Digital video broadcasting module

CONDITIONAL ACCESS SYSTEM (CAS)

h.shirazi@qmul.ac.uk

Dr Hamid Shirazi

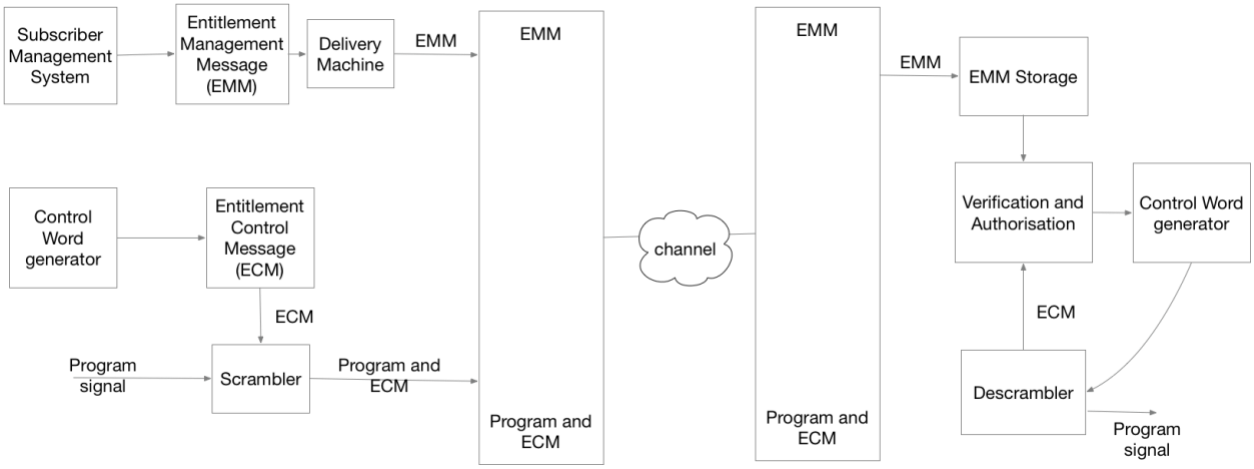
Table of Contents

Week3: Day-5

What is Conditional Access?

- Conditional access (CA) is a technique that implement a variety of technical and commercial systems components
    - to protect a TV program (or a number of TV program) form unauthorised viewers
    - thereby ensures that only those who paid will be able to access the program
- Implementation requires a variety of technical and commercial system to control the access
- Users have few options:
    - A monthly subscription fee (pay per channel/group of channel)
    - Fee for individual program (pay per view)
- The program signal is processed in a scrambler before transmission
- Within the framework of DVB, a **Common Scrambling System (CSS)** has been developed
- Specification is not published to deter pirates from developing illegal descrambler
- Absolutely secure scrambling procedure is almost impossible to build
- Additional initiative for developing anti-piracy law

Overview of complete CA system



- Some definitions:
    - Scrambling : re-ordering of the programme data according to an algorithm
    - Encryption : keys and codewords are encrypted to prevent non-authorised access
    - Ciphering : encryption
    - Control Word : required to scramble and de-scramble the data
    - Keys : required for encryption and decryption of control words
    - PRBS : Pesudo-random bit stream
    - EMM : Entitlement Management Message - authorizes the smart card to receive the programme. Changed fairly frequently.
        - For pay-TV the EMM is changed by the day or month depending on the subscription parameters.
        - For pay per view or video on demand it will be changed for each programme.
    - ECM : Entitlement Control Message - used to let the smart card descramble the programme. Changed very frequently.

Common Scrambling System (CSS)

- Common scrambling system is based on the cascading of the two ciphering procedure
    - In the first system, data block of 8 bytes each consisting of 8 bits are scrambled
    - In the second, the resulting data are re-scrambled bit by bit
- Figure 1 in the next slide shows scrambling procedure
- A decision needs to be taken which data to scrambled
- In MPEG-TS, header can not scrambled as it is required for receiver sync
- Mechanism should allow scrambling only a part of the program if necessary.
- In the MPEG-2 structure two levels at which ciphering can take places are envisaged:
    - The level of Packetised Elementary Stream (PES)
    - The level of Transport Stream (TS)
- Only one of these levels should be used at any time
- The respective headers (which are not ciphered) include control bits which has the same meaning at both level
    - First bit to determine if cipher is used
    - Second bit to determine even or uneven code word is used
        - Code words (keys) are changing from time to time

