RC 20567 (10/01/96)
Security of Digital Video Distribution

# IBM Research Report

## On the security of Digital Video Distribution Systems

Abdelnaser Adas
Department of Electrical Engineering
Georgia Institute of Technology
Atlanta, GA 30332

Ahmed Tantawy
IBM Research Division
T.J. Watson Research Center
Yorktown Heights, New York

Tri Tran
Department of Electrical Engineering and Computer Science
Massachusetts Institute of Technology
Cambridge, MA 02139



Research Division
Almaden · T.J. Watson · Tokyo · Zurich

# On the Security of Digital Video Distribution Systems

*Abdelnaser Adas**
Department of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, GA 30332

*Ahmed N. Tantawy*
IBM Thomas J. Watson Research Center
Yorktown Heights, NY 10598

*Tri Tran**
Department of Electrical Engineering and Computer Science
Massachusetts Institute of Technology
Cambridge, MA 02139

**Abstract**

This paper discusses issues related to security in digital video distribution systems. Topics of examination include private, public, and hybrid key cryptosystems used for data encryption and decryption. Work done by standarization bodies such as MPEG, DAVIC, and DVB is also summarized. Relevant practical issues regarding the conditional access system for a typical broadcast TV system and other products available in the industry are highlighted.

*This work was done while at IBM Thomas J. Watson Research Center, Yorktown Heights, New York

# 1 Introduction

In recent years digital information has become one of the most important assets in the society. With the advent of broadband and public high speed networks, the information superhighway that is designed to carry all forms of digital information (Voice, Video, data, ...etc) became closer to reality. The security of this information is of major concern. Wide availability of precious information and its accessibility via networks will be limited unless the intellectual property and the privacy of the parties involved are protected.

The need for security is evident and it is hardly necessary to stress the importance of data encryption, a procedure that limits the usefullness of data to intended parties only. Problems arising from lack of security include the credit card fraud, which leads to a loss of about $3.5 billion/year, the cellular telephony fraud which costs approximately $1 billion/year, and the large losses incured by cable operators and content providers due to cable box cloning and theft of services.

The future of digital video systems is also at risk of similar security failures. Such video distribution systems are implemented to operate on Cable TV (CATV), Cellular TV, Telco, and closed circuit pay-per-view systems. Obviously, since digital information is sent from servers and CATV head-ends to the users over an unsecured channel, its security is always an issue. However, in Telco systems which transmit video programs to users via existing copper twisted pairs used for telephone lines, encryption may not be very critical. This is because the video program is not transmitted to the subscriber until his identity is validated and moreover, transmission over a subscriber's particular copper pair is relatively secure. On the other hand, if a CATV system broadcasts the video program to a particular subscriber, the signals will reach all subscribers in the cable cell. Hence, this video program would need to be encrypted and only the intended subscriber should be allowed to decrypt the program. Any video distribution system which provides return program selection path should also consider providing security for the subscriber's requests and other billing or private information.

An example of such video distribution system is the Multimedia Information Resources Access Gateway (MIRAG) system [11]. MIRAG supports video on demand (VoD) delivery and other network services over Hybrid Fiber Coax (HFC) plants to home users. This system, which is implemented at IBM Research Division, is depicted in Figure 1. The MIRAG system or any other system that uses a broadcast network, is vulnerable to unauthorized users who can easily tap into the network. A comprehensive security system that supports the basic security services such as authentication, restricted access, confidentiality, integrity and non-repudiation is needed. Preferably, this security system should be embedded into the gateway and into the customer premises equipment [2].

Data Encryption Standard (DES), the widely used encryption and keying scheme based on symmetric (private) keys, and asymmetric (Public) key schemes like Rivest, Shamir, and Adleman (RSA) and Deffie-Hellman are among the schemes currently being investigated for their use in broadband and public networks. Symmetric key schemes can operate at higher speeds than asymmetric key schemes. In symmetric schemes, however, keys must be kept secret and authentication can not be performed. Asymmetric key schemes cannot encrypt video streams on the fly at regular video speed. Therefore, the solution for a practical security system appears to be a combination of both schemes–a hybrid approach where an asymmetric key scheme is used for key distribution and authentication while a private key scheme is used for high speed data encryption. Whichever solution is considered, it has to comply with appropriate standards and include key management, safe key storage, and non exposure of keys or information in the clear.

The rest of this report is organized as follows: Section 2 gives a quick overview of cryptology; Section 3 discusses an example of a conditional access system for broadcast TV; Section 4 discusses the work regarding security in the international standardization groups such as ISO/IEC (MPEG), Digital Video Broadcast (DVB) and the Digital Audio-Visual Council (DAVIC); Section 5 presents the current technologies in the industry, and finally Section 6 presents some conclusions.

