

# A Key Transport Protocol Based on Secret Sharing – An Application to Conditional Access Systems

Ahmet M. Eskicioglu\*

Thomson Multimedia  
101 West 103rd Street, INH 725  
Indianapolis, IN 46290

## ABSTRACT

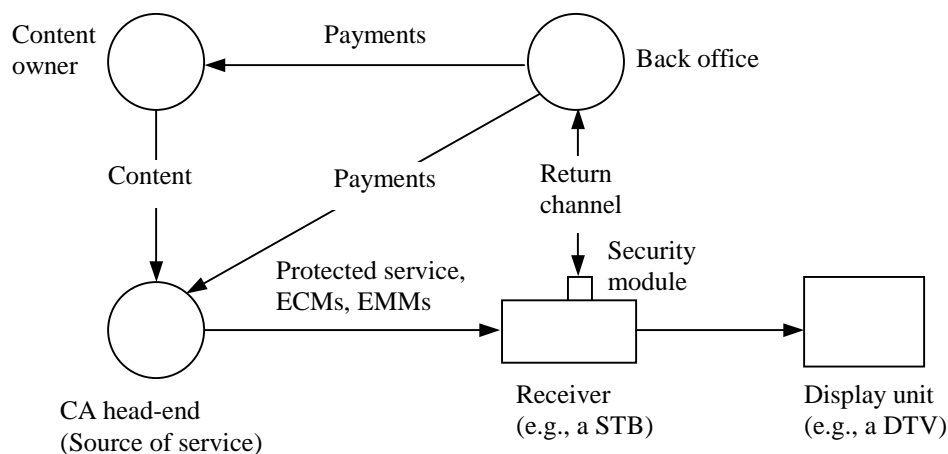
In today's digital world, multimedia content is delivered to homes via the Internet, satellite, terrestrial and cable networks. Scrambling is a common approach used by conditional access systems to prevent unauthorized access to audio/visual data. The descrambling keys are securely distributed to the receivers in the same transmission channel. Their protection is an important part of the key management problem. Although public-key cryptography provides a viable solution, alternative methods are sought for economy and efficiency. This paper presents a key transport protocol based on secret sharing. It eliminates the need for a cipher, yet combines the advantages of symmetric and public-key ciphers.

**Key words:** conditional access, content protection, key transport, multimedia, public-key cryptography, secret sharing, symmetric cipher.

## 1. INTRODUCTION

With the widespread availability of digital distribution technologies, consumers have access to a variety of services from satellite or terrestrial broadcasters, cable operators, and the Internet. The service providers deliver different types of multimedia content ranging from free access programs to services such as PayTV, Pay-Per-View and Video-on-Demand.

A conditional access (CA) system<sup>1,2</sup> is a system that allows access to services based on payment or other requirements such as identification or authorization. The user enters into an agreement with the service provider to obtain the access rights. A typical architecture of a CA system and its major components are shown in Figure 1.