Bit values	Meaning in TS and PES respecitively
00	No scrambling
01	Not used
10	Scrambled with even code word
11	Scrambled with uneven code word

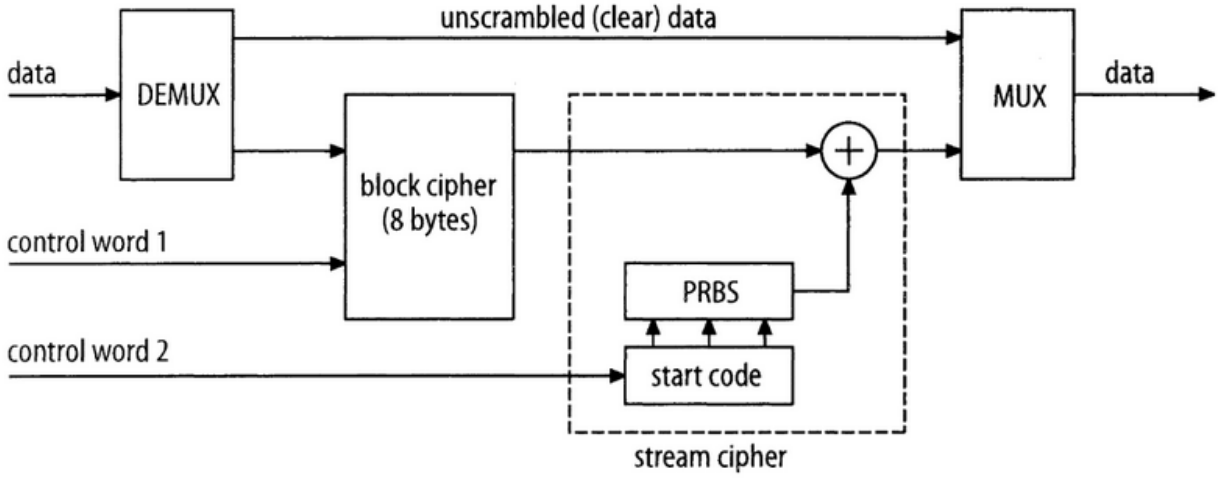


Figure 1: Block diagram common scrambling system (CSS)

How Scrambler Works?

- The first step utilises a block cipher procedure, a technique based on 8 bytes block
- A first “control word” is required for the ciphering
- The data stream coded in that way is then fed in to a stream cipher mechanism which operates on a pseudo random number generator
- It actually creates the random number for a certain period based on another control word
- This step can be implemented with the aid of feedback shift register, which at a given moment, with a specified initialisation value
- The bit-stream which is output by this generator is then added modulo-2 to the data to be scrambled

Restriction of Scrambling in PES Level

- With regard to mapping the PES onto the TS, following are the restrictions on scrambling
    - The PES header should not be larger than 184 bytes, i.e. it must fit into useful data range of the TS packet
    - From the beginning of the header, PES packet is divided into 184 byte segments which are then mapped onto TS packet
    - TS packets can therefore have no adaptation fields
    - If the last segment is smaller than 184 bytes, it will be preceded within the TS packet by an adaptation field of appropriate length
    - Should an adaptation field become necessary during the transmission of a scrambled PES packet, a separate TS packet has to be inserted which only contains this **adaptation field**.
- The aim of this limitation is to minimise the storage requirement at the receiver side by simplifying the deciphering

Descrambling Procedure

- A conditional access table (CAT) is specified as a part of Service Information (SI) within the framework of DVB.
- Two control words are required for descrambling. They are subject to separate encryption procedure at transmitter.
- They are combined to generate ECM: Block-wise & bit by bit descrambling
- The CAT also contains EMM
- The key (the encrypted version of the two control words) is changed frequently.
- The header has 2 bits to indicate whether scrambling has been applied
- Odd/even code words:
    - A new control word must be sent to the set-top box (STB) before it is required (we do not want to have to wait for the new control word before we can descramble).
    - However, we do not necessarily want to start using the new control word as soon as it arrives.
    - A system of alternating odd and even control words is used.
    - Each control word and scrambled packet is identified as either odd or even.
    - Only odd packets can be descrambled with the odd control words and vice-versa.