Key Distribution and Management for Conditional Access System on DBS

Jang Won Lee

Electronics and Telecommunications Research Institute

ABSTRACT

In this paper, key distribution and management for Conditional Access System(CAS) on Digital Broadcasting System(DBS) via KoreaSat is proposed in order to provide Pay TV services. The levels of keys for CAS are defined and analysis of characteristics of key and management on CAS are considered. In addition to that, we also discuss the key distribution protocols. Finally, the scenario of key distribution and management on overall system is described.

1. Introduction

Conditional Access System(CAS) is essential in order to provide Pay TV services on digital broadcasting system. The key management and distribution are as important as cryptographic algorithm. There are four levels of keys. Using these keys, broadcasting data is transmitted securely.

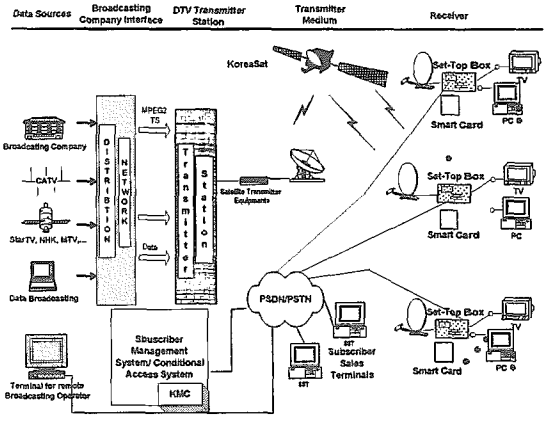
After the information for conditional access service are encrypted, the encrypted messages are transmitted to receiver sides. The necessary keys to be distributed only to authorized subscriber in order to decrypt the message sent from transmitter side. If we assume the cryptographic algorithm is secure enough, the stability of conditional access system depends on the key distribution and management.

In chapter 2, we discuss the overview of the Pay TV service and the functions of the conditional access system. In chapter 3, we deal with key matters; the characteristics of key on CAS, the proposal for managing keys on CAS. We also define four levels of keys and mention the distribution and update. In chapter 4, we discuss the distribution and update protocols between the center and subscriber. Finally, in chapter 5, the scenario of overall system architecture is presented. Both the transmitter and receiver side are described in more details.

2. Pay-TV Services

2.1 Overview

As shown in Fig. 1, Pay TV system consists of broadcasting service provider, transmitter station which connected through broadcast distribution network, subscriber management system, conditional access system, KoreaSat as a transmitter medium, receiver antenna, set-top-box, smart card and receiver including monitors for receiving . The broadcasting service provider sends the program to be transmitted through broadcast distribution network. The transmitter station transmits the scrambled data to receiver using transmitter medium after scrambling the broadcasting source program with control word. The transmitting data format references to MPEGII standard, and the average of data rate is 0.78Mbps in worst case. The key management center(KMC) on CAS generates the secret keys and performs to authenticate the subscriber.



(Fig. 1) Pay-TV System Architecture

The subscriber inserts the smart card into set-top-box then decrypts PK or GK obtained from EMM using master key stored in the smart card. DEK obtained from

EMM is decrypted using PK or GK. Finally, CW obtained from ECM is decrypted using DEK. Then the descrambling process is performed using the control word(CW). Hence, the subscriber then could be able to watch the program via monitor.

2.2 Functions of Conditional Access System

A conditional access requires scrambling/descrambling, entitlement control and entitlement management. These need encipherment for effective and secure operation.

2.2.1 Scrambling/Descrambling

The scrambling makes unintelligible signal, such that an unauthorized receiver can not see and hear. The scrambling method is varying according to the program type and the signal type. The descrambling process is achieved by any receiver which is withholding the control word.

2.2.2 Entitlement Control

Entitlement control broadcasts entitlement control message(ECM). The ECM consists of encrypted control word(CW) and control parameter, and is broadcast and re-generated periodically. The receiver transfers ECM to smart card, and microprocessor in the smart card compares the received control parameter with authorization parameter in the smart card. If the comparison is equal, then the receiver is authorized. Authorized receiver can decrypt CW by a service key in the smart card, then generate the initialization word which is necessary in descrambling.