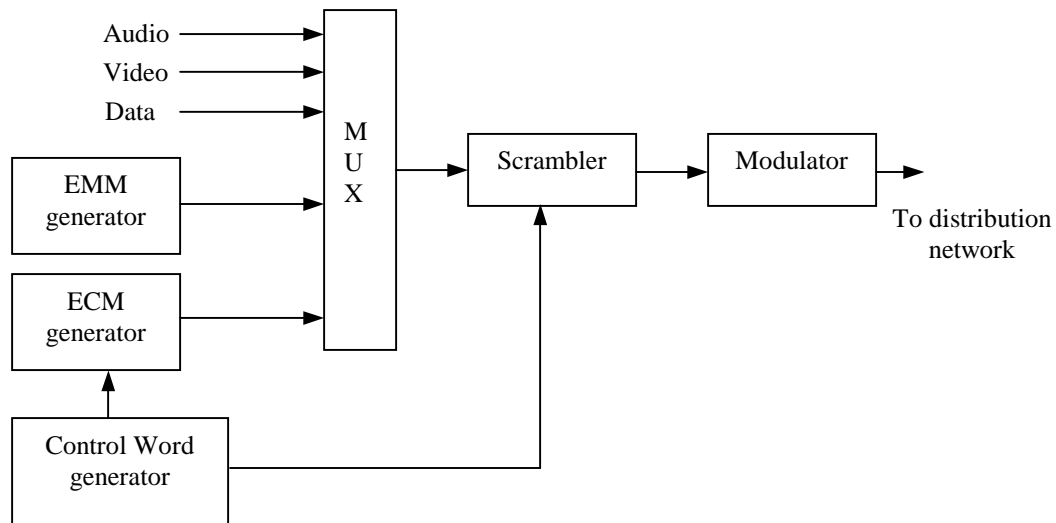
**Figure 1.** CA system architecture

\* Further author information: Email: eskicioglu@tce.com

Presently, an important source of content is the movie studios represented by the Motion Picture Association of America (MPAA). ABC, CBS, NBC, DirecTV and Time-Warner are among the leading service providers in the US. CA systems are developed by companies commonly called the CA providers. NDS, Canal+ and Nagravision are examples of CA vendors with businesses in both the US and Europe.

The service and the entitlement messages indicating the access conditions are protected at the CA head-end before they are delivered to the customer. There are two types of entitlement messages<sup>3</sup> associated with each program in a service: The Entitlement Control Messages (ECMs) carry the descrambling keys (usually called the “control word”’s in the terminology for CA systems) and a brief description of the program (program number, date, time, cost, etc.) while the Entitlement Management Messages (EMMs) specify the service-related authorization levels. The EMMs can be distributed on the same channel with the service or sent on a separate channel such as a telephone line. The ECMs are usually multiplexed with the associated program.

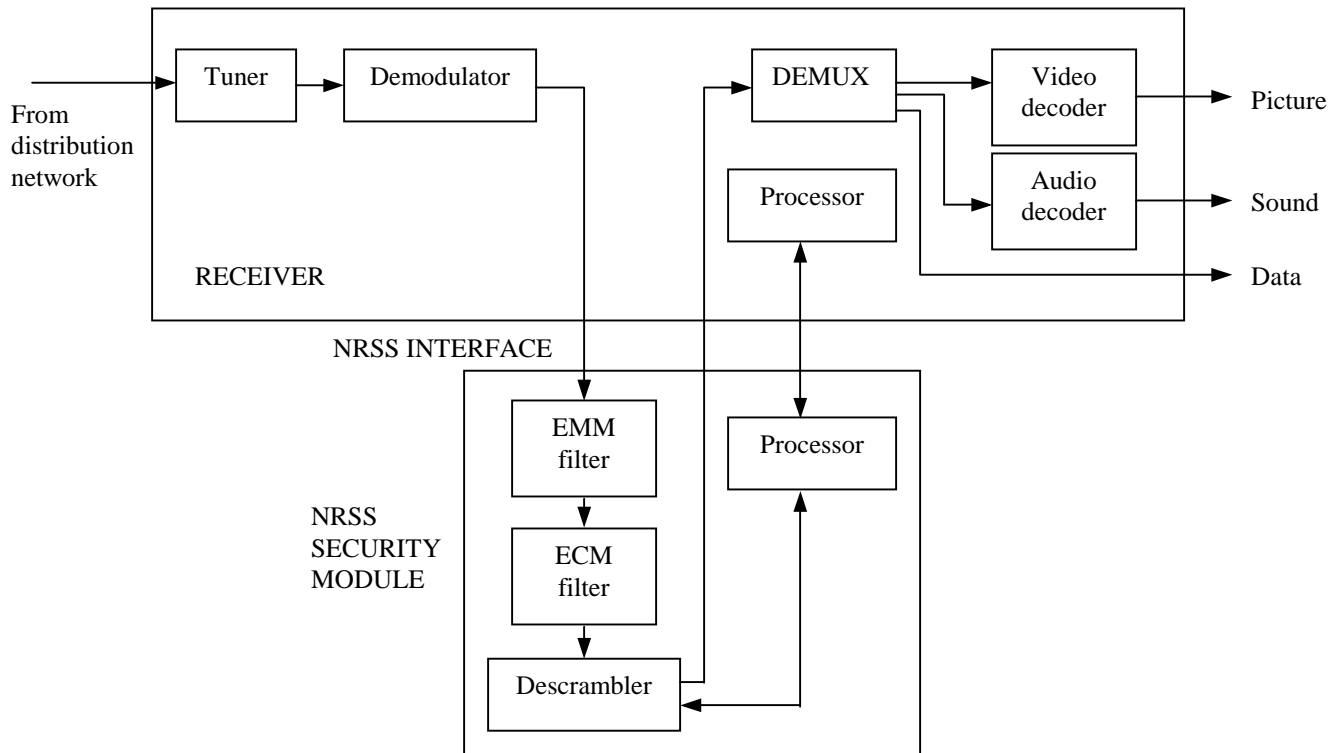
A simplified head-end architecture is given in Figure 2. Multiple streams input to the multiplexer are time multiplexed before the audio/video (A/V) data is scrambled. The signal is finally modulated for transmission through the network.



