Scrambling and conditional access

5

The proportion of free access programs among analog TV transmissions by cable or satellite is decreasing continuously, at the same time as their number increases; hence, it is almost certain that the vast majority of digital TV programs will be pay-TV services, in order to recover as quickly as possible the high investments required to launch these services. Billing forms will be much more diversified (conventional subscription, pay per view, near video on demand) than what we know today, made easier by the high available bit-rate of the system and a "return channel" (to the broadcaster or a bank) provided by a modem.

The DVB standard, as explained in the previous chapter, envisages the transmission of access control data carried by the conditional access table (**CAT**) and other private data packets indicated by the program map table (**PMT**). The standard also defines a common scrambling algorithm (**CSA**) for which the trade-off between cost and complexity has been chosen in order that piracy can be resisted for an appropriate length of time (of the same order as the expected lifetime of the system).

The conditional access (**CA**) itself is not defined by the standard, as most operators did not want a common system, everyone guarding

jealously their own system for both commercial (management of the subscribers' data base) and security reasons (the more open the system, the more likely it is to be cracked quickly). However, in order to avoid the problem of the subscriber who wishes to access networks using different conditional access systems having a stack of boxes (one set-top box per network), the DVB standard envisages the following two options:

1. **Simulcrypt.** This technique, which requires an agreement between networks using different conditional access systems but the same scrambling algorithm (for instance, the CSA of the DVB), allows access to a given service or program by any of the conditional access systems which are part of the agreement. In this case, the transport multiplex will have to carry the conditional access packets for each of the systems that can be used to access this program.
2. **Multicrypt.** In this case, all the functions required for conditional access and descrambling are contained in a detachable module in a **PCMCIA** form factor which is inserted into the transport stream data path. This is done by means of a standardized interface (common interface, **DVB-CI**) which also includes the processor bus for information exchange between the module and the set-top box. The set-top box can have more than one DVB-CI slot, to allow connection of many conditional access modules. For each different conditional access and/or scrambling system required, the user can connect a module generally containing a smart card interface and a suitable descrambler.

The multicrypt approach has the advantage that it does not require agreements between networks, but it is more expensive to implement (cost of the connectors, housing of the modules, etc.). The DVB-CI connector may also be used for other purposes (data transfers for instance). Only the future will tell us which of these options will be used in practice, and how it will be used.

5.1 Principles of the scrambling system in the DVB standard

Given the very delicate nature of this part of the standard, it is understandable that only its very general principles are available; implementation details only being accessible to network operators and equipment manufacturers under non-disclosure agreements.

The scrambling algorithm envisaged to resist attacks from hackers for as long as possible consists of a cipher with two layers, each palliating the weaknesses of the other:

- a *block layer* using blocks of 8 bytes (reverse cipher block chaining mode),
- a *stream layer* (pseudo-random byte generator).

The scrambling algorithm uses two control words (even and odd) alternating with a frequency of the order of 2 s in order to make the pirate's task more difficult. One of the two encrypted control words is transmitted in the entitlement control messages (**ECM**) during the period that the other one is in use, so that the control words have to be stored temporarily in the registers of the descrambling device. There is also a default control word (which could be used for free access scrambled transmission) but it is of little interest.

The DVB standard foresees the possibility of scrambling at two different levels (transport level and PES level) which cannot be used simultaneously.

Scrambling at the transport level

We have seen in the preceding chapter (Fig. 4.6) that the transport packet header includes a 2-bit field called "transport_scrambling_ flags." These bits are used to indicate whether the transport packet is scrambled and with which control word, according to Table 5.1.

Table 5.1 Meaning of transport_scrambling_flag bits

Transport_scrambling_flags	Meaning
00	No scrambling
01	Scrambling with the DEFAULT control word
10	Scrambling with the EVEN control word
11	Scrambling with the ODD control word

Scrambling at transport level is performed after multiplexing the whole payload of the transport packet, the PES at the input of the multiplexer being "in the clear." As a transport packet may only contain data coming from one PES, it is therefore possible to scramble at transport level all or only a part of the PES forming part of a program of the multiplex.

