Encipherment and Conditional Access

By Louis Claude Guillou and Jean-Luc Giachetti

This article discusses modeling conditional access in any television environment (terrestrial broadcasting, cable, and satellite). After conditional access has been defined, two models are presented that correspond to two different systems, widespread in Europe:

- *Distribution of control words. This model is illustrated by a proprietary system of Canal-Plus, used by about 3.5 million subscribers in France. This proprietary system is known as Discret 1.*
- *Distribution of authorizations. This model is illustrated by an open system used by about 1 million receivers throughout Europe: Kinnevik (500,000); FilmNet (250,000); France Telecom (60,000); Canal-Plus (60,000); Polycom; Maxat; KabelKanal, and others. Known as Eurocrypt, this open system is standardized by CEN/CENELEC (Eurocrypt, EN 50 094:1992).*

The emergence of digital signals technically facilitates the design of open systems, and the use of strong cryptography becomes justified. The encipherment techniques appear at three different levels: for managing entitlements (updating authorization keys and distributing access rights); for checking entitlements; and for scrambling program components. This modelization emphasizes the impact of standardization and the reserve for further evolution. The knowledge gained from existing systems allows the determination of the axes for additional developments, specifically in relation to digital television.

Terrestrial television broadcasting is a limited resource. Consequently, several technologies aim at developing alternate resources (cable networks and direct broadcasting satellites) and increasing the possibilities of the existing resources (e.g., by digitalizing and compressing mobile pictures).

More and more operators are offering an increasing number of television programs. The traditional sources of income (advertisements and TV taxes) are no longer sufficient to ensure program production. Pay TV is today a major component of the audiovisual landscape. Conditional access, for pay TV as well as for other professional purposes, makes use of encipherment techniques. This article proposes models for conditional access systems.

An unedited version of this article originally appeared in *ITU/SMPTE Tutorial Digital Terrestrial Television Broadcasting (DTTB)*, published 1994, SMPTE. Louis Claude Guillou and Jean-Luc Giachetti are with CCETT, Cesson Sévigné, France.

Definition of the Subject

In order to focus the subject, the article first considers two related aspects: some solutions specific to cable networks and the component scrambling techniques. The control words are introduced by their roles, so as to later introduce the modeling of conditional access systems.

Some Implementations Dedicated to Cables

Some conditional access implementations are dedicated to cable networks.

- The user connected to a cable receives [part of] the signal propagated through the cable, while the same signal is not accessible to somebody not connected to the cable.
- The physical connection may be improved by black boxes where filters select bands in the signal carried by the cable, thus limiting the access to levels of programs.
- Such a black box may include a counter for storing the accesses performed by the user, to personalize the payment. The survey of the storage in the black boxes is an essential element in the economy of the system. Various solutions have been investigated, since a channel is on the cable itself until an answering modem is automatically called by the management center. Such a black box must remain the property of the cable operator.
- At the ultimate stage of this evolution, switching facilities in the cable network allow a selective distribution of programs upon the user's requests. The counters are located in the network, the same as the telephone system. Such a solution is definitely not usable in a broadcasting environment. In all the previous particular implementations, the user is identified through his physical connection to the network. We will no longer consider those implementations dedicated to cable.

Need for Scrambling in Any Broadcasting Environment

On the terrestrial television broadcasting networks, as well as via the direct broadcasting satellites, each user receives the same signal, except for a few transmission errors. The radio waves are propagated in our domestic environment without any personal action. Because each user accesses the same signal, the program components (sound and picture, sometimes completed by various data) should be broadcast in a scrambled form. Such scrambling should be sufficiently robust to deter an attack by an intruder breaking the code of the components.

From a practical point of view, the choice of analog signal processes at a reasonable price is limited. The analog signals (NTSC, PAL, SECAM)

do not support processes that should make them resistant to piracy. The scrambling techniques should satisfy two constraints that are rather contradictory. On one hand, piracy is easier, and consequently more widespread, when the signals are badly protected, i.e., when the security of the scrambling techniques is weak. For the purposes of limiting fraud, only sophisticated scrambling techniques should apply.

On the other hand, the comfort of the user should not be affected by the successive processes of scrambling (centralized at the transmitting station) and descrambling (performed in each decoder, in the user's domestic environment). As soon as sophistication appears, the degradation due to the successive scrambling and descrambling operations on analog signals is no longer acceptable to the user. To ensure the user's comfort with decoders of limited cost, only elementary scrambling techniques should be used. (*Note*: This is a good solution where sound channels are switched at variable times. However, such a solution is only applicable when several sound channels are associated to the same program.)

Let us take as an example the first system used by Canal-Plus in France.

- The spectrum of the sound signal is reversed. The sound processing has no key at all.
- Each line of the picture is affected by a variable delay selected in a set of three possible values: {+d, 0, -d}. The selection of the delay for each line is determined by an automaton initialized by 12 bits chosen from 16 bits that constitute a control word valid for one month. The systematic search for 16 bits every month is not an important work factor for a pirate; the very low entropy of the control word is the major cause of piracy in the case of Discret 1.

For reducing the life of the control words to a typical period of approximately 10 sec, additional data have to be multiplexed with the broadcast signal, which consists of the scrambled components of the program. However, the geographical zones where the plain program is correctly received are no longer the same as the zones where the controlled program is correctly received. The propagation of digital signals for control is very sensitive to defaults that do not affect the analog signals for the sound and picture.

