Lecture

Technologies and Services on Digital Broadcasting (6)

Scrambling (Conditional Access System)

1. Digital broadcasting and conditional access systems

The essential role of broadcasting is to convey information on a broad scale; therefore, "scrambling", which has the aim of restricting reception, is at odds with this role. In recent years, however, the implementation of fee-based broadcasting has made it necessary to prevent non-subscribers from receiving broadcasts, so scrambling of broadcast signals has nonetheless become widespread. This has been achieved through the "conditional access system", which is now a normal prescription for any new broadcast system. Although scrambling began with cable television (CATV) and limited-range terrestrial broadcasts, the advent of worldwide satellite-based broadcasts has fueled the development and implementation of large-scale conditional access systems.

A conditional access system generally consists of two main subsystems:

① A scrambling subsystem that a) scrambles the signal to prevent non-subscribers from receiving it and b) descrambles the signal at the subscribers' receivers.

② An access control subsystem that processes access control messages to determine whether descrambling is to be performed.

Satellite broadcasting, in particular, features a very broad broadcast target, for which unauthorized reception can have far reaching effects. It is for this reason that highly secure systems are employed for both the scrambling subsystem and access control subsystem.

The general requirements that scrambling systems must satisfy are as follows:

(1) it must be difficult for a third party to perform unauthorized reception (security);

(2) scrambled signal content must not be understandable (concealment);

(3) quality must not deteriorate (perceptibly) on restoring the signal (quality restoration); and

(4) receiver and operating costs must be low.

In digital broadcasting, moreover,

(5) efficient scrambling of all kinds of signals (as in multimedia broadcasts) must be possible, and

(6) various business formats such as multi-channel services and billing schemes must be supported.

2. Configuration of a conditional access system

Although a conditional access system can be achieved in

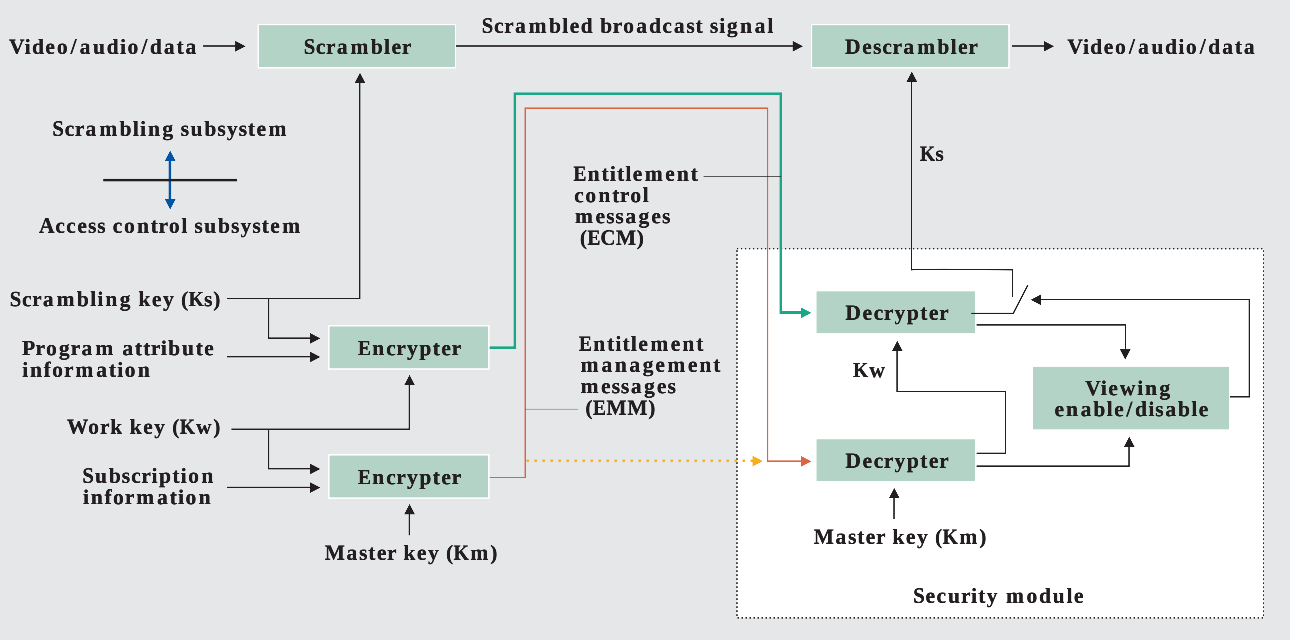


Figure 1: Configuration of a conditional access system

various ways depending on targeted services, required functions, and security, the basic configuration shown in Fig. 1 has been recommended by ITU-R [1].