## 2 A Quick Overview of Cryptology

Cryptology consists of two parts: cryptography and cryptanalysis. Cryptography is the science of devising secure methods for transforming clear messages, called *plaintext*, into a secretive form, called *ciphertext*. The transformation of the plaintext into ciphertext is called *encryption*. An algorithm and a key (called encryption key) are used in the transformation process. The inverse of this transformation is called *decryption* and the key used in the decryption process is called

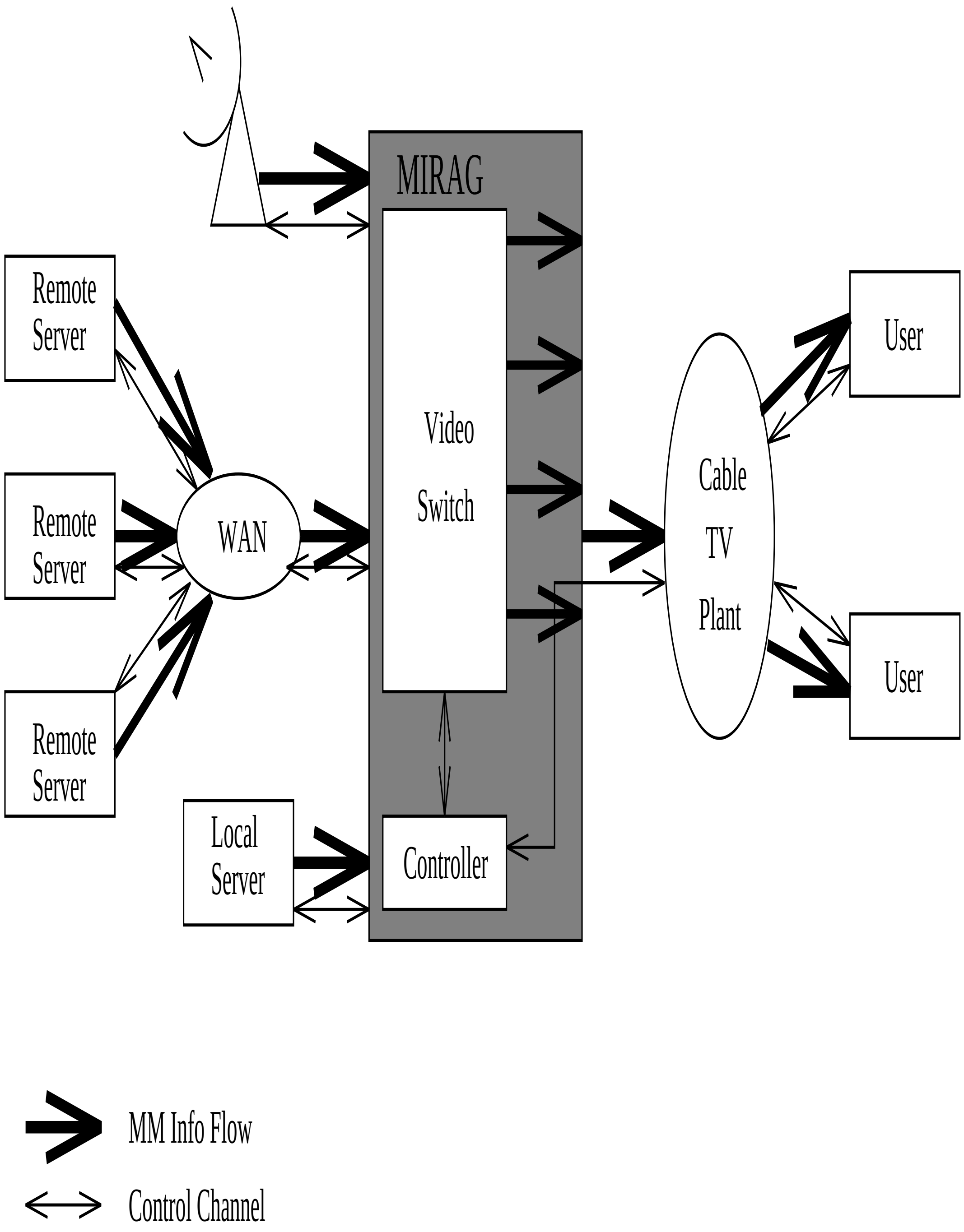


Figure 1: MIRAG as an example of a digital video distribution system

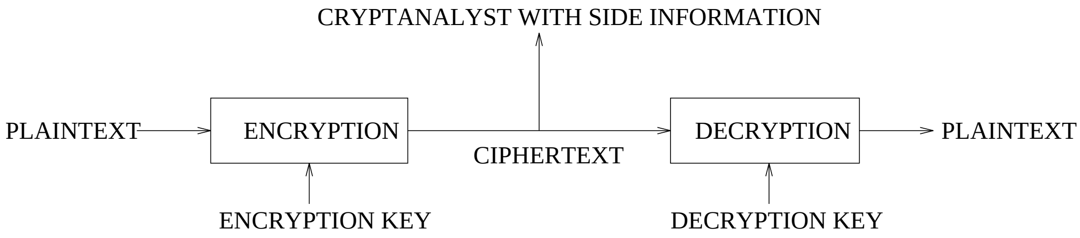


Figure 2: Cryptography

the decryption key. A system that performs the transformation and the inversion is called a *cryptosystem*. Publicly advertised algorithms are preferred over proprietary ones because they can be tested for any mathematical weaknesses. Encryption can be done at each network node in which the network operator is responsible for the key management or it can be done end-to-end, i.e., data is encrypted at the source and decrypted at the destination [2].