Let us, however, stress that the decrease in the lifetime of the control words and the increase of the length in bits of the control words should not tremendously modify the global security of a system based on all analog components because the attacks of the scrambled components remain practical.

The emergence of the MAC family coding modifies the situation.

- The picture is coded as two separate components: luminance and chrominance are successively transmitted with two different compression factors. In the decoders, digital processing is required to recover the picture. Consequently, descrambling each line by a cut-and-rotate process is obtained for very little additional cost in the decoders. The address of each cut point is a word of 8 bits produced by an automaton present in the encoder as well as in each decoder.
- The sound is coded and transmitted as a string of bits. The scrambling is ensured by an elementary operation: the string of bits coding the sound is combined exclusive-or with another string of bits representing a string of concealing bits.
- Additional data are multiplexed with the digital sound signal at a marginal cost. Some data are used for maintaining the synchronization between the transmitting station and the decoders; others are used for transmitting the cryptograms of the control words. Sound data and control data are sensitive to the same defaults; the reception zones of the plain programs are exactly the same as the reception zones of the controlled programs.

Finally, the introduction of digital TV will allow the use of strong scrambling methods, easy to implement and inducing no degradation of the signals (Fig. 1). The fastest and easiest way to scramble digital data is to exclusive-or these data with a string of concealing bits. Such a string of bits is generally produced by a pseudorandom binary sequence (PRBS) generator. PRBS generators are cryptographic algorithms having the following characteristics:

- The correlation of the output bits must be very low over a very long period.
- The correlation of two sequences from two different initializations must be very low.
- Knowing a part of a pseudorandom sequence must not reveal the initializing data.

Location of the Scrambling Operation

In all the existing access control systems, the broadcaster achieves the scrambling operation at the multiplex level. Each program provider gives the broadcaster one or more plain sources, and the broadcaster is responsible for scrambling them. Alternately, the program providers may scramble at the source level. Scrambling at the source level can be done only if the source coding allows insertion of control data. The multiplexer is then transparent and multiplexes the sources without any scrambling action.

All the existing systems scramble at the multiplex level, and not at the source level. Indeed, scrambling at the source level has the following drawbacks:

- Each source needs to have its own signaling and synchronization words to synchronize the scramblers and descramblers.
- The zapping time will be long and incompressible.
- The decoder needs several descramblers: one per program component.

Scrambling at the multiplex level allows the programs to share signaling and synchronization.

Role of the Control Words

When recovered by deciphering, the control words are used by the decoders for initializing the automata producing the sequences required for descrambling the picture (for each line, a cut point is selected among 256 possible points) and the sound (with the content of each packet of sound information, a string of scrambling bytes of the same length is combined by exclusive-or). The brute attack of the scrambled components

is not very economical, especially for the sound.

The same control word is used in a similar manner at the transmitter level for the scrambling operations and at the level of each decoder for the descrambling operations. Access to the program is therefore reduced to the access to the control words for keying the descrambling operations in the decoders. The remaining part of this article deals exclusively with the method of recovering those control words and of managing the audience so as to minimize the constraints for the user, the cost of the management system, and of fraud.

The evolution is not necessarily from simple to complex solutions. The economical optimizations are rather linked to the general availability of technology, specifically integrated circuits.

Model with Distribution of Control Words

Figure 2 shows the model currently used in France by Canal-Plus, which is moving to alternate solutions. Each month, each user receives a personalized mailing that provides a digital code to be pressed on the keypad of the decoder to key it for the next month. From the string of characters pressed by the user on the keypad, a security microcomputer buried in the decoder recovers a word of 16 bits. This word is the control word previously defined.

The string of keys pressed on the key pad represents a cryptogram of the control word. Indeed, each decoder is personalized by a diversified distribution key, i.e., a key varying from one decoder to another and obtained by enciphering the serial number of the decoder under a secret master key. The security microcomputer uses the distribution key and a cryptographic algorithm for deciphering the cryptogram and consequently, for recovering the control word. This algorithm is secret.

Let us stress some consequences at the system level:

- The physical security of the decoders is essential in the global security of the system. Each decoder is registered and has a unique identification number. The decoders are the property of the system manager. The manufacturing and the maintenance of the decoders shall be controlled. Such a decoder cannot be integrated in a TV set.
- Such a decoder is dedicated to a given service; it cannot be shared by several services. If independent services are developed with such a proprietary solution, the user shall have several decoders, which is unacceptable from the ergonomic point of view.
- The decoders are leased together with the subscription to the service. A user's file stores the correspondence between users and decoders. The user's file has to be updated each time a decoder fails and has to be replaced.
- The monthly codes are limited to the number of characters the user is ready to press. Other means may be considered for entering the monthly code: bar codes, magnetic tickets, etc., but that is not compatible with the constraint on the cost of the decoder.

In one word, such a system shall be proprietary. Such specifications are also not directly usable by any other potential challenger in the pay-TV business.