Firstly, the system should perform scrambling according to the properties of the signals in question. Secondly, it should change the key regularly to maintain the security of the scrambling system, and transmit this key information to the receiver in a secure manner using a hierarchical encryption system. Thirdly, for the purpose of operating fee-based broadcasting, reception should be controlled according to the details of each user's subscription.

The following sections describe the conditional access functions implemented in digital broadcasting.

3. Signal scrambling system

The signal scrambling system is selected in accordance with the properties of the target signals. In this regard, conditional access systems for television broadcasting have once targeted analog broadcasting, and degradation in the restored signal due to transmission-path characteristics could occur if advanced signal scrambling were performed. Under these circumstances, many systems have been developed and deployed according to the level of security, restoration quality, etc., required by the target system.

On the other hand, scrambling of digital broadcast signals causes no degradation of the restored signal provided that the transmitted signal is correctly received. This makes it possible to use advanced scrambling techniques.

Various kinds of encryption technologies targeting digital data can be applied to the scrambling of a digital signal. Broadcast scrambling, however, may also employ an "effect control" system to reduce the degree of concealment and allow a slight amount of content to be recognized to promote subscriptions. In this case, control techniques based on detailed properties of the signal will be required in addition to encryption technology for digital signals.

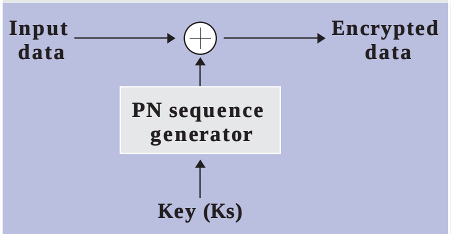
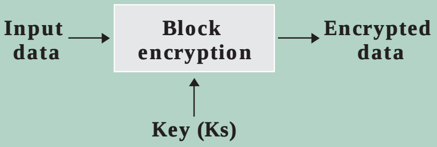
Technology for encrypting digital signals can be broadly classified as stream ciphers and block ciphers. Table 1 summarizes the features of these two types of ciphers.

In digital broadcasting, signals like video, audio, and various kinds of data having greatly different properties can be unified in the form of a digital signal and multiplexed on one stream for transmission. The most common system for performing this multiplexing is the one standardized by MPEG. This system features two signal scrambling methods: the first method scrambles transport stream (TS) packets, and the second method scrambles packetized elementary streams (PES) [2].

In either case, a detailed scrambling method is not specified and is instead prescribed on the application system side. For example, the Digital Video Broadcasting (DVB) system in Europe has standardized a signal scrambling system that combines block and stream ciphers[3]. A description of this scrambling system has not been officially released, though, and the system itself cannot be used outside Europe. As a result, different scrambling systems must be used when operating DVB-based systems outside of Europe.

Such a situation has occurred in Japan where some companies have implemented digital television broadcasting via Communication Satellite (CS) in which the signaling system conforms to DVB, but the scrambling system has been independently developed. As shown in Fig. 2, this scrambling system combines a block cipher and a stream cipher (which is applied to those sections of data

Table 1: Scrambling schemes for digital signals

System	Principle	Features	Application Examples
Stream cipher	 Input data Encrypted data PN sequence generator Key (Ks) A PN sequence bit (or byte) is added (EX-OR) to each bit (or byte) of the input stream.	Processing speed: High-speed processing easily achieved. Security: A difference in 1 bit (or byte) in the input stream generates a difference of 1 bit (or byte) in encrypted output.	- Satellite television, Hi-Vision audio (MUSE Hi-Vision broadcasts only) - Digital television
Block cipher	 Input data Block encryption Encrypted data Key (Ks) The input stream is divided into blocks (e.g. 64 bits) and encrypted accordingly.	Processing speed: High-speed processing difficult for a highly secure system. Security: A difference in 1 bit in the input stream usually generates a change in many bits.	- Data encryption in communications - Digital television