2.2.3 Entitlement Message

Entitlement management gives the access rights to the authorized viewers and updates the authorization key for the receiver. The entitlement management function manages the information of the program, achieve the entitlement management message(EMM). Transmission of EMM is not simultaneous transmission of the program but a batch processing. The EMM can be transferred by mail or a specific channel.

3. Key

In this chapter, we describe the characteristics and proposal of managing the key on conditional access system. The definition of the key and key generation are also mentioned.

3.1 Characteristics of key on CAS

The method of key management is closely related to cryptographic system as well as characteristics of communication channel. Therefore, in order to provide security services of communication environments, the characteristics of communication ,used for selecting the method of key management, are seriously considered.
The broadcasting environments applied to conditional access system are such that one way channel namely broadcasting station unilaterally transmits the broadcasting data to receiver side. So it is like the way one to multi-functional relation. The characteristics of this kinds of broadcasting channel differs from key management problem in general network. These are as following:

- o In general network environments, the users do not trust each other. On the other hand, in case of conditional access system ,under the assumption that the subscriber must trust the broadcaster, the broadcaster performs as a role of key server;
- o The key management methods used for general network environments need hand shaking including the mutual authentication procedure. On the other hand, in case of conditional access system, it is impossible due to use the one way channel.

3.2 Proposal for managing keys on CAS

There are several kinds of key management methods. In simplest one is to distribute key in broadcasting environments, all the information to be broadcast are encrypted with single key. This actually does not exist key distribution and easily implemented. However, the disadvantage of this method is that the lack of security. What more an additional procedure needed for appending or deleting of the subscribers.
In second method, the information to be broadcasted are encrypted with each subscriber's secret key then broadcasting this encrypted messages. This method also simply implemented and easily done the subscriber's management. The disadvantage of this method is not reflect the real world, commercial market, due to increase the size if the broadcasting data as increasing the number of subscribers.
In conditional access system, as designing the key management system, to focus on that subscriber management and minimize the increase of message when the subscriber is increasing. For this, setting the group and sharing the key should be dependent on the forms of service and impose the rates. Hence, it cause the problem that sharing group key's update and deletion of certain subscriber within the group. In order to simplify the deletion and addition of the subscribers, it is more efficient that the distribution is performed in hierarchical key system.
Repeatedly speaking, the actual service element is encrypted with group key(GK) for each group and the

encrypted PK is transfered to authorized subscribers after the GK is encrypted with the subscriber's unique private key(PK). When the subscriber is added, the problem of increasing message is drastically cuts down as only transferring the GK to new subscriber. The deletion of subscriber within the certain group could be easily solved as updating GK sharing group.
The both symmetric and public algorithm could be used for key distribution. In case of using symmetric algorithm, the subscriber maintain the secret for key information with program provider, which may be broadcasting company and subscriber registered. The subscriber also wants to register new service provider, the new information must be input into smart card. It is possible that all the service provider could maintain the subscriber's master private key (MPK). Due to insecurity, the service providers are required the safe management. In case of using the public algorithm, the subscriber needs only to maintain his own secret key in his/her smart card. The service provider use it as a master key maintaining the subscriber's public key as registered

3.3 Definition of keys

Each service stream is distinguished from channel, and channel data are scrambled with control word(CW). The CW is encrypted with Direct Entitlement Key(DEK) and broadcasts in forms of messages. Therefore, it should be possible to access DEK in order to access Entitlement Control Message(ECM) for each channel. The DEK also imposes the entitlements to subscribers by Entitlement Management Message(EMM), encrypted with PK or GK. Finally, PK or GK is encrypted with Master Private Key(MPK). The Fig. 2 depicts the architecture of key hierarchy.

