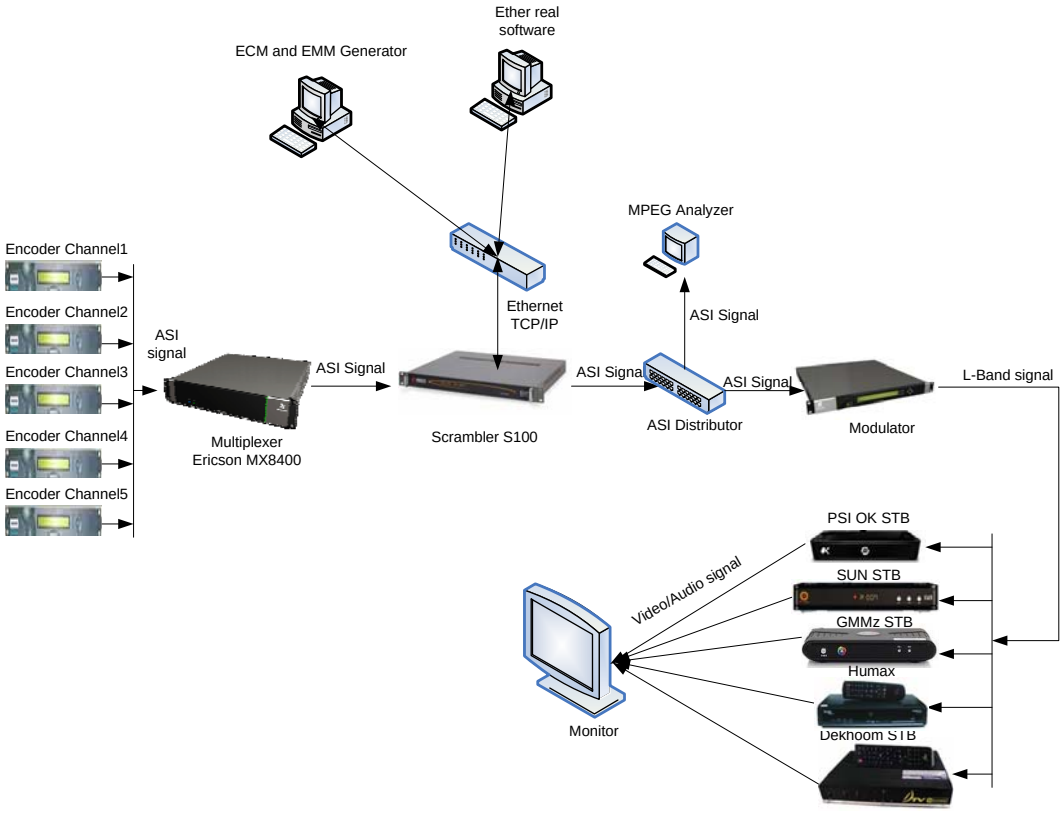

Figure 5.5 Experimental system diagrams.

With this solution shown in Figure 5.5, the encoded five PES channels from each Encoder are combined into one transport stream by Multiplexer. The three channel1-3 are encrypted by using CAS (Irdeto, ABV and Novel) respectively. Channel4 is scrambled with BISS by Multiplexer. The channel5 is implemented with our solution by External scrambler. The ECM is generated by CAS when getting the CW from Multiplexer, the process of both ECM and BISS is done by External scrambler. The five encrypted are multiplexed into a transport stream and sent through Modulator for converting to L-band frequency.

The network monitoring software is connected in the same network as CAS and Multiplexer in order to monitor and analyze the DVB packet and CW values.

Furthermore, we have a MPEG analyzer to analysis the ECM packets and TS packet and these results is recorded in the Table 5.6. Finally, there are five STBs to monitor the Video and Audio signal and the results are shown in Table5.7.

Table 5.6 Table ID and Scrambling Control Bits values with 15 seconds CP duration.

Channel Name	**Type of encryption**	**CW on Scrambler**	**CW on Ether-real**	**Table ID in ECM TS on TS Analyzer**	**Scrambling control bit on TS Analyzer**
Channel1	Irdeto CAS	N/A	Changing every 15 Second	changing “80” and “81” every 15 second	changing “10” and “11” every 15 second
Channel2	ABV CAS	N/A	Changing every 15 Second	changing “80” and “81” every 15 second	changing “10” and “11” every 15 second
Channel3	Novel CAS	N/A	Changing every 15 Second	changing “80” and “81” every 15 second	changing “10” and “11” every 15 second
Channel4	BISS	7895B5C25 AE7A1E2	7895B5C25 AE7A1E2	Fixed at “80”	Fixed at “10”
Channel5	BISS and Irdeto CAS	7895B5C25 AE7A1E2	7895B5C25 AE7A1E2	changing “80” and “81” every 15 second	changing “10” and “11” every 15 second

Table 5.7 The results of decryption in each channel.