**Figure 2.** Major components of the CA head-end architecture

Encryption-based technologies are widely used for protecting distributed content. If the customer is authorized to watch a particular protected program, the A/V stream is descrambled, and sent to the display unit for viewing. In today’s CA systems, a removable security module (e.g, a smartcard) is commonly used for securely handling the ECMs and EMMs, and handling authorization checks and purchases. In the US, the National Renewable Security Standard (NRSS)<sup>4</sup> defines a renewable and replaceable security element for use in consumer electronics devices such as digital set-top boxes and digital TVs. In Europe, the Digital Video Broadcasting (DVB)<sup>1</sup> project has specified the common interface (CI) between a host device and a security module.

Separating the security functionality from the navigational devices (i.e., devices that are capable of switching between the channels) has an important consequence. It will allow the consumer electronics (CE) industry to manufacture devices independent of the private CA systems. Commercial availability of CE products at retail stores is an essential factor for a fair market competition. Figure 3 depicts the architecture of a generic receiver with an NRSS-compliant security module. Note that EMM and ECM processing and content descrambling all take place in the NRSS module.



**Figure 3.** NRSS security module and its host

A major component of every CA system is a back office that keeps track of all the transactions made. It is the responsibility of the security module to temporarily store the transaction records. At specified times, these records are sent to the back office for processing. As this transmission involves sensitive financial and personal data, a secure channel has to be established between the security module and the back office. In the case of Internet Service Providers (ISPs), the source of content and the back office may be co-located.

To complete the cycle, a portion of the payments received from the customers for the purchased services is sent to the content owners and service providers.

If the receiving and display units are two different devices in a home network, the interface between them should also be protected. The current DirecTV or cable systems include separate receivers popularly called set-top boxes (STBs). In the newly developed Advanced Television System Committee (ATSC)<sup>5</sup> system or in Internet-based CA applications, the receiver and the display unit are in the same box.

The services are usually scrambled using symmetric ciphers such as the Data Encryption Standard (DES). For security reasons, the scrambling key is changed frequently, the period of change being on the order of a few seconds. Although the protection of the ECMs is often privately defined by the CA providers, public-key cryptography<sup>6,7</sup> is a viable tool for transporting the keys from the service source to the receivers. The descrambling keys are encrypted with a public key at the source, and recovered by the corresponding private key stored in the receiver.

In spite of the fact that public key cryptography is an elegant way to protect ECMs, it has major disadvantages. Public key schemes are considerably slower than symmetric key schemes, and have longer keys. Their security is based on the difficulty of solving number-theoretic computational problems. RSA (the most widely used algorithm), for example, assumes that the integer factorization problem is intractable.