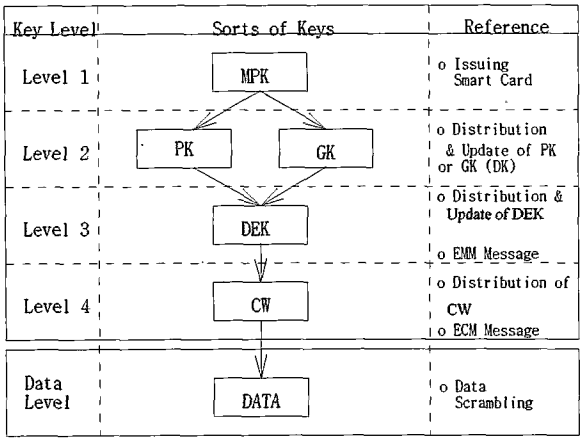


Fig. 2 Architecture of Key hierarchy

The key management system consists of four levels, control word(CW), direct entitlement key (DEK), distribution key (DK), which consists of private key(PK) and group key (GK), master private key (MPK) from bottom to upwards. The each key is used for encrypting the next higher level key and distribution. The roles and characteristics of these keys are as following:

o Control Word(CW)
The control word is used for scrambling broadcasting program. This is unique for each service channel. In order to increase the security, the control word should be updated with short(5-10 second) periods whenever transmission occurs using ECM.

o Direct Entitlement Key(DEK)
The direct entitlement key is used for encrypting the control word and to access Entitlement Control Messages. This is unique for each subscriber or group according to form of group. This key is never revealed to the subscriber and updated about a month periods.

o Distribution Key(DK)
The Distribution key consist of private key and group key according to form of group for subscribers. It is used for encrypting direct entitlement key. The private key is unique for each subscriber distinguished with subscriber's address and the group key is unique for each group distinguished with group address. The key is stored in the smart card and never revealed to the subscriber. The group key can be updated via a broadcast Entitlement Management Messages.

o Master Private Key(MPK)
The Master key is used for encrypting the distribution key and is unique for each subscriber distinguished with subscriber address. The key is stored in the smart card and is never revealed to the subscriber. The key is never changed during the life cycle of the card.

3.4 EMM/ECM

- EMMs(Entitlement Management Message) are addressed to individual subscribers to authorize them for program viewing. They are encrypted with the cardholder's private key(PK) or group key(GK). These messages give the subscriber the access information it needs to access the ECM messages. These messages are re-transmitted periodically. The period is determined by the number of subscribers and the required update time.
- ECMs(Entitlement Control Message) accompany

each program stream and it gives the parameters necessary to generate the scrambler control words for that channel. These messages are re-transmitted periodically. The period between re-transmission depends on the required channel acquisition time.

3.5 Key generation

3.5.1 MPK Generation

MPK generator is used to generate master private key(MPK) as issuing the smart card in subscriber management system. The following Fig. 3.1 depicts the configuration of MPK generator.

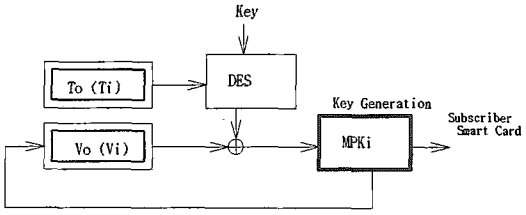
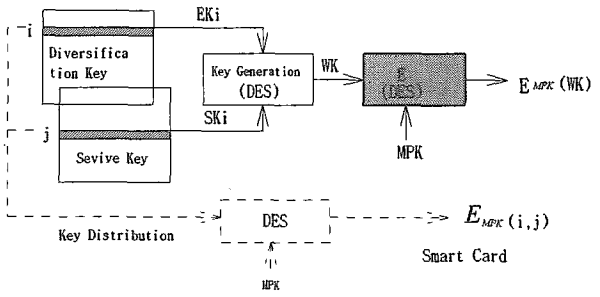


Fig. 3.1 MPK Generator

3.5.2 Using Key Generation Matrix

The matrix method is used to generates expect master private key(MPK) and the procedure of generating key is as following:

- A service key address(I) and diversification key address are specified;
- A service key is obtained using the next 8 bytes of the matrix and a diversification key is obtained using the next 8 bytes of the matrix;
- The service key is then input to a generator with the diversification key as the input parameter;
- The result from the generator is the encryption key to be used unless the encryption key generated is a private key(PK). In case of a PK, the generated key is then randomized again using a Data Encryption Standard(DES) encryption with the master private key(MPK) as the key. The extra step used for generation of a PK is necessary since there are potentially 5 million subscribers and only 256^2 possible keys generated from the matrix.