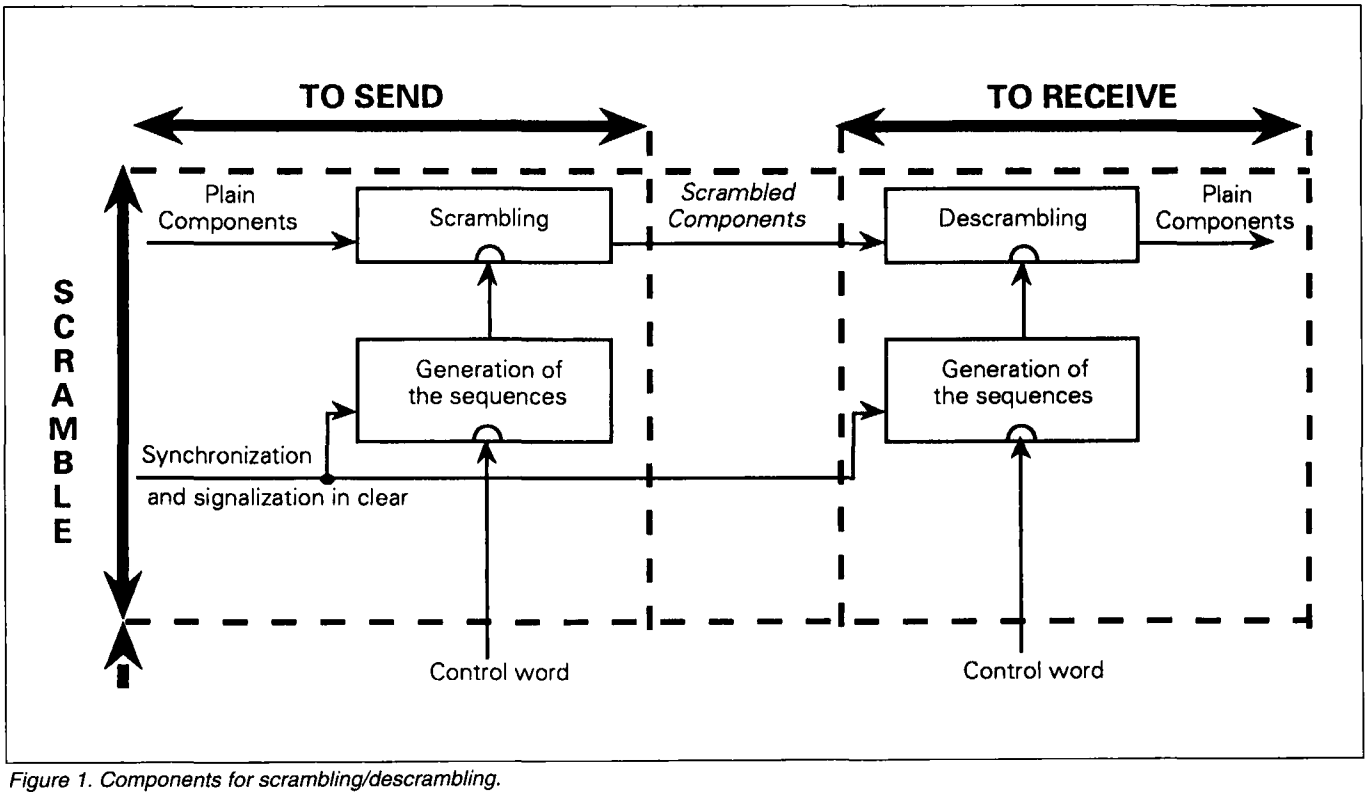

Figure 1. Components for scrambling/descrambling.