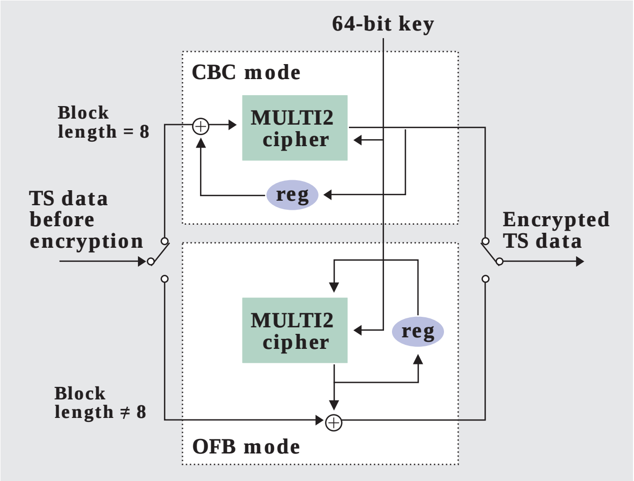


Figure 2: Example of a scrambling system for digital broadcasts

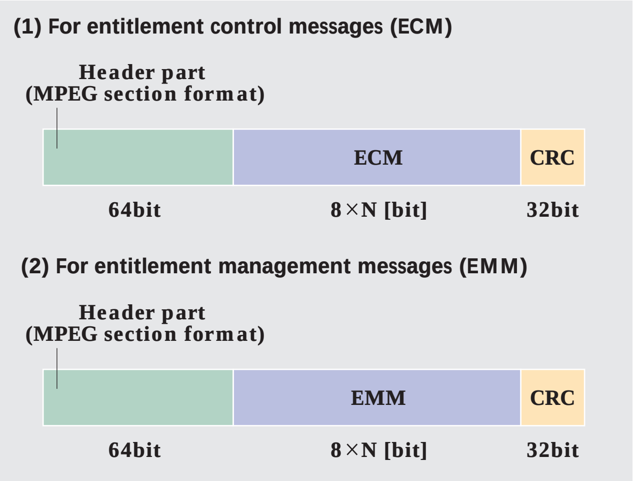


Figure 3: Example of signal configurations for sending ECM and EMM

targeted for scrambling that exceed an integer multiple of the block length in the block cipher). The system has also been introduced in Japanese digital broadcasting via Broadcasting Satellite (BS) and terrestrial waves.

4. Key configuration and transmission of key information

In signal scrambling, a scrambling key (Ks) determines the scrambling pattern, and it is common to change this key at fixed intervals of time such as every second to maintain a secure system. This Ks information must therefore be continuously transmitted to the subscriber's receiver, and this is done by encrypting and transmitting it within related information called entitlement control messages (ECM) together with the scrambled broadcast signal.

ECMs include program attribute information for determining whether a subscriber is entitled to view a program on the basis of his or her subscription. To prevent the ECM that includes the Ks from being understood by a third party, it is encrypted before transmission by using a work key (Kw) that is also updated typically on a monthly or yearly basis. This work key is sent to the receiver through related information called entitlement management messages (EMM) together with subscription contents that are sent with subscription updates.

Besides broadcast waves, other physical media like telephone lines or IC cards (smart cards) may be used to transmit EMMs. On transmission, the EMM is also encrypted by a master key (Km) unique to each receiver. This means that security for master keys must be commonly managed among different broadcast operators that use the same type of receiver. This can normally be accomplished by setting up an organization for uniform key management.

A system using the MPEG multiplexing system sends out ECMs and EMMs using signal configurations like the ones shown in Fig. 3. (Note: Packet identifier (PID) values of the packets used to send these ECM and EMM sections are included in the Program Map Table (PMT) and Conditional Access Table (CAT), respectively.) Here, specific ECM and EMM contents can be specified according to business format, billing system, etc., enabling a variety of conditional access systems to be implemented.

The Association of Radio Industries and Businesses (ARIB) has standardized the Japanese system for transmitting ECMs and EMMs and the information needed to receive and process these messages. These standards allow operators to decide on contents, encryption systems, etc. The conditional access system, moreover, includes a function for sending individual information to each receiver within a broadcast system that targets an unspecified number of the general public. This function can therefore be used to send different messages to different receivers.