## 2. A KEY TRANSPORT PROTOCOL BASED ON SECRET SHARING

We describe an alternative system<sup>†</sup>, based on secret sharing,<sup>6-9</sup> that eliminates the need for public key cryptography (or any other cipher), and facilitates the secure transmission of A/V data from the service providers.

### 2.1 Threshold schemes

A  $(t, n)$  threshold scheme ( $t \leq n$ ) is a method by which  $n$  secret shares  $S_i$ , ( $1 \leq i \leq n$ ), are computed from a secret  $S$  in such a way that at least  $t$  shares are required to reconstruct  $S$ . A perfect threshold scheme is a threshold scheme in which a knowledge of  $(t-1)$  or fewer shares gives no information about the secret. For example, with a  $(3,4)$  threshold scheme, the secret is divided into four pieces, and only three of the four pieces are required to reconstruct the secret.

In Shamir's  $(t, n)$  threshold scheme<sup>8</sup>, the secret  $S$  is the coefficient  $a_0$  of a random  $(t-1)$ -degree polynomial

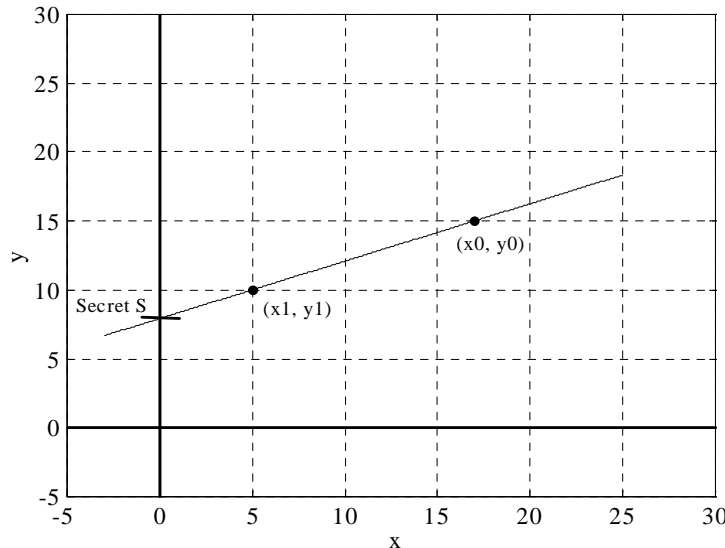
$$f(x) = (a_{t-1}x^{t-1} + \dots + a_1x + a_0) \bmod p$$

over the finite Galois Field  $GF(p)$ , where  $p$  is a prime number larger than both  $S$  and  $n$ . Each of the  $n$  shares  $(x_i, y_i)$  is a point on the curve defined by the polynomial  $f(x)$ . As a polynomial of degree  $(t-1)$  can be uniquely determined by  $t$  points, the secret can be computed from  $t$  shares. Threshold schemes have proved useful in many applications of cryptography including electronic cash, group signatures, key recovery and voting. Shamir's  $(2, 2)$  threshold scheme will be used in presenting the key transport protocol.

In Figure 4<sup>‡</sup>, the first degree polynomial  $f(x)$  is uniquely defined by the two points  $(x_0, y_0)$  and  $(x_1, y_1)$ . The shared secret  $S$  is then expressed as the  $y$ -intercept, i.e.,

$$S = f(0) = y_0 - \frac{(y_1 - y_0)}{(x_1 - x_0)}(x_0).$$

The knowledge of  $(x_1, y_1)$  alone does not reveal the secret.



**Figure 4.** Shamir's threshold scheme

<sup>†</sup> Thomson Multimedia patent pending.

<sup>‡</sup> Note that for demonstrative purposes the plots in Figures 4 and 5 are obtained using real numbers, and not modular arithmetic.

The following numerical example will use the same points on the graph, but the arithmetic will be performed in GF(23).