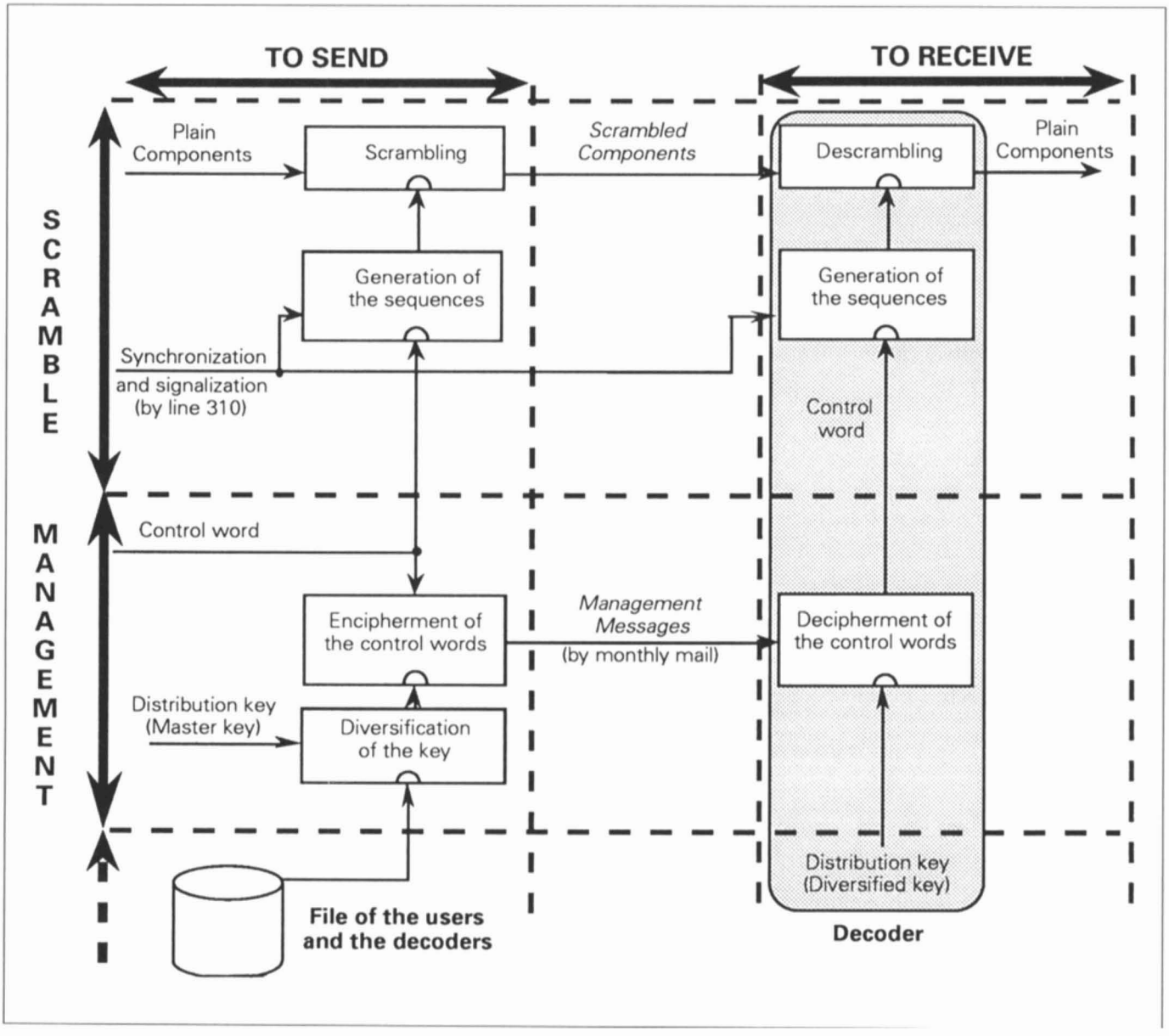

Figure 2. Model with distribution of control words.

There is a kind of homogeneity in the product specified and used by Canal-Plus — the physical security of the decoder is consistent with the resistance of the scrambling techniques. There is no reason to place a secure lock on an easily by-passed door. The limited resistance of the decoder has induced a legal statement outlawing the use of the pirate boxes and, consequently, the manufacturing and the distribution of such boxes.

Despite very limited resistance, those specifications have led a pay-TV channel to birth and to growth while earning a large amount of money.

Model with Distribution of Authorizations

When the broadcast signals include a synchronization indication such as a frame counter, that indication may well be used for producing the control words. A one-way function, easy to compute but difficult to invert, generates the control words. One of the arguments of the function is a "basic" authorization key. The wording "basic authorization key" means that at a given moment, on a given service, all the daughter cards use the same unique authorization key.

The UER/EBU specifications take such a possibility into account. A new control word is produced for every block of 256 frames (approximately every 10 sec) from the 20 most significant bits of the frame counter transmitted in the line 625.

The previous possibility should not be confused with the local control word, which is fixed over a long period and managed manually by the operator. The UER/EBU specifications allow a local control word. While providing an extra free limitation of 1.5 dB of cross-picture between adjacent channels, the systematic scrambling under control of a

default value of the local control word is not mandatory.

When the system has a sufficient resource for broadcasting service messages at a marginal cost inside the multiplex, then the control words may advantageously be picked at random by the transmitter.

- The control words are converted into cryptograms by a cryptographic algorithm controlled by a basic authorization key.
- The cryptograms are transmitted in the broadcast signal. The service messages are the entitlement control messages (ECMs).
- At the level of each decoder, the control words are recovered from the ECMs by a cryptographic algorithm using the same basic authorization key. Security microcomputers are storing the authorization keys and the algorithms. They represent the entitlements of the users.

The result, illustrated in Fig. 3, is very close to the scheme standardized by the UER/EBU for the D-2-Mac packet signals. The control words (CWs), are long in bits (typically 60 bits) and short in life span (typically 10 sec).

The entitlements of the users should preferably be managed and stored in security microcomputers. For management operations, the device shall recognize the "voice of its master." The microcomputer uses a distribution key for checking the entitlement management messages (EMMs). The distribution keys are typically diversified, i.e., varying from one device to another, as a cryptogram of the unique address under the control of a master distribution key. If the check is positive, i.e., if the message authentication checksum is correct, then the microcomputer, being convinced of the authenticity of the message, executes the management operation.

The management operation results in distributing access rights and/or updating keys. The authorization keys have indeed to be modified from time to time, for security reasons. They may be updated by EMMs conveying cryptograms.