Cryptanalysis is the art of breaking the cryptosystem. The goal of the cryptanalyst is to determine the key(s) in order to infer the plaintext from its ciphertext [7]. This is illustrated in Figure 2.

There are two general types of crytosystems: private (symmetric) key cryptosystems and public (asymmetric) key cryptosystems.

## 2.1 Symmetric (Private) key cryptosystems

In a symmetric key cryptosystem, the algorithm and the key used to encrypt and decrypt the plaintext are the same. The algorithm used is typically a series of substitutions and permutations of the plaintext. whoever knows the key will be able to encrypt or decrypt messages. Therefore, the keys the keys must be kept secret. The most widely used symmetric key algorithm is the Data Encryption Standard (DES) [4, 6]. It has been adopted as a standard by the National Bureau of Standards in 1977. Typically, DES has a 56-bit key and views data as a string of 64-bit blocks. The algorithm takes each data block through 18 stages of data-manipulation. Sixteen of these stages are identical. They execute complex series of bit manipulation and permutations of the data block using the symmetric key. The DES algorithm transforms the 64-bit input data block into a 64-bit output cipher data block. The major weakness of DES is the size of the key. It is argued that if given a ciphertext sample and its corresponding plaintext, an expensive machine can be built to carry out an exhaustive search in a few hours to find the key. This problem can be avoided by changing the key frequently.

There are four mode of operations defined by the DES standard:

(1) Electronic Code Book (ECB): It is a direct implementation of the DES algorithm. The same plaintext always generates the same ciphertext for a given key. It is the easiest to break but it treats each data block independently, therefore it has advantage in that an error in processing one block will not affect any other subsequent blocks.

(2) Chain Block Cipher (CBC): In this mode the 64-bit input data block is EXORed with an Initial Value (IV) of 64-bit length, then the result is processed by the DES algorithm to obtain the ciphertext. The ciphertext is then used as the IV to be EXORed with the next input data block. CBC will produce different ciphertexts for the same plaintext block, thus making attacks harder. However, if an error occurs in the output block, it will extend and affect the next output block.

(3) Cipher Feedback (CFB): The input data block used is of length n-bit, $1 \leq n \leq 64$. The IV will be processed by the DES algorithm and the most significant n data bits of the result are EXORed with the input n-bit data block to obtain the ciphertext. Finally, the ciphertext is shifted into the n least significant bits of the IV register. CFB will produce different ciphertexts for the same plaintext and any error in one block will extend and affect the next output block (same as CBC).

(4) Output Feedback (OFB): It is a data independent stream cipher where the output data block is a function of only the input data block and the number of preceding blocks. The feedback is therefore data-independent and if errors occur in the output block, they will not affect the subsequent output blocks.

Another DES variation is to use multiple encryptions of the same data block (like the triple DES algorithm). The cryptosystem using this scheme is more difficult to break using exhaustive search than one using the single DES algorithm [10].

There are many other proposed and existing symmetric key algorithms like LOKI, FEAL-N, IDEA, REDOC II [10]. Some of these algorithms, like IDEA and REDOC, are known to be secure, but they are not challenged as often as the DES algorithm.

## 2.2 Asymmetric (Public) key cryptosystems

The concept of public key was introduced in 1976 by Diffie and Hellman [1]. Public key cryptosystems use keys in pairs, one key is private and the other is public. Knowing the public key, it is infeasible to generate the private key, and vice versa.

Public key cryptosystems are explained by the notion of one way functions. A function $F$, where $F : S \rightarrow T$, is a one way function if it satisfies:

1- $F(x)$ is easy to compute for all $x \in S$.

2- Given that $F(x) = y$ for some $y \in T$, it is very difficult to determine $x$.

Many public key cryptosystems have been proposed and a few of them are secure and practical. The most popular public key cryptosystem is the RSA. Other public key cryptosystems include Diffie-Helman, El-Gamal, Knapsack, etc [9].

Public key cryptosystems resolve the problems of key distribution and sender authentication that private key cryptosystems suffer from. For N users in a public key cryptosystem, only $N$ pairs of keys are required while in a private key system $\frac{N(N-1)}{2}$ keys are needed. Moreover, if user A's message is encrypted with A's private key, then this serves as a digital signature and the signature can be verified by decrypting the message using A's public key. If the message is successfully decrypted, it is safe to conclude that only user A could have sent it.

Public key cryptosystems are computationally intensive. This makes them inefficient and infeasible for bulk data (at least for the present), and, in turn, limits their use to the distribution of secret keys, digital signature, and authentication.

## 2.3 Hybrid Model

This model is suggested to combine the best features of both private and public key cryptosystems. It resolves the problems of key distribution and key management that private key systems suffer from and avoids the low speed problem of public key systems. In this approach, private key systems provide high speed encryption of exchanged data, while public key systems are used for secure and authenticated exchange of keys over unsecured communication paths. To provide enhanced security, this scheme does not require that all users establish a common key which might reveal information to an undesirable third party.

# 3 An Example Broadcast System with Conditional Access

This section describes a rather conditional access (CA) TV system developed for a BBC service targeting special interest groups. The BBC broadcasts special programs during the evening hours when normal programs are not being transmitted. The system uses a smart card based conditional access (CA) system [8].