5. Configuration of a conditional access receiver

A conditional access receiver consists of a section that descrambles the scrambled signal and a section that processes related control information like ECMs and EMMs. Figure 4 shows the three possible configurations of the conditional access receiver. Configuration A integrates the signal-descrambling section and related-information-processing section in the receiver unit. Configuration B, on the other hand, includes the signal-descrambling section in the receiver unit but implements the related-information-processing section in a removable security module. Configuration C makes both the signal-descrambling section and related-information-processing section removable.

To deal with threats to security, changes to the billing system, etc., configuration A requires that the entire receiver be repaired or replaced. Configuration B, in

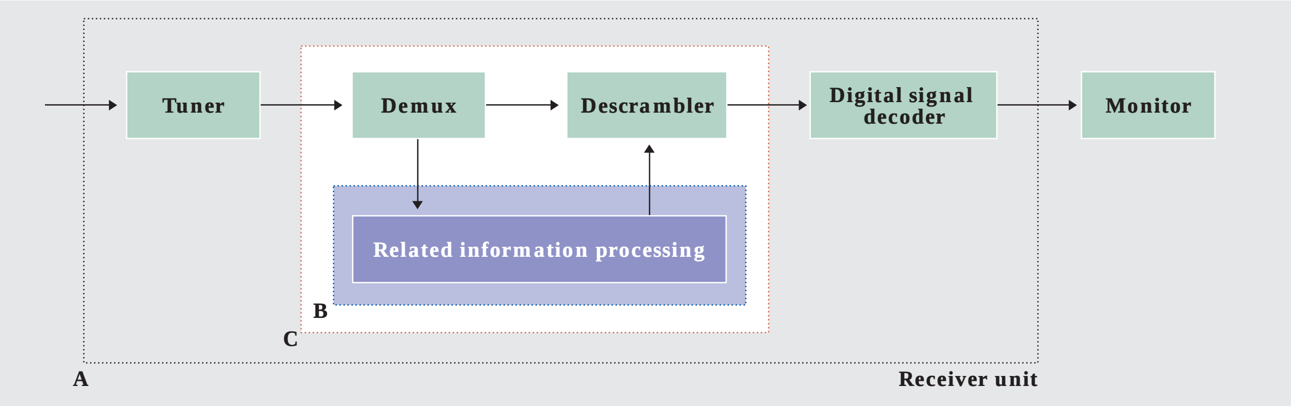


Figure 4: Conditional access receiver configurations and interface comparison

contrast, can deal with such occurrences by simply replacing the security module, which can be implemented in the form of a smart card with a built-in processor. This smart card approach has recently been adopted in many systems, including BskyB in Europe, DirecTV in the United States, and the CS and BS digital broadcasting systems in Japan. Configuration B does not allow changes to be made to the signal descrambling scheme, whereas configuration C allows even the descrambling algorithm to be updated, enabling system security to be improved all the more. With regard to module interface signals for conditional access (CA), configuration B requires them only for the section concerned with related information, for which low-speed exchange of these signals would be acceptable. In contrast, configuration C requires, for example, an interface for an MPEG transport stream using high-speed signals.

The low-speed CA interface of configuration B has been standardized in Japanese CS digital television broadcasts. The interface of configuration C has been standardized in the European DVB system, since various security modules with different interfaces have already been deployed and a uniform interface under configuration B is not possible. Japanese CS digital broadcasting has also initiated a conditional access system in which reception can be prevented by simply replacing the smart card. For CS digital broadcasting in which the receiver simply receives signals, a system has been standardized that allows a CA processing program to be downloaded by using a radio signal sent to the receiver. As for Japanese BS digital broadcasting, configuration B was standardized for the launch of this form of broadcasting in 2000. The CA interface of configuration C, however, features high security and extendibility, and studies continue on its use in future receivers providing diversified broadcast services.

(Dr. Seiichi Namba)

References

(1) ITU-R Rec. BT.810 : Conditional-access broadcasting systems (1992.9)

(2) ISO/IEC 13818-1:2000, "Information Technology-Generic Coding of Moving pictures and Associated Audio Information-Part1: Systems"

(3) W.G. Mooji : Conditional access systems for digital television, International Broadcasting Convention, IEE Conference Publications, No. 397, pp. 489-491 (1994.9)