The number of bits by user may be reduced by sending EMMs valid for several users who form a group. Such

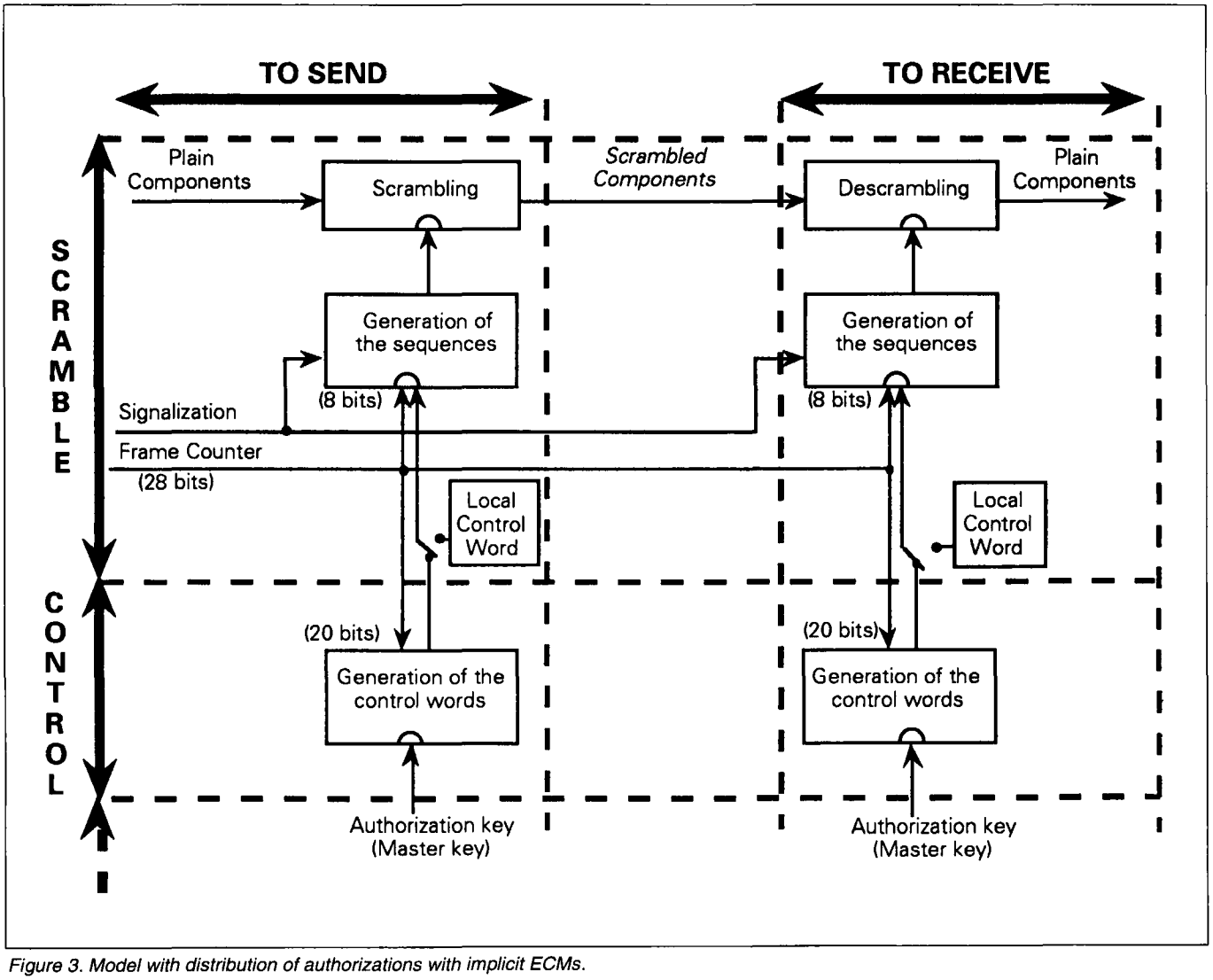

Figure 3. Model with distribution of authorizations with implicit ECMs.