Figure 3 shows the system architicture which includes three new components added to the head-end. These components are: subscriber management system, security computer, and an encoder. The subscriber management system handles all customer related data, the security computer performs data encryption of the data, and the encoder scrambles the video and inserts the data in the video.

## 3.1 Scrambling

The scrambling technique used is line shuffling. The scrambling of the lines themselves is performed by a permutation generator driven by a 20 bit control word (CW) generated by the security computer. The CW is transmitted with the video over the air in an encrypted form to be used by the de-scrambler at the receiver end.

## 3.2 Encryption and decryption

The information needed to derive the CW is encrypted using a proprietary algorithm developed for this purpose. The decryption process is carried out by the smart card which has a unique serial ID number. To reduce the threat of cloned cards or card emulators with different ID serial numbers, an authentication scheme based on the zero-knowledge algorithm [3] is used. In this scheme each card is signed with a function that has a secret code. The zero-knowledge algorithm is used to test

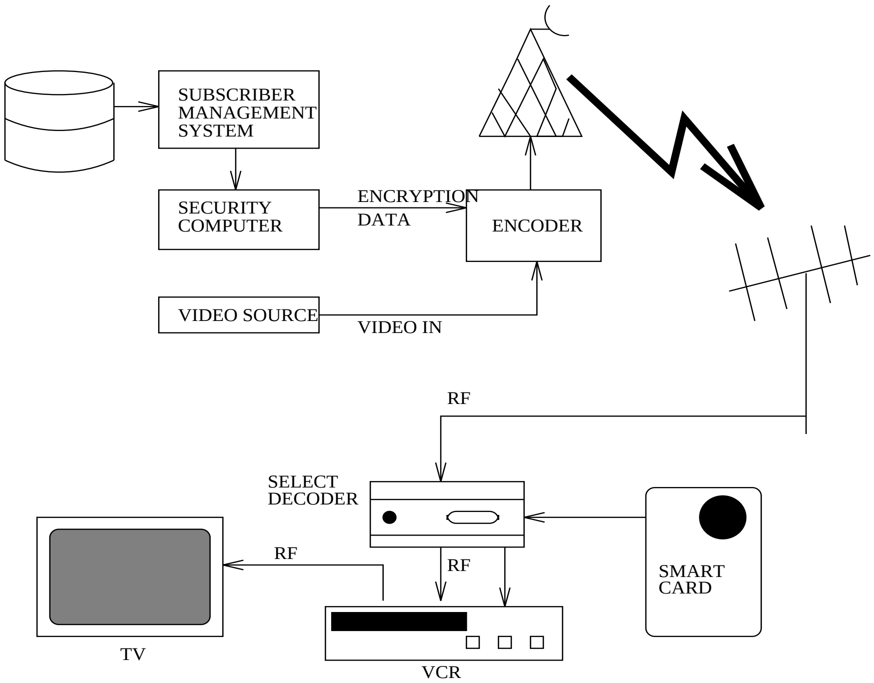


Figure 3: An example system architecture

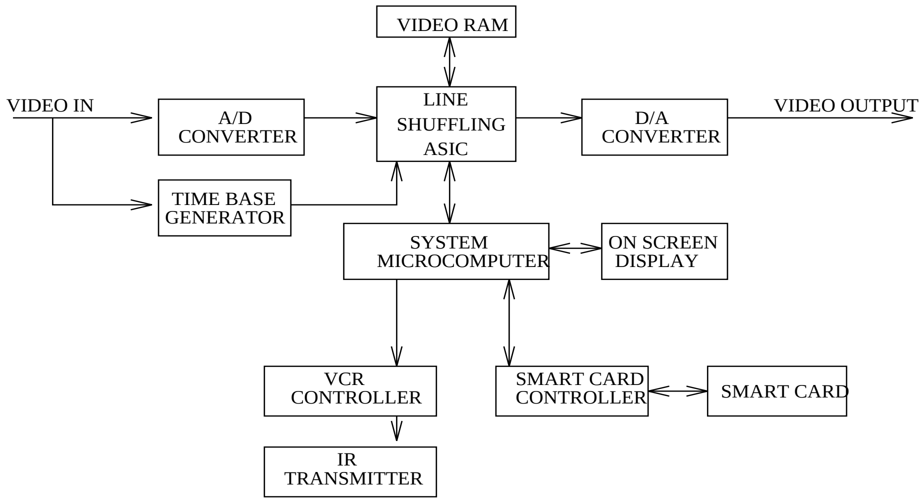


Figure 4: Decoder architecture

the authenticity of the card without the need to know the secret code. Therefore, it is very difficult to emulate cards with a new ID and has the proper signature. However, unless the secret code and ID pairs are made unknown to even the manufacturer of the smart card, the problem of cloning will still persist.

### 3.3 Decoder Architecture

Figure 4 shows the BBC decoder architecture. The main functions of the shuffling ASIC are data retrieval and permutation generation. After the conversion of the received video signal from analog to digital, the de-scrambling and de-shuffling is performed within the video RAM on the video lines. The video lines can then be read out using an address bus controlled by the permutation generator, which is initialized by the CW. The decryption process, communication with the smart card, and other security functions are done by the smart card controller.