**Example 1:** Let  $(x_0, y_0) = (17, 15)$ ,  $(x_1, y_1) = (5, 10)$ , and  $p = 23$ . The polynomial

$$f(x) = a_1x + a_0 \pmod{23}$$

passing through these two points can be constructed by solving

$$a_1 * 17 + a_0 = 15 \pmod{23},$$

$$a_1 * 5 + a_0 = 10 \pmod{23}.$$

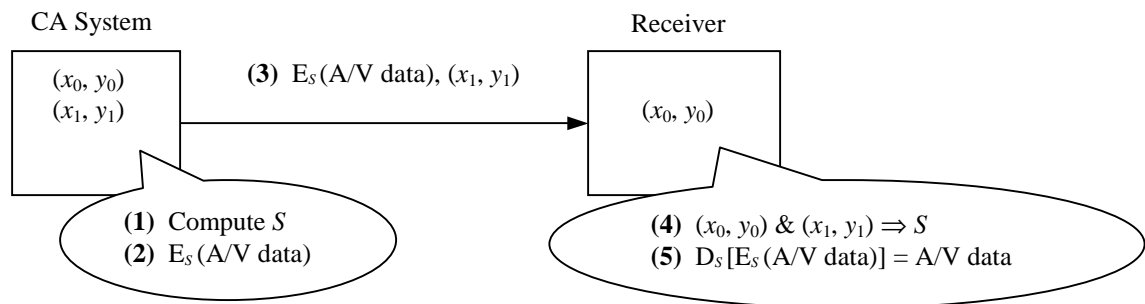
The solution  $(a_1, a_0) = (10, 6)$  gives the polynomial

$$f(x) = 10x + 6 \pmod{23}.$$

The value of the secret  $S$  is therefore  $f(0) = 6 \pmod{23}$ . In practice, much larger values should be used with the scheme.

## 2.2 Shamir's threshold scheme for key transport

An application of Shamir's scheme to transport descrambling keys is shown in Figure 5. The receiver (or the removable security module) is manufactured with the point  $(x_0, y_0)$  on the first degree polynomial to be constructed. The CA system at the source uses the points  $(x_0, y_0)$  and  $(x_1, y_1)$  to compute the secret  $S$ , scrambles the A/V data, and transmits the scrambled A/V data with  $(x_1, y_1)$  in-the-clear. On receiving  $(x_1, y_1)$ , the receiver constructs the polynomial passing through the two points, and recovers the secret.  $E_S$  and  $D_S$  denote scrambling and descrambling with the symmetric key  $S$ , respectively.



**Figure 5.** Protection of content with secret sharing

Each time a fresh key is needed, the CA system picks a point that would result in a polynomial with a different y-intercept. Hence, although the point  $(x_0, y_0)$  remains the same in the computation, a new key is obtained. In practice, it is important to choose the scrambling keys randomly and independent of the polynomial construction. The key generation and distribution process can be automated by using the following steps:

- (i) Choose  $S$ .
- (ii) Construct the polynomial  $f(x)$  that passes through  $(0, S)$  and  $(x_0, y_0)$ .
- (iii) Compute  $f(x)$  at  $x_1, x_1 \neq x_0$ .
- (iv) Distribute  $(x_1, y_1)$  with the content protected with  $S$ .

This is an example of a prepositioned shared secret scheme<sup>9,10</sup> where it is possible to reconstruct different keys by communicating different activating shares for the same prepositioned information. The use of such a scheme has been discussed within the context of critical military applications. An interesting scenario is when a private piece of information must be communicated from a commander to a group of subordinate officers to launch a missile. Two desired requirements of the system would be:

- (1) the officers should not be able to cooperate to find the launch code without their commander's participation.
- (2) the commander should be able to send a different piece of private information to activate a different launch code.