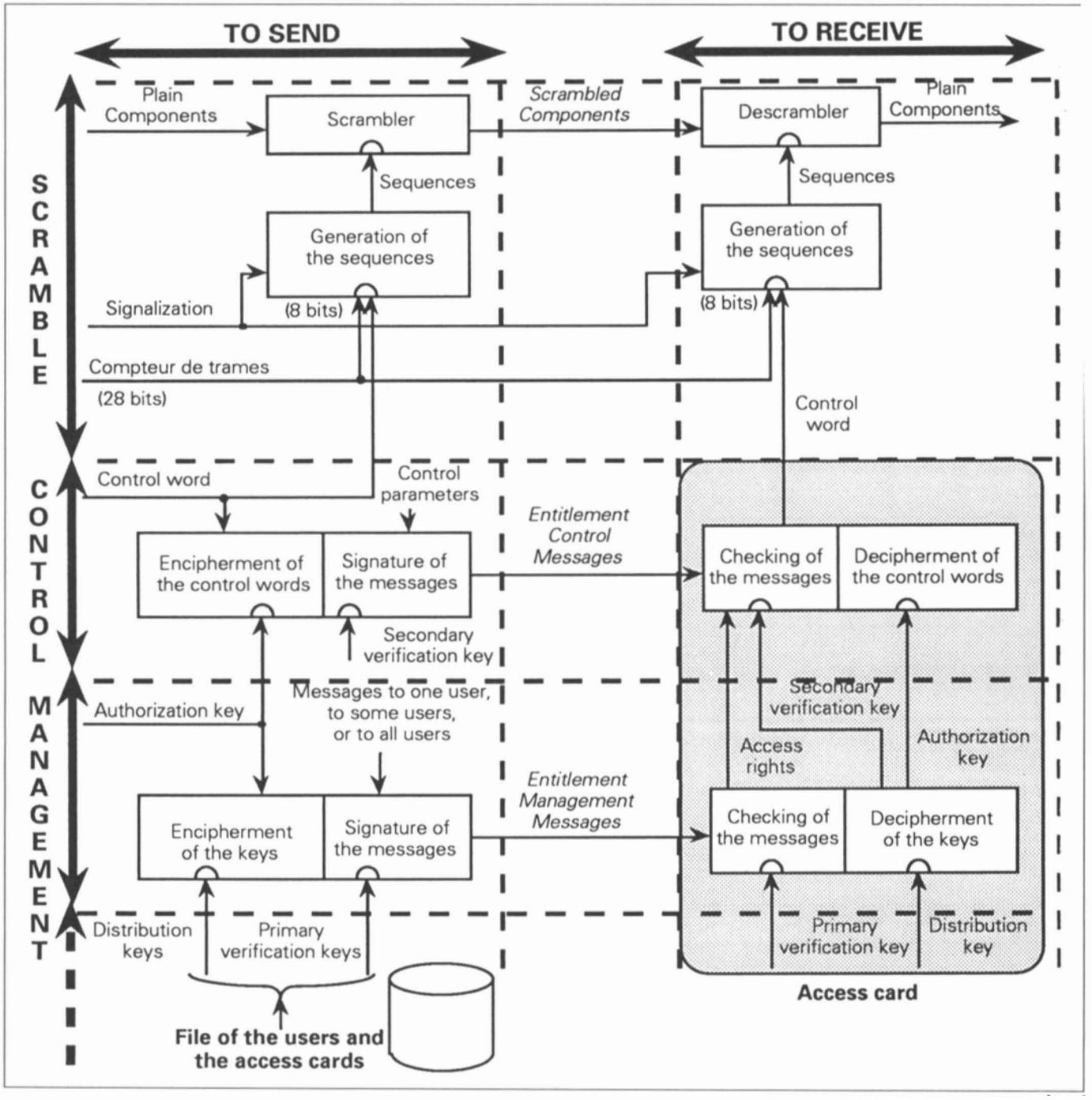

Figure 4. Model with distribution of authorizations.

a group of users must share the same diversified distribution key, which varies from one group of devices to another group of devices, as the cryptogram of the group address under control of another master distribution key.

Consequently, there are currently three categories of EMMs.

- Each EMM-U is intended for a unique user in the system.
- Each EMM-S is intended for a group of users in the system.
- Each EMM-G is intended for all the users in the system.

When the control word is long enough in bits and short enough in life, the security microcomputer may be detachable. In Fig. 4, the security microcomputer connected to the user's decoder is implemented as an access card.

For computing ECMs and EMMs, the service operator uses other types of security microcomputers. The major security modules essentially differ from the minor security modules. When implemented as smart cards, the major and minor security modules are currently referred to as

mother cards and daughter cards, respectively.

The next scheme is an answer to question 23/CMTT, newly revised as question 103 by Working Party 9 of ITU-T. That question aims at ensuring privacy and conditional access in long-distance international transmission of digital television, on the basis of the 34 to 45 Mbit/sec system (Rec. 723). The response to that question should allow the UER/EBU to protect the signals exchanged between its members. That scheme takes into account all the particularities of the UER/EBU application.

Some details are completely clarified when comparing Fig. 5 with Fig. 4. Figure 5 shows the categories of EMMs and the types of security devices used by the service operator. By reducing danger to the reporter, the remote control is a very practical option when reporting news from a mobile satellite station. All the major security modules may thus be kept in a secure environment, for example, at the UER/EBU premises in Geneva.

Entitlement: Either a Key or a Right to Use a Key

What is an entitlement? Two statements have been extensively debated at the UER/EBU.

1. All the users having the same authorization key have the same right. While very simple to understand, this statement complicates the management. To modify the right of a single user, the authorization key has to be replaced. The management of an element implies the management of the whole audience. When the change of the authorization key is done over the air, the new key is eventually distributed to pirates who should use clones of an original device and who continue to pay for the original device. The security of such a system is not improved by frequently changing the authorization key. The confusion between the management of the authorization keys and of the entitlements induces a totalitarianism in the management of the system. Any modification of the audience implies the whole audience.

2. An entitlement is defined by conditions limiting the right to use an authorization key. Those conditions are managed by the card, on a personalized basis. More complex at the first sight than the previous statement, the second statement simplifies the management of the system.To modify the entitlements of a user, it suffices to alter the conditions associated with the relevant authorization key in the security device of the specific user. The remaining part of the audience is unaffected by such personalized management.

The over-air addressing is mainly used for managing the conditions associated to the authorization keys in the security devices of the users. Examples of conditions are a subscription period, a pre-booked program, a credit for impulse accesses, etc.

This second statement induces the following analysis.

- On one hand, the management of entitlements is partly a problem of secrecy in keying the security device. The key management is essentially a management of secrets. The standardization of a universal solution for key management is unrealistic, due to the political problems arising from secrecy.
- On the other hand, the management of entitlements associated with an authorization key is a problem of integrity and authenticity, where the security device has to recognize the "voice of its master." The management of entitlements does not necessarily imply privacy or secrecy. The standardization of techniques for secure messaging is realistic. Those techniques should allow the restriction of the cryptographic capabilities of the security devices.