## 4 International Standards

The International Standardization Organization (ISO), the Digital Audio-Visual Council (DAVIC), and the Digital Video Broadcast (DVB) are organizations group are concerned with the success of digital video distribution and its applications. They develop industry-wide agreements about the specifications of open interfaces and protocols that maximize inter-operability across devices, applications, and services. This section discusses the recent work done regarding conditional access (CA) and security.

## 4.1 ISO-IEC (MPEG)

ISO-IEC Moving Picture Expert Group (MPEG) is an organization responsible for the standardization of coded representation of video and audio. The MPEG committee has standadized video and audio compression. In MPEG[5], compressed video and audio is packetized into Program Elementary Stream (PES) packets. The PES packets are used to carry the elementary stream data defined by MPEG. ISO/IEC 13828-1 specifies two ways for combining the elementary streams of video, audio, and other data into streams that are suitable for transmission or storage. The two streams are: Transport and Program streams. Program streams are used in relatively error-free environments. Program stream packets may be of variable length and relatively large. Transport streams are used in an environment where errors are likely to occur such as transmission in a noisy media. The packet length is fixed to 188 bytes.

Although MPEG does not specify any conditional access mechanism, it supports scrambling of Transport or Program streams through the definition of system data streams and other specifications. We discuss below the definitions concerning the support of conditional access systems for programs encoded in the Transport stream.

Data scrambling can be done at either the PES level or the Transport stream (TS) level. PES level scrambling requires that the headers remain un scrambled and not spanning across TS packet boundaries. MPEG also requires the alignment of a PES packet load with the end of a TS packet. The header of the PES packet contains a 2-bit PES scrambling control field to indicate the scrambling mode of the PES packet payload. The values for this field are presented in Table 1.

For scrambling at the TS level, the TS packet header has a 13-bit field called the Packet ID (PID) field. The type and properties of data stored in the TS packet load are given in Program Specific Information (PSI) tables. There are four types of PSI tables:

- Program Association Table (PAT),

| Value | Description |
|---|---|
| 00 | Not scrambled |
| 01 | user defined |
| 10 | user defined |
| 11 | user defined |

Table 1: Scrambling Control Values

- Program Map Table (PMT),
- Conditional Access Table (CAT), and
- Network Information Table (NIT).

PSI tables are carried in TS packets. PID 0x0001 is reserved for the CAT table. For more specific details of these tables see [5]. The TS packet header also contains a 2-bit transport_scrambling_control field whose semantics are the same as for the PES header.

MPEG has also defined two special messages for private conditional access systems: entitlement control messages (ECM), which specify control words and other scrambling and/or control parameters and entitlement management message (EMM), which specifies the authorization levels or the services of specific decoders.

## 4.2 DAVIC

The Digital Audio-Visual Council is a non-profit association registered in Geneva, Switzerland. It has more than 150 corporate members belonging to over 20 countries. The purpose of DAVIC is to support the emergence of digital audio-visual applications and services [12].

DAVIC has identified the following security services: peer entity authentication, data origin authentication, confidentiality, integrity, access control, non-repudiation, key management, audit, and anonymity. Most security requirements for various applications will be met by combining the above security services. For the definitions of these services and the applications they are used in, see [12].

| Value | Description |
|---|---|
| 00 | Not scrambled |
| 01 | Reserved for future use |
| 10 | Scrambled with Even CW |
| 11 | Scrambled with Odd CW |

Table 2: DAVIC Defined Transport Scrambling Control Field

Security services will be provided using a mechanism based on cryptography. The cryptosystem should never expose long term keys. This may require the use of a tamper resistant security device in which the keys reside. The security device should have all the information needed to authenticate the end-user.

#### 4.2.1 Implementation requirements for scrambling

The following are implementation requirements for DAVIC systems:

- Control word (CW) is to be encrypted and distributed with the MPEG-2 transport stream packets using Entitlement Control Messages (ECMs).
- The transport scrambling control field in the MPEG-2 transport packet header is defined in Table 2.
- The scrambling algorithm should be accepted by standardization bodies such as ISO, ITU, or ETSI. The following algorithms are among those proposed to DAVIC: DVB Super Scrambling, DES, Triple DES, and FEAL.
- The scrambling algorithm must be identified since different scrambling algorithms may be used in DAVIC compliant systems. This is done either at the Session layer before the delivery of the service, or it is indicated in the CA descriptor of the program map table (PMT) during the delivery of the MPEG-2 scrambled services as per the ISO 13818-1 IS.
- TS packets must be scrambled independently and packet headers should not be scrambled.

- A key hierarchy is used for key distribution. At the top of the hierarchy are the asymmetric (public) keys. The decryption keys at the top of the hierarchy must be kept secret; Even the legitimate end-user should not know them.

### 4.2.2 ECM/EMM structure

Keys are distributed in Entitlement Control Messages (ECM) and Entitlement Management Messages (EMM).

- **ECM**: ECM messages include the conditions required to access a service, the CW, access parameters such as program number and cost per view, date and time, etc. ECM messages are sent frequently to allow quick access for new users. The parameters in the ECM messages are compared with the local entitlements and if the user is entitled to a program or a service, the CW is decrypted and passed to the descrambler.