### 2.3 Generalization of the scheme

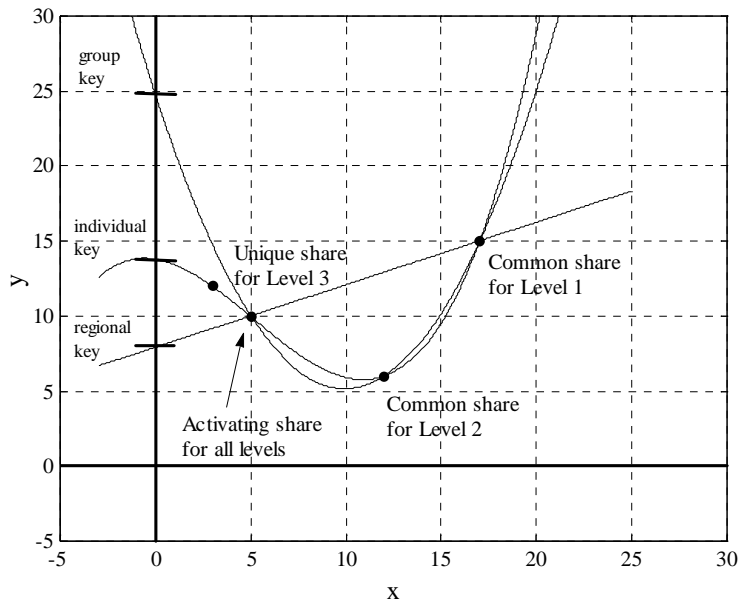
In a generalization of the proposal, the value of  $t$  is a system parameter. Choosing a higher value for  $t$ , and storing  $(t-1)$  shares in the receiver would increase the system's resistance to ciphertext-only attacks, but lead to more computations for polynomial construction.

Multiple shares can also be used to build a convenient key management scheme in a CA system. CA system operators usually define three levels of keys: individual, group and regional. Receivers can be assigned different authorization levels by storing different numbers of shares. The simple scenario below will explain how the required key hierarchy can be established with secret sharing.

Consider a CA system in which a population of smartcards is used for keeping authorizations and descrambling services. Three different card types are specified:

- Level 1: All the smartcards in the broadcast region are assigned one common share (the polynomial is of first degree).
- Level 2: All the smartcards in a given group are assigned an additional common share (the polynomial is of second degree).
- Level 3: Each smartcard is assigned a unique additional share (the polynomial is of third degree).

As shown in Figure 6, if the service is broadcast for all the receivers in the region, the smartcards will construct a first degree polynomial using the common share, and obtain the same descrambling key. If a particular group or an individual is authorized to have access to the service, the additional share(s) will result in a key that cannot be constructed by the other smartcards in the region.



**Figure 6.** Key generation for three authorization levels

**Example 2:** Three polynomials will be constructed using the points on the graph. The first degree polynomial is already constructed in Example 1. The second degree polynomial will pass through the common share for Level 1, the common share for Level 2 and the activating share. For the construction of the third degree polynomial, the additional point will be the unique share for Level 3.

Let  $p = 23$ . The coordinates of the points needed for the three polynomials are given in Table 1.

Point \ Degree of polynomial	First	Second	Third
The activating share = (5, 10)	x	x	x
The common share for Level 1 = (17, 15)	x	x	x
The common share for Level 2 = (12, 6)		x	x
The unique share for Level 3 = (3, 12)			x

**Table 1.** Points for polynomial construction

(a) First degree polynomial

From Example 1,  $f(x) = 10x + 6 \pmod{23}$  and  $S = 6 \pmod{23}$ .

(b) Second degree polynomial

The coefficients of the second degree polynomial

$$f(x) = a_2x^2 + a_1x + a_0 \pmod{23}$$

are obtained by solving

$$a_2 * 17^2 + a_1 * 17 + a_0 = 15 \pmod{23},$$

$$a_2 * 12^2 + a_1 * 12 + a_0 = 6 \pmod{23},$$

$$a_2 * 5^2 + a_1 * 5 + a_0 = 10 \pmod{23}.$$

The solution gives  $(a_2, a_1, a_0) = (10, 20, 5)$ . Hence,  $S = 5 \pmod{23}$ .