Security Device: Either Buried or Detachable

The security device must remain the property of the system manager. When using an image, we say that it recognizes the voice of its master; this means that it shall execute the commands of its master and not the wishes of its user. Any solution shall imply devices with a minimum of tamper resistance.

If the security device is buried in the decoder, then the decoder itself must remain the property of the system manager. We have already considered the consequences of such a choice for the manufacturing, the distribution, and the maintenance of the decoders. The same decoder cannot have two different masters at the same time. Consequently, multiplication of pay-TV operators should result in multiplication of the decoders connected to the user TV set.

If the security device is detachable, then the decoders may be rendered commonplace. The manufacturing, distribution, and maintenance are free, and the devices may be integrated into some TV sets. As a consequence, a set of standards on the transmission of the ECMs, EMMs, and the interface between the decoder and the security device shall be established.

What is the best solution: to describe a cryptographic algorithm without knowing on which microcomputer it will be executed; or to describe an interface with a security device without having to fix a cryptographic algorithm and without having to specify all the conditions on the use of the authorization keys?

The potential evolution of the solutions is an essential aspect to be considered when establishing the basic specifications. The detachable security devices allow free evolution of the cryptographic algorithm, free evolution of the commercialization of the audiovisual services, and free use of the up-to-date silicon technology.

Smart Cards

The model of conditional access with distribution of authorizations using a smart card was designed and developed by CCETT before the existence of Canal-Plus and before any action of ISO and UER/EBU on conditional access. In the proceedings of a symposium held in Liège (Belgium) on November 24, 1980, a paper by Louis Guillou introduced pay techniques for a teletext service (Radiodiffusion à péage pour le télétexte ANTIOPE). The PC0 card had been designed at this time.

Professional information on the stock exchange is currently broadcast in real time in France using this method and the smart cards designed in 1979. The control words consist of

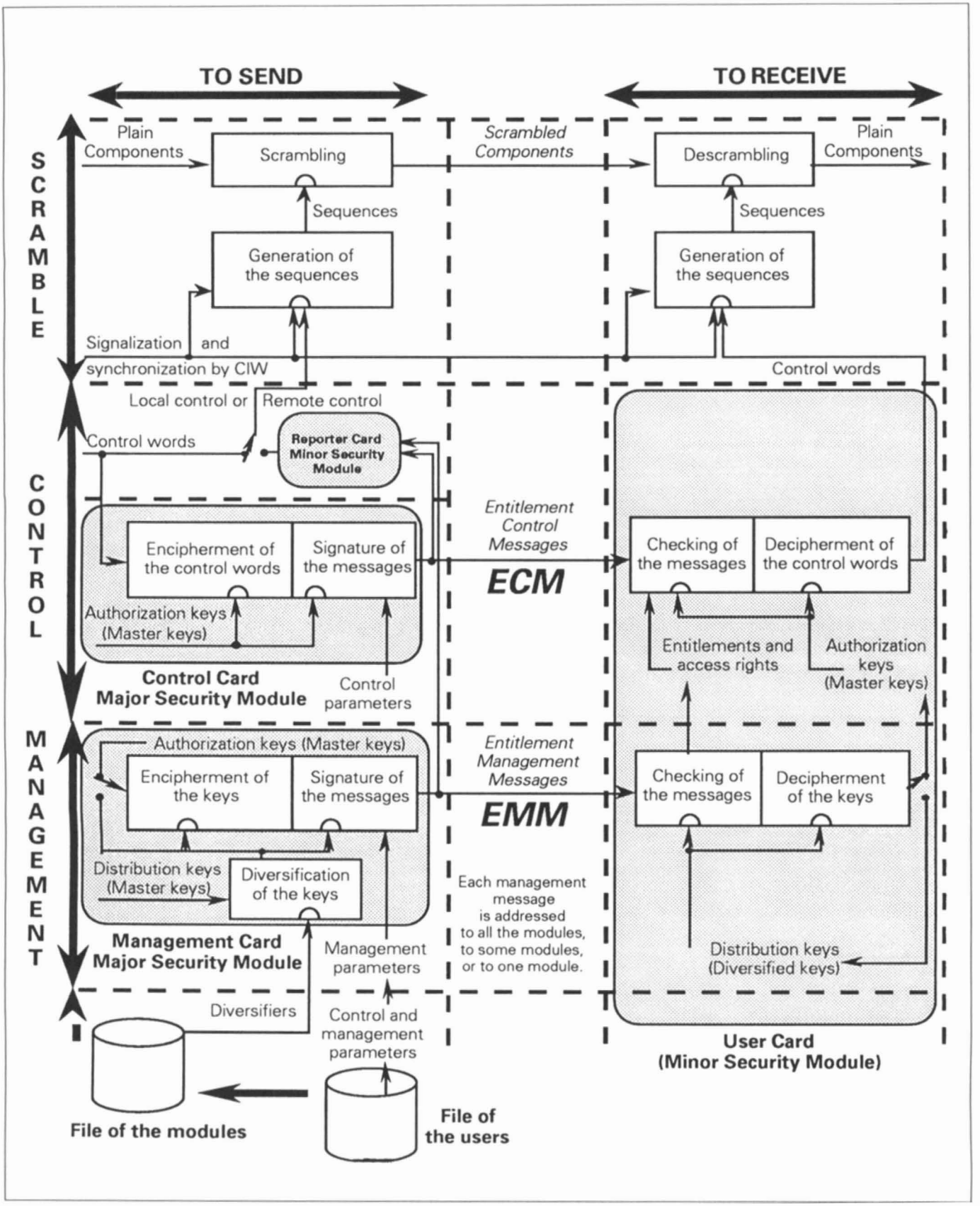

Figure 5. Model proposed by CMTT/1 as an answer to question 23.