- **EMM**: EMM messages are used to distribute the entitlements and information about consumption to the receivers. They are also used to distribute the secret keys.

### 4.2.3 Authentication

Authentication is divided into two services: peer entity authentication and data origin authentication. There are two proposals for the implementation of the authentication: X.509 and Zero knowledge authentication protocols, based upon identity.

DAVIC does not specify any particular algorithm for authentication since some algorithms are patented. The following algorithms are proposed: RSA, DSS, Elliptic curve methods, Rabin, and the zero-knowledge techniques.

## 4.3 DVB

The European standardization project on Digital Video Broadcasting, or better known as DVB, is a voluntary congregation of currently more than 130 organizations which have joined forces to make possible the development of standards for DVB in Europe as well as the early introduction of DVB services. Security for DVB is handled by an ad-hoc group, which is responsible for the definition of a policy related to conditional access and scrambling.

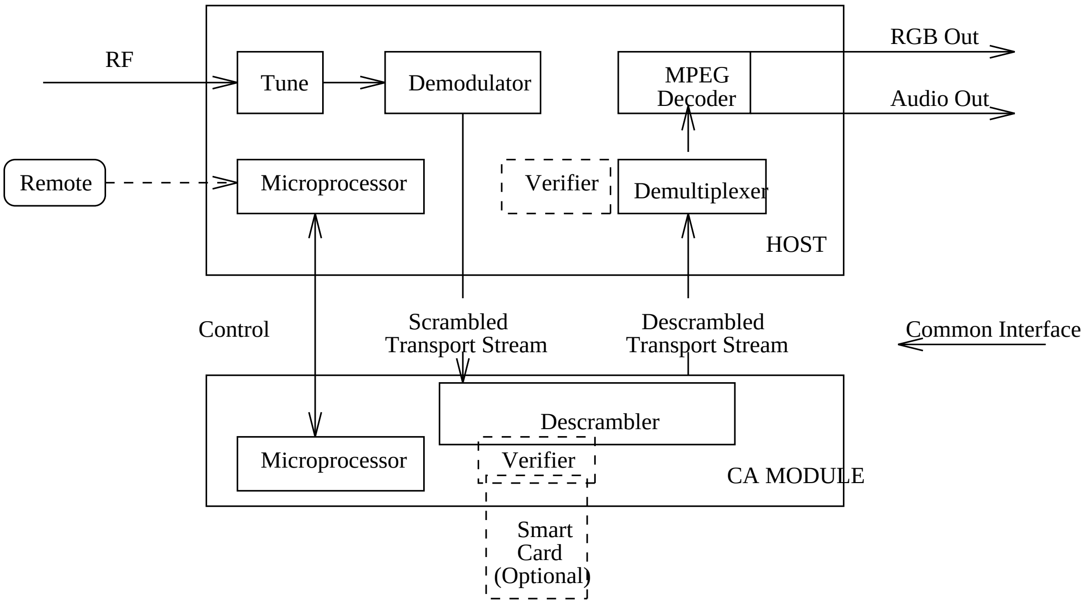


Figure 5: DVB Interface

### 4.3.1 Interface specifications for conditional access

Although DVB has issued several specifications regarding source coding, channel coding, and decoder interfaces, it has decided that no specific conditional access system for broadcast services needs to be standardized. A common scrambling algorithm however. The technical details of the algorithm is discussed in more details in the next subsection. The non-standardization allows broadcasters to provide their own conditional access systems or use the common scrambling algorithm.

One way to simplify control access interoperability is to standardize the interface between a system and a module where Conditional Access (CA) and other related functions are located. This solution allows a wider variety of anti-piracy options since there are may be various modules with different approaches offered by various suppliers.

The common interface consists of two components: the Transport Stream Interface and the Command Interface. In order to make the design and implementation of these interfaces easier, both are layered in such a way that the upper layers are common to all implementations but allows flexibility for lower layers. The Transport Stream interface is designed to carry MPEG-2 transport packets in both directions while the Command Interface takes charge of all the communications between the application(s) running in the module and the host. An example of this interface is shown in Figure 5. For further technical details, see [13].

This layout only specifies the components required to enable the interactions across the interface. There is no assumption about the design of neither the host nor the module. Nor is the operation or functionality of the module specified here. In other words, the applications running on this interface are not limited to this specification. Furthermore, more than one module may be connected simultaneously.

For efficiency, DVB provides further definitions and recommendations for MPEG-2 bit streams. The MPEG-2 Systems standard contains two bits for the scrambling control field, both in the Transport Stream packet header and in the PES packet header. The definition of these control bits in the TS packet header are given in Table 2. PES scrambling control values are identical to TS control values, except that PES packets are being scrambled instead of TS packets. However, DVB recommends that scrambling should be done at either TS or PES level, and scrambling occurring at both levels simultaneously is not allowed. Further recommendations regarding PES level scrambling are:

- The size of a PES packet header shall not exceed 184 bytes.
- A TS packet carrying a PES packet header shall have an Adaptation Field of suitable size to align the end of the PES packet header with the end of the TS packet.
- TS packets carrying scrambled PES packet data shall not have Adaptation Fields with the exception of the TS packets containing either the start or the end of a PES packet. The TS packet carrying the end of a PES packet, may carry an Adaptation Field for alignment of the end of the PES packet with the end of the TS packet.