(c) Third degree polynomial

The coefficients of the third degree polynomial

$$f(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \pmod{23}$$

are obtained by solving

$$a_3 * 17^3 + a_2 * 17^2 + a_1 * 17 + a_0 = 15 \pmod{23},$$

$$a_3 * 5^3 + a_2 * 5^2 + a_1 * 5 + a_0 = 10 \pmod{23},$$

$$a_3 * 12^3 + a_2 * 12^2 + a_1 * 12 + a_0 = 6 \pmod{23},$$

$$a_3 * 3^3 + a_2 * 3^2 + a_1 * 3 + a_0 = 12 \pmod{23}.$$

The solution gives  $(a_3, a_2, a_1, a_0) = (18, 19, 0, 22)$ . Hence,  $S = 22 \pmod{23}$ .

In general, the coefficients of the polynomial  $f(x)$  of degree at most  $(t-1)$ , defined by the points  $(x_i, y_i)$ ,  $0 \leq i \leq (t-1)$ , are computed from

$$f(x) = \sum_{i=0}^{t-1} y_i \prod_{0 \leq j \leq t-1, j \neq i} \frac{(x - x_j)}{(x_i - x_j)}.$$

The shared key obtained from  $t$  secrets can then be expressed as

$$f(0) = \sum_{i=0}^{t-1} y_i \prod_{0 \leq j \leq t-1, j \neq i} \frac{x_j}{(x_j - x_i)}.$$

## 2.4 Cryptanalysis

In the prepositioned shared secret scheme for missile launching, the activating share is the only data communicated to the officers to determine the corresponding missile launch code. In our scheme, the shared secret is used to scramble the service which is broadcast with the activating share. The system is therefore exposed to brute-force attacks for small values of  $t$ , i.e., lower degree polynomials. A potential hacker may use the available ciphertext in an attempt to find the prepositioned information.

For  $t = 2$ , the system is most vulnerable to ciphertext-only attacks. The hacker needs to find two descrambling keys to compute the prepositioned information. The intersection of the two first degree polynomials gives the single share  $(x_1, y_1)$ . With higher values of  $t$ , it becomes increasingly more difficult to estimate the stored information even if multiple descrambling keys are found.

The robustness of the system can be substantially increased in a number of ways:

1. Define the scrambling key as a function of the shared secret: In Shamir's (2, 2) scheme, the secret (hence the key) is defined to be the  $y$ -intercept of the constructed polynomial. In general, the key can be generated by evaluating a predefined function at the value of the secret. Alternatively, any other definition can be used once the coefficients of the polynomial are obtained. For practical purposes, the function may need to have an entropy preserving property, i.e., the entropy (secret) = the entropy [f (secret)].
2. Make  $t$  a time-dependent secret system parameter: Cryptanalysis would become a more demanding task for the adversaries because they would first have to estimate the degree of the polynomial (hence the number of shares needed for key recovery).
3. "Mask" the activating share before transmission: The activating share transmitted with the scrambled content can be unmasked by the receiver in a predefined process. An example of masking would be to use a hash value of the activating share for content scrambling but transmit the share instead.
4. Add redundant activating shares: Additional activating shares transmitted with the actual share are filtered out by the receiver in a predefined process. The redundant shares can also be used to determine the value of  $t$  if it is used as a system parameter.

Any combination of these improvements will hide the real value of the activating share in transmission, and introduce an additional level of protection for the system.

Copy protection is another important issue for the content providers. Delivery systems will carry the information along with the copyrighted content that indicates if the consumer is authorized to make a copy. Other methods and key management schemes are needed to prevent unauthorized access to content across the interfaces and in storage.<sup>11</sup> Conditional access and copy protection are two critical issues that need to be addressed in parallel for the management of rights associated with the consumption of digital content.