strings of 60 bits and have a life span of 20 sec. The management is based on a monthly subscription. However, an efficient transposition for TV programs was accomplished only 10 years later, on the D-2-Mac Packet signals. Eurocrypt and the PC2 card have been deeply influenced by the work done previously on ANTIOPE and the PC0 card.

The International Organization for Standardization (ISO) and the International Electrotechnical Committee (IEC) are standardizing the interface of the integrated circuit cards with contacts in a series of standards referenced as ISO/IEC 7816. The interface between the Eurocrypt decoders and the PC2 smart cards respect those specifications.

- *1987, Physical Characteristics,* ISO 7816/1
- *1988, Dimensions and Locations of Contacts,* ISO 7816/2
- *1989, Electrical Signals and Transmission Protocols,* ISO/IEC 7816/3

(*Note*: The microcomputers especially designed for smart cards are good candidates as security devices, either as buried devices or as detachable devices.)

. In the systems using smart cards, several categories of cards appear.

- The program operators use control mother cards for constructing the ECMs intended for conveying access criteria and cryptograms of control words.
- The management servers use management mother cards for constructing the EMMs intended for conveying keys and entitlements.
- The users use daughter cards for recovering control words and for storing keys and entitlements.

In Eurocrypt, a message to be submitted to the daughter PC2 cards for any control or management operation is structured as a string of consecutive data objects coded in TLV (Tag-Length-Value).

- The first objects specify the receiving entity: all the cards, a group of cards, or a unique card. They also specify the goal of the operation: ECM for distributing control words, EMM for distributing a distribution key, EMM for distributing entitlements, etc. When a message is sent to a group of cards, a binary indication is provided for each card of the group.
- Subsequent objects convey access criteria, entitlements, and cryptograms.
- The last object conveys a cryptographic checksum covering [part of] the message, more precisely all the sensitive information in the message.

Before taking any further action, the card checks the cryptographic checksum. When the checksum is invalid, the card stops. It can be reactivated by a further reset. From a practical point of view, when receiving a message taken at random, the PC2 card looks like a function null. The density of the messages, followed by a result, is approximately one message over 264 strings of bytes picked at random.

In the PC2 cards, the keys used for the ECMs are distinct from the keys used for the EMMs.

Moreover, the same PC2 cards may be given to different service providers without any interference at security level. The same PC2 card may store several bunches of keys owned by different service providers without any interference between the secrets and the entitlements of those service providers. The architecture of the PC2 cards consists of a master file (MF) and one or more dedicated files (DF). The card ensures the insulation at the dedicated files and between the master file and the dedicated files. In the relevant committee of ISO/IEC, those problems are presently being standardized in part 4 of ISO/IEC 7816. The knowledge obtained from PC2 is very useful.

Evolution of Cards and Decoders

The problems associated with Pay TV are now felt worldwide. The diversity of the present solutions is a demonstration of vitality. We should focus instead on the various possible evolutions.

The debate between buried and detachable security devices is not ended.

- There is room enough for a buried security device along with a detachable security device. The parts of the two devices should be clarified. The expansion of fraud is not the only justification. A buried security device allows additional methods of commercialization.
- The solution chosen by video crypt includes two security devices. Upon request from the TV operator, the buried device has to authenticate the detachable device.

The simultaneous use of two security devices (one buried and the other detachable) certainly allows better control of the fraud evolution by complicating the work of pirates. However, it also allows an authority who has developed decoders for his own use to control the use of his decoders by other operators, so as to avoid the openness of the system.

The use of accreditations, zero-knowledge techniques, and public keys has been evaluated for such services. The accreditation is a signature of the identity of the detachable device; it is provided by the card issuer according to a public key technique. The card may prove by a "zero-knowledge" technique that it knows the signature of its identity without revealing anything upon the exact value of that signature. The verifier uses only the public key of the card issuer. Zero-knowledge techniques are the ultimate stage of evolution in public key techniques.

Zero-knowledge techniques have an impact on the evolution of the cards. In the future, cards may thus be issued by one or several organizations recognized by the service operators.

- The role of such an organization is the harmonization of the standardization, the maintenance of the technical specifications, and the conformance testing of the cards proposed by the manufacturers. Examples of such an organization are a regional authority or a Federal Reserve bank.
- Later on the cards may be freely sold in the general stores to potential users under closed protection. By delegation of the authority, one or more service operators create one or more DFs in the card for nesting their bunches of keys and the entitlements of the users.

The descrambler itself may become semidetachable. In the European digital video broadcasting (DVB) project, several research centers are considering the impact of a mandatory PCM-CIA slot on the TV sets. Inside the PCM-CIA card, the same chip of silicon could implement the descrambler and the buried security device. The PCM-CIA card should itself be an interface device for the smart card.