In addition, the Program Specific Information (PSI) part of the MPEG-2 Standard defines where to find CA system information. PID values of Transport Stream packets located within CA table and Program Map table are used to carry CA information such as EMMs and ECMs. For flexible replacement of the CA information in these TS packets with other CA data at broadcast distribution media boundary, the two following constraints are recommended:

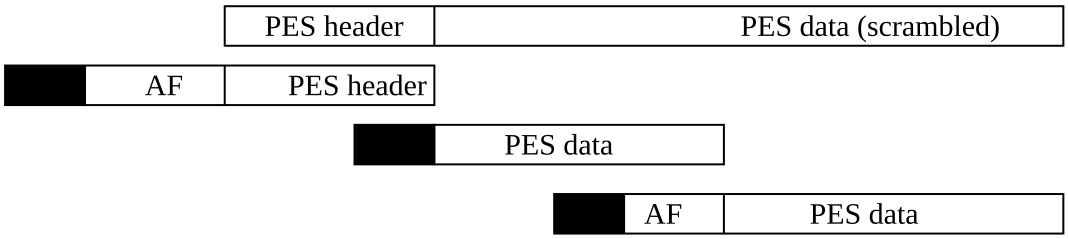


Figure 6: PES mapping to TS

- All TS packets with same PID values equal to a CA_PID value given in a CA_descriptor of a CA table shall only contain CA System information. No CA information shall be carried in any other place (e.g. Adaptation Fields).
- Different CA suppliers shall not have common CA_PID values.

#### 4.3.2 The Super Scrambling Algorithm

Another solution to control access is to use the common scrambling algorithm where access is provided upon agreements among network operators. This solution allows operation with single CA systems embedded in decoders. The common scrambling algorithm consists of a super encipherment mechanism which combines two different and unrelated ciphers.

(a) A block cipher which uses a Reverse Cipher Block Chaining (RCBC) mechanism and operates on blocks of 8 bytes.

(b) A stream cipher which combines the output bits of the block cipher with the output of a bit generator.

In block cipher, if a message has two identical blocks, the corresponding two blocks of cipher text will be identical. Hence, anyone seeing the ciphertext can gain information from repeated blocks and can re-arrange blocks to his/her advantage. Therefore, the stream cipher protects the output of the block cipher from these possible attacks by making the ciphertext different even for the same plaintext. Operating in tandem, these two ciphers can alleviate some of the strict operational recommendations.

# 5 Current security chip technology

This section discusses some of the encryption, decryption, and security system hardware solutions that are available in the market and can be used with a proper interface with video distribution systems. Two different types of hardware solutions are presented: Encryption Engines based on symmetric key cryptosystems and security system that includes Encryption Engines and key management. An important issue for most of the security products is the exportability to other countries.

## 5.1 Encryption Engines

There is a number of data encryption and decryption silicon products available in the market. These chips are usually designed to achieve high speed data rate and support various modes of symmetric key cryptosystems. Many DES based encryption engines are available in the market. They can handle a data transfer rates up to 100M bytes/sec, they support different DES modes, and they have a standard microprocessor interface. Although DES keys are usually stored in a device which is not accessible externally, they still need to be down loaded in the clear in most cases. This compromises security. The encryption engines do not provide any key management. This require the application to find a way to distribute the symmetric keys and load them securely. Therefore, encryption engines are used as building blocks for a complete security system.

## 5.2 Encryption Engines with Key Management

There are also products available in the industry which integrate encryption, decryption, and key management. This provides better convenience for users but perhaps limits them to the implanted key management system, see Figure 7.

The security chip incorporates both key management and encryption/decryption functions. These chips usually include a RISC processor which has a dual mode and can be used as a general processor or for secure cryptographic applications, standard bus interface, on-chip memory, and external memory support.

Some of these chips are designed for use with MPEG video streams not with plain data bit streams. The input data handler (IDH) accepts data in bytes from MPEG-2 demultiplexer chip

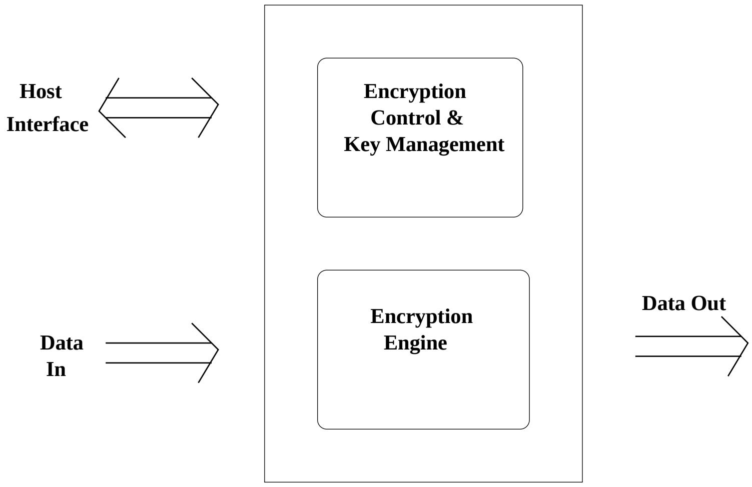


Figure 7: Encryption engine with key management

and passes it to the RISC processor. The data is then processed by the DES engine.