WK : Working Key
MPK: Master Private Key

Fig. 3.2 Key generation based on matrix method

3.5.3 PK,GK,DEK(PGD) Generation

PGD generator is used to generate private key(PK), group key(GK) and direct entitlement key(DEK). This method is based on ANSI X9.17 Standard. The symmetric algorithm is used and the seed value and encryption key used in algorithm is securely generated and managed in order to generate secure key generation. The following are depicted the definition of key generator and the configuration as shown Fig. 3.3.

$$R_i = E_k(E_k(T_i) \text{ XOR } V_{i+1})$$
$$V_{i+1} = E_k(E_k(T_i) \text{ XOR } R_i)$$

where k : reserved key for secret key generation
T : time stamp
V : secret 64 bit seed

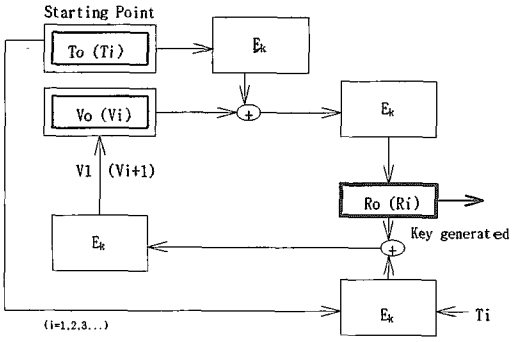


Fig. 3.3 PGD Generator

To and Vo are used as a starting points. The To is the value of current time stamp and the Vo is the secure 64 bits information, could be defined using subscriber's password. The value of R is generated to key and the exclusive -OR operation between the value of V in previous round and time stamp in next round. The result then encrypted. Hence, the value of key is generated.

3.6 Distribution and update

The procedure of key distribution carried out firstly issuing master private key, then distribution of the distribution key(DK), PK or GK, distribution of direct entitlement key(DEK) and distribution of control words(CW) in turn.

- Issuing Master Private Key(MPK)

After the smart card is issued to subscriber, the MPK, which is stored in the smart card never changed during the life cycle of the card. The service provider which the subscriber is registered must maintain the same MPK as the subscriber have. MPK is used to distribute

DK and protect the usage records.

- Distribution of Distribution Key(DK)

The DK consists of PK and GK and is used to encrypt the DEK. When the subscriber is registered, it is obtained as the forms of EMM(MPK[PK,H]), EMM(MPK[GK,H]). If any change occurs within the group, update can be done using EMM, updated with a period of one month. The H is the one way hash value for integrity of messages. The subscriber receives the broadcasting EMM then decrypts the message using MPK. After that, comparison is performed between the H which is generated and the H from transmitted. If this succeeded, the DK is obtained.

- Distribution of Direct Entitlement Key(DEK)

The DEK is used to protect CW and is unique for each service channel. As servicing the program, the DEK encrypted with PK or GK for each subscriber or subscriber group and contained in EMM then transmitted. Since receiving the EMM, the subscriber decrypts it with PK or GK then obtains the value of H. The subscriber obtains the DEK after comparing the H from EMM and generated H.

- Distribution of Control Word(CW)

The CW is used to scramble the original source program and is unique for each service channel. This is broadcast the form of containing in ECM. The subscriber obtains the CW by decrypting the message with DEK which is already distributed. The CW then is used to decrypt the scrambled program.

4. Distribution and update Protocol

In this chapter, we describe the protocols of key distribution and how each key is distributed. The Figure helps to understand the procedure of key distributions.

4.1 Protocol of PK distribution and update

The Fig. 4.1 shows the procedure of distribution and update. The steps are described as following:

1) Generates Pki in Center;
2) Encrypts the generated key using encryption algorithm with MPK;
3) Transfer it to subscriber contained by EMM;
4) The subscriber receives the EMM safely;
5) Decrypts the encrypted Pki using decryption algorithm with MPK;
6) Stores PKi.