### 3. CONCLUSIONS

The proposed scheme can be a convenient key transport mechanism for conditional access systems delivering multimedia content. It can also be used in other architectures requiring secure communications. The major strengths of such an approach are:

- It drastically reduces the computational requirements for the receiver in symmetric key recovery. For each new key, only a simple operation (i.e., construction of a low-degree polynomial) is performed. This is in sharp contrast with RSA decryption which involves modular exponentiation.
- From a security viewpoint, it is “perfect,” i.e., given knowledge of the activating share, all values of the secret remain equally probable. For sufficiently high values of  $t$ , i.e., the degree of the polynomial, brute-force attacks can be made harder.
- For a given prepositioned information shared between the receiver and the service source, different symmetric keys can be derived and used frequently.
- Different customer authorization levels can be defined by assigning different shares to the receivers.
- Security does not rely on unproven mathematical assumptions (e.g., the security of RSA is based on the difficulty of the integer factorization problem).

The scheme effectively combines the advantages of symmetric and public key systems. The prepositioned information can be considered to be the “private key” of the receiver. The symmetric key to be constructed is determined by the public information sent as part of the ECM. As the descrambling keys are not generated at the service source, no additional cipher is needed to protect them in distribution.

It is evident that secret sharing schemes can also be used for message authentication<sup>7</sup> which is another important objective of information security. This objective is met by providing the receiver of a message an assurance of the sender’s identity. Methods for message authentication require symmetric or public key ciphers, and management of their keys.

Ramp schemes<sup>12</sup> or dynamic threshold schemes<sup>13,14</sup>, which are extensions of conventional threshold schemes, may prove useful in developing similar key transport protocols. An investigation in this field is encouraged as future work.

### REFERENCES

1. R. de Bruin and J. Smits, *Digital Video Broadcasting: Technology, Standards and Regulations*, Artech House, Inc., 1999.
2. H. Benoit, *Digital Television: MPEG-1, MPEG-2 and Principles of the DVB System*, Arnold, 1997.
3. International Standard ISO-IEC 13818-1 “Information technology – Generic coding of moving pictures and associated audio information: Systems,” First Edition, 1996.
4. “EIA-679B National Renewable Security Standard,” September 1998.
5. “Advanced Television Systems Committee Standard A/53,” available at <http://www.atsc.org>.
6. B. Schneier, *Applied Cryptography*, John Wiley and Sons, Inc, 1996.
7. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.
8. A. Shamir, “How to share a secret,” *Communications of the ACM*, Vol. 22, No. 11, pp. 612-613, November 1979.

9. G. J. Simmons, "How to (really) share a secret," *Advances in Cryptology – CRYPTO '88 Proceedings*, Springer-Verlag, pp. 390-448, 1990.
10. G. J. Simmons, "Prepositioned shared secret and/or shared control schemes," *Advances in Cryptology – EUROCRYPT '89 Proceedings*, Springer-Verlag, pp. 436-467, 1990.
11. A. M. Eskicioglu and E. J. Delp, "An overview of multimedia content protection in consumer electronics devices," accepted for publication in *Signal Processing: Image Communication*.
12. G. Blakely and C. Meadows, "Security of ramp schemes," *Advances in Cryptology – CRYPTO '84 Proceedings*, Springer-Verlag, pp. 242-268, 1985.
13. C. -S. Lai, L. Harn, J. -Y. Lee and T. Hwang, "Dynamic Threshold Scheme based on the definition of cross-product in an n-dimensional linear space," *Advances in Cryptology – CRYPTO '89 Proceedings*, Springer-Verlag, pp. 286-298, 1990.
14. C. Blundo, A. Cresti, A. De Santis and U. Vaccaro, "Fully dynamic secret sharing schemes," *Advances in Cryptology – CRYPTO '93 Proceedings*, Springer-Verlag, pp. 110-125, 1994.