The desirable features of these security chips are:

- Complete cryptosystem on a single chip with high speed FIFO buffering optimized for MPEG.
- high throughput.
- On-chip non-deterministic randomizer for key and IV generation. Public key cryptosystem to be used for key distribution. The private key of the public key needs to be generated internally inside the chip and should never to be exposed.
- Distribution of the entitlements without ever exposing any of the keys.

# 6 Concluding Remarks

In this paper, we address the security issues for digital video distribution and other network services. Symmetric and asymmetric key algorithms are presented. Example of a video broadcast system with conditional access, recent work on security in MPEG, DAVIC and DVB, and current chip technologies for network security systems are also discussed.

Symmetric (private) key cryptosystems achieve high encryption throughput but they lack key management and cannot perform authentication. Asymmetric (public) key cryptosystems are computationally intensive. Therefore, they have a low encryption throughput. This inefficiency has limited the use of public key cryptosystems to two main applications: distribution of secret keys and authentication. Therefore, the adequate solution appears to be a hybrid model which uses a public key system for key management and authentication while it uses a private key system for high speed data encryption.

To incorporate a conditional access system, a TV broadcaster should link it to other components of its TV system's head-end (e.g., the subscriber management system, the security computer, and the encoder). The scrambling technique used is line shuffling. On the receiving end, smart cards are used with the zero-knowledge algorithm to test their validity.

International organizations(such as MPEG, DAVIC, and DVB) are currently working on the standarization of security issues in digital video distribution. MPEG categorize data streams into Transport and Program streams. Scrambling done at either PES or TS level brings about identification of the scrambling control bits located in the packet headers. MPEG mandates that the headers must not be encrypted. DAVIC identifies security services and their implementation requirements. The council recommends the use of a key hierarchy where the public key is at the top. This public key is also known as a long term key. Long term keys should never be exposed even to the legitimate user. DAVIC does not specify any private key algorithms for encryption or any public key algorithms for authentication because of patent-related and national regulations. It only requires algorithms in use to be accepted by standardization bodies such as ISO, ITU, or ETSI. DVB describes the common interface between the host and the module, where the data scrambling and the conditional access application reside on the module. Similar to DAVIC, DVB does not standardize any particular conditional access system, although it does provide a common scrambling algorithm called the Super Scrambling Algorithm.

Two different hardware solutions were highlighted: a data encryption processor based solely on symmetric key algorithms (encryption engines) and a security system which consists of both encryption processor and key management. Encryption engines cannot perform authentication and do not support any key management. However, encryption engines with key management offer authentication and key management using Public key algorithms and fast encryption using symmetric key algorithms. They are available on a single chip or module with private key generation internally done. This will prevent it from ever being exposed. The encryption engines with key management present a more complete solution than pure encryption engines. The main problem with all these hardware solutions remain to be their throughput (number of concurrent streams they can deliver) and their exportability. Together with the Super Scrambling Algorithm, the single chip solution with key management is a strong candidate for any digital video distribution system or other network services that require data security and authentication.

## References


[1] Diffie, W. and M. Hellman, "New Directions in cryptography," *IEEE Trans. Infor. Theory,* Vol. IT-22, pp. 644-654, Nov. 1976.

[2] Fernandez, I. and W. Subbarao, "Encryption based security for ISDN communication: Technique & applications," *Proc. IEEE SOUTHEASTCON,* pp 70-72, 1994.

[3] Fiat, A. and A. Shamir, "How to prove your self: practical solutions to identifications and signature problems," *Proceedings of Crypto,* 1986.

[4] Kaufman, C., R. Perlman, and M. Speciner, "Network Security, Private Communication in a Public World," *Prentice Hall,* Englwood Cliffs, NJ., 1995.

[5] ISO/IEC 13818-1, "Generic coding of moving pictures and associated audio:systems," *International Standard,* November 1994.

[6] Newbridge Microsystems, "Encryption Products Catalogue," *Newbridge Networks Corporation,* Canada, 1995.

[7] Rifai, A. and S. Wicker, "Evaluation of Public Key Cryptosystems," *Georgia Institute of Technology,* Atlanta, Georgia, April 1, 1995.

[8] Saini, J.S., "The BBC Select Decoder," *IEE International Broadcasting Convention,* pp. 410-413, Amsterdam, Netherlands, 1992.

[9] Salomaa, A., "Public-Key Cryptography," *Springer-Verlag,* New York, 1990.

[10] Schneier, B., "Applied Cryptography," *John Wiley & Sons, Inc.,* New York, 1994.

[11] Anzick, W. et-al, "MIRAG:An Experimental Multimedia Delivery System," *International Conference on Multimedia Communications,* South Hampton, U.K., April, 1995.

[12] DAVIC 1.0 Specification Part 10, Rev. 3.0, "Security," *Digital Audio-Visual Council,* Switzerland, June 1995.

[13] ETSI-DVB Document Number: TM 1341, Rev. 3, "Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications," February 16, 1995.