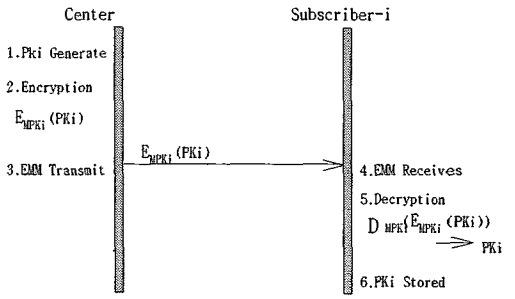


Fig. 4.1 Protocol of distribution and update for PK

4.2 Protocol of GK distribution and update

The Fig. 4.2 shows the procedure of distribution and update. The steps are described as following:

1) Generates Gki in Center;
2) Encrypts the generated key using encryption algorithm with MPK;
3) Transfer it to subscriber contained by EMM;
4) The subscriber receives the EMM safely;
5) Decrypts the encrypted Pki using decryption algorithm with MPK;
6) Stores GKi.

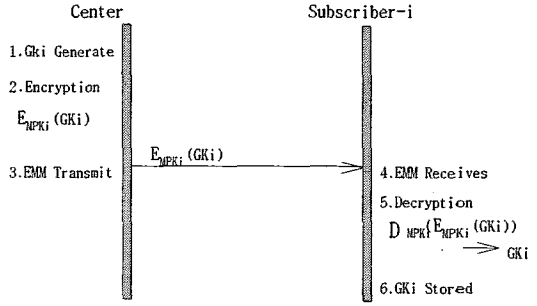


Fig. 4.2 Protocol of distribution and update for GK

4.3 Protocol of DEK distribution and update

The Fig. 4.3 shows the procedure of distribution and update. The steps are described as following:

1) Generates DEKi in Center;
2) Encrypts the generated key using encryption algorithm with PK or GK;
3) Transfer it to subscriber contained by EMM;
4) The subscriber receives the EMM safely;
5) Decrypts the encrypted DEKi using decryption algorithm with PK or GK;
6) Stores DEKi.

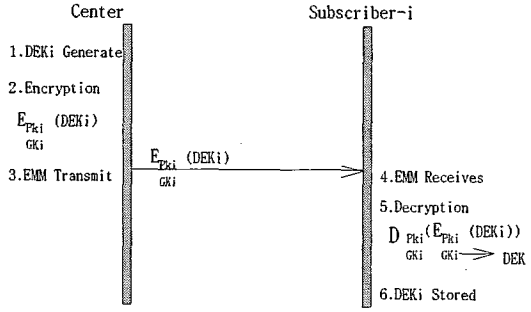


Fig. 4.3 Protocol of distribution and update for DEK

4.4 Protocol of CW distribution

The Fig. 4.4 shows the procedure of distribution. The steps are described as following:

1) Generates CW in Center;
2) Encrypts the generated control word(CW) using encryption algorithm with DEK;
3) Transfer it to subscriber contained by ECM;
4) The subscriber receives the EMM safely;
5) Decrypts the encrypted CW using decryption algorithm with DEK;

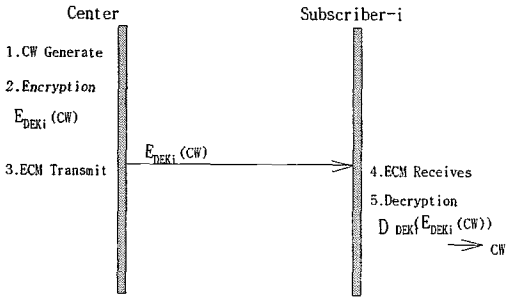


Fig. 4.4 Protocol of distribution for CW

5. System Architecture

In this chapter, we describe the overall system includes transmitter and receiver sides. This shows how each side of the system is operated.

5.1 Transmitter Side

The transmitter side consists of smart card issuing emulator, key generator, key database, scrambler with DVB common scrambling algorithm and transmitter.

The master private key is generated by the MPK generator. When the smart card is issued, the master private key is injected into the card then stored in key Database(DB). The master private key is used as a key for distributing and updating of private key or group key.

PGD generator generates private key(PK), group key(GK) and direct entitlement key(DEK) then the generated keys are stored in the key database(KDB). These are used as a key for distributing and updating of private key, group key and direct entitlement key.

The CW generator generates control word(CW) in every 5-10 seconds. Since the control word is updated so often, the random function could be used to generate it. The CW is transmitted to receiver side as containing ECM.