Scrambling at the PES level

In this case, scrambling generally takes place at the source, before multiplexing, and its presence and control word are indicated by the 2-bit PES_scrambling_control in the PES packet header, the format of which is indicated in Figure 4.4. Table 5.2 indicates the possible options. The following limitations apply to scrambling at the PES level:

- the header itself is, of course, not scrambled; the descrambling device knows where to start descrambling due to information contained in the PES_header length field, and where to stop due to the packet_length field;
- scrambling should be applied to 184-byte portions, and only the last transport packet may include an adaptation field;
- the PES packet header should not exceed 184 bytes, so that it will fit into one transport packet;
- the default scrambling word is not allowed in scrambling at the PES level.

Table 5.2 Meaning of PES_scrambling_control bits

PES_scrambling_control	Meaning
00	No scrambling
01	No scrambling
10	Scrambling with the EVEN control word
11	Scrambling with the ODD control word

5.2 Conditional access mechanisms

The information required for descrambling is transmitted in specific conditional access messages (**CAM**), which are of two types: entitlement control messages (**ECM**) and entitlement management messages (**EMM**). These messages are generated from three different types of input data:

- a *control_word*, which is used to initialize the descrambling sequence;
- a *service_key*, used to scramble the control word for a group of one or more users;
- a *user_key*, used for scrambling the service key.

ECM are a function of the control_word and the service_key, and are transmitted approximately every 2 s. EMM are a function of the service_key and the user_key, and are transmitted approximately every 10 s. The process for generating ECM and EMM is illustrated in Figure 5.1.

In the set-top box, the principle of decryption consists of recovering the service_key from the EMM and the user_key, contained, for instance, in a smart card. The service_key is then used to decrypt the ECM in order to recover the control_word allowing initialization of the descrambling device. Figure 5.2 illustrates schematically the process for recovering control_words from the ECM and the EMM.

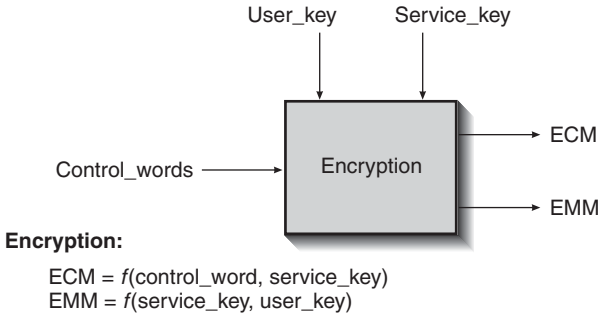

Figure 5.1 Schematic illustration of the ECM and EMM generation process.

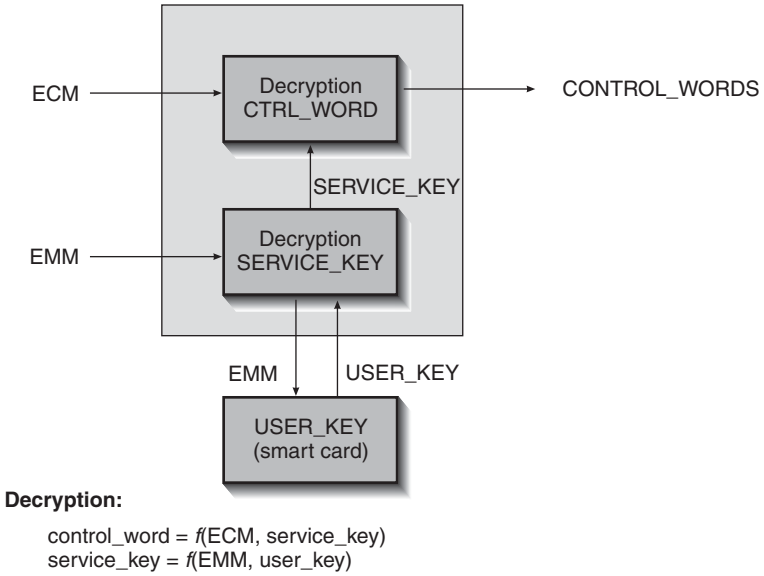

Figure 5.2 Principle of decryption of the control words from the ECM and the EMM.