Channel Name	Type of encryption	PSI S-X	SUN BOX	HUMAX IR-H100S	GMMz	D-Khoom
Channel1	Irdeto CAS	X	X	Y	X	X
Channel2	ABV CAS	X	Y	X	X	X
Channel3	Novel CAS	X	X	X	Y	X
Channel4	BISS	Y	X	X	X	Y
Channel5	BISS and Irdeto CAS	Y	X	Y	X	Y

X= cannot descramble and Y= Show Video and Audio

5.4 Comparison of experiment results.

This section compares the three techniques that the system has been used for our solutions. Table 5.8 shows the comparison of three techniques to fix Control Word (CW).

Table 5.8 Comparison of three techniques to fix control word (CW) on Channel5.

No.	Description	Channel 5				
		PSI S-X	**SUN BOX**	**HUMAX IR-H100S**	**GMMz**	**D-Khoom**
1	Fixing Control Word (CW) in the Multiplexer	W	X	Y	X	W
2	Encryption by external Scrambler and scrambling with fixed CW by Multiplexer	Y	X	Y, tableID=80 N, tableId=81	X	Y
3	Ecryption with fixed Control Word (CW) by external Scrambler.	Y	X	Y	X	Y

W= sometimes cannot descramble X= cannot descramble all the time and Y= Show Video and Audio

The results in Table 5.8 show that two models of STBs sometimes cannot watch the channel5 on the solution1 because the Multiplexer could not fixed the CW all the specific of time and the other two channels are encrypted with others CAS. The result of solution2 is to show that PSI S-X and D-khoom STBs are able to watch the channel5 except HUMAX in the period of tableID=81 (15Sec). Finally, the solution3 is allowed all complied CAS-STBs and BISS-STB able to watch channel5 for all periods of specific time.

5.5 The Problems Found in the Proposed Work

During the experiments, encounter with some problems and issues. Some equipment that is used for experiments are very expensive. We need to perform the experiment carefully. The changing of CWs values is random, we cannot move backward to the last CWs values in order to record or perform the previous experiment, otherwise we need to start to perform at the beginning again.

CHAPTER VI
CONCLUSIONS AND FUTURE WORKS

Now, all TV channels via satellite are required to encrypt. The security of encryption of all channels is depending on which type of services and business models of channel owner. The pay TV channels need to have the CAS to protect their value channels and be able to disable or enable the subscribers for payment the subscription fee. The other channels called “free-view-channel” are required to encrypt the content as well but the security of the channels can be lower. In the real situation of STBs in the field, there are many brands and models being used and some of them are not supported the BISS function. Currently, no standard mentioned about CAS using fixed control word and no related research found. We implement these solutions in order to avoid changing a million of STBs in the field.

6.1 Conclusions

After the experiments, we analyze, verify and evaluate the results. We get the conclusion of both methods to fixed control words which are “encryption by external Scrambler and scrambling with fixed CW by Multiplexer” and “encryption with fixed Control Word (CW) by external Scrambler”. There are five channels in different type of encryption and five STBs to be used for testing with the channels. The conclusions of each method are described as follows.

1) Fixing Control Word (CW) in the Multiplexer: the multiplexer is not allowed to have the long crypto period. In the other word, the control word value cannot be fixed.

2) Encryption by external Scrambler and scrambling with fixed CW by Multiplexer: there are two equipment scramblers to perform the encryption. Scrambler S100 is responsible for encryption the control word and generating the ECM. The multiplexer MX5640 is to scramble the transport stream with the control word.

Therefore, there is no synchronization between scrambling control bits value in header of TS packet and location of keys in the ECM. The results of this method are to make the STBs getting black screen within two crypto periods.

3) Encryption with fixed Control Word (CW) by external Scrambler:

For this method, an equipment scrambler is used to perform the scrambling TS packet and negotiate with ECMG to obtain the ECM. The scrambling control bits and the location of keys in the ECM are synchronized. However, the number of encrypted channels of this method is less than the method in (1)

6.2 Future works

The equipment scrambler needs to be developed to have the number of channels more than that of channels currently supported. In other word, STBs have to be developed to ignore the synchronization of scrambling control bits and location keys in the ECM.

REFERENCES

1 Digital Video Broadcasting (DVB), “Head-end implementation of DVB SimulCrypt”, ETSI TS 103 197 V1.1.1 (2000-02), pp.15-20, 135-136

2 European Broadcasting Union, “Basic Interoperable Scrambling System with Encrypted keys”, (August 2002),pp. 6.

3 European Broadcasting Union, “Scrambling Basic Interoperable System (BISS)”, (March 2000),pp. 2-4.

4 European Broadcasting Union, “Digital Video Broadcasting (DVB);Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems”, October 1996, pp.10-11.

5 Joseph Tsun Kiet Man, “Broadcast Encryption”.

6 http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

7 Digital Video Broadcasting (DVB), ‘Technical Specification of DVB Simulcrypt”, 15 May 1997.

BIOGRAPHY

NAME	Mr. Witcha Burirak
DATE OF BIRTH	24 March 1997
PLACE OF BIRTH	Bangkok, Thailand
INSTITUTIONS ATTENDED	Mahanakorn University of Technology, 1994-1997: The Degree of Bachelor of Engineering (Telecommunication Engineering)
POSITION & OFFICE	1997 - Present Thaicom Public Company Limited. Tel. 0-2591-0736 Position : Engineer Specialist E-mail : wichab@thaicom.net