Figure 5.3 illustrates the process followed to find the ECM and EMM required to descramble a given program (here program no. 3):

1. the program allocation table (**PAT**), rebuilt from sections in packets with PID = 0 × 0000, indicates the PID (M) of the packets carrying the program map table (**PMT**) sections;

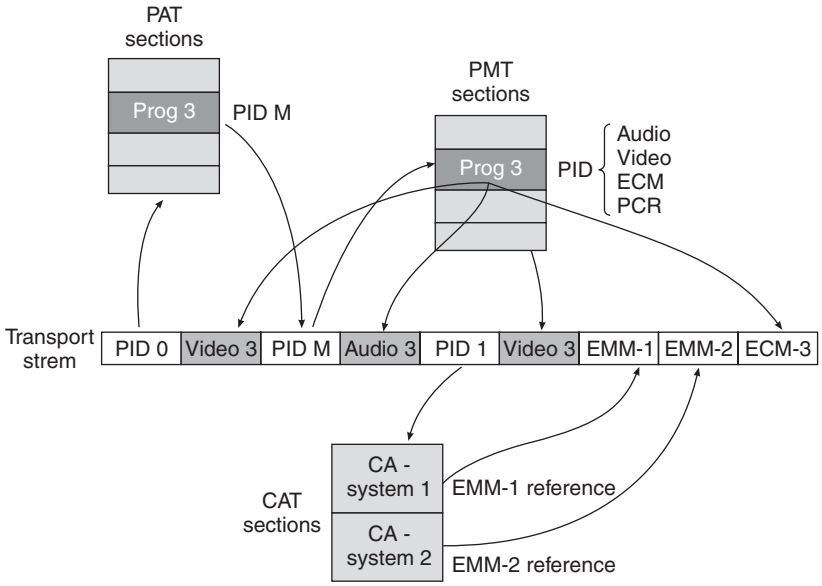

Figure 5.3 Process by which the ECM and the EMM are found in the transport stream.

2. the PMT indicates, in addition to the PID of the packets carrying the video and audio PESs and the PCR, the PID of packets carrying the ECM;
3. the conditional access table (**CAT**), rebuilt from sections in packets with PID $= 0 \times 0001$, indicates which packets carry the EMM for one (or more) access control system(s);
4. from this information and the user_key contained in the smart card, the descrambling system can calculate the control_word required to descramble the next series of packets (PES or transport depending on the scrambling mode).

The above-described process is indeed very schematic; the support containing the user_key and the real implementation of the system can vary from one operator to another. The details of these systems are, of course, not in the public domain, but their principles are similar.

5.3 Main conditional access systems

Table 5.3 indicates the main conditional access systems used by European digital pay TV service providers.

Most of these systems use the DVB-CSA scrambling standard specified by the DVB. The receiver has an internal descrambler controlled by an embedded conditional access software which calculates the descrambler control words from the ECM messages and keys contained in a subscriber smart card with valid access rights updated by the EMM.

Systems allowing pay-per-view often have a second card reader slot for a banking card as well as a modem to order the programs as well as charge the bank account.

Table 5.3 Main conditional access systems

System	Origin	Service providers (examples)
Betacrypt	Betaresearch (obsolete)	Premiere World, German cable
Conax	Conax AS (Norway)	Scandinavian operators
CryptoWorks	Philips	Viacom, MTV Networks
IrDETO	Nethold	Multichoice
Mediaguard 1 & 2	SECA (now Kudelski S.A.)	Canal+, Canal Satellite, Top Up TV
Nagravision 1 & 2	Kudelski S.A.	Dish Network, Premiere, German cable
Viaccess 1 & 2	France Telecom	TPS, AB-Sat, SSR/SRG, Noos
Videoguard/ICAM	News Datacom (NDS)	BskyB, Sky Italia