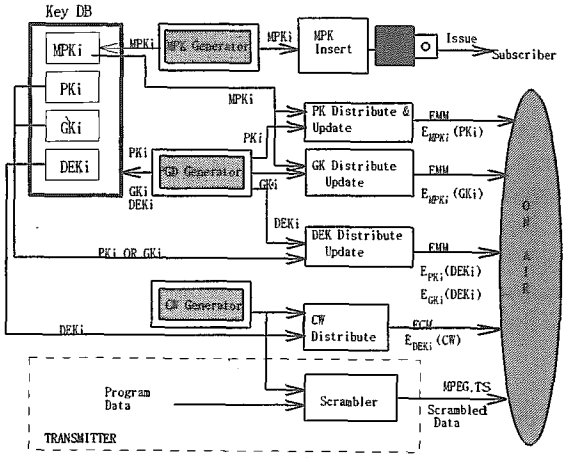


Fig. 5.1 Configuration of Transmitter Sides

5.2 Receiver Side

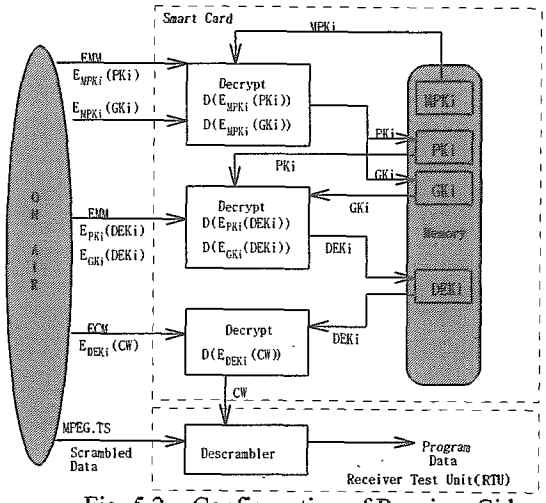


Fig. 5.2 Configuration of Receiver Side

PK and GK can be obtained by decrypting EMM with MPK which is stored in smart card. In order to obtain the DEK, PK and GK are used to decrypt the messages. Similarly, as ECM is decrypted with DEK, CW is obtained. Finally, original source program data can be obtained by descrambling the scrambling data with CW.

6. Conclusion

In this paper, we presented the key distribution and management on Conditional Access System(CAS) on Digital Broadcasting System(DBS). We show overviews of Pay TV system, described in chapter 2. We also describe the characteristics of key on CAS and propose the key management schemes on CAS. In addition, we define the sorts of key and its function to ensure for secure key management and distribution. Some of key generation methods were suggested. We were able to show that the protocol met the requirements of key distribution on CAS. EMM and ECM are used to distribute the several levels of the keys. Finally, the overall system was designed to show the configuration of transmitting side and receiving side. This also describe the scenario of key distribution from transmitting side to receiving side. More features could be updated in future in terms of security. For instance, more stable and random key generation method.

References

[1] H.S.Cho, C.S.Lim, " DigiPass : Conditional Access System of KoreaSat DBS," Journal of Electronics, Vol. 22, No 7, July 1995, pp. 768-775

[2] H.S.Cho, C.S.Lim, " Smart Card for Pay TV," Satellite Communications and Space Industry, Aug. 1995, pp. 58-65

[3] Bruce Schneier, " Applied Cryptography," John Wiley & Sons, Inc., 1994, pp. 129-186

[4] D.E Denning, " Cryptography and Data Security," Reading, MA: Addison -Wesley

[5] Tsubakiyama, Koya, " A study on the scramble key distribution method for conditional access broadcasting," IEICE Japan Workshop in Security and Reliability of Communication Network, March 1995

[6] Akiyama, Tanaka, Nishimura, " Subscriber individual Encryption System for Pay Television Service," Trans. IEICE Japan, B-1, Vol. J75-B-I No. 1, pp. 41-47, Jan. 1992

[7] Hamasaki, " Conditional Access Satellite Broadcasting and Keys Management System," IEICE Japan, Technical Report, ISE91-28, 1991

[8] Nanba, " Information Security in Broadcasting," IEICE Japan, Technical Report, ISEC 89-35, Dec. 1985

[9] Mason, " A Pay-per-view conditional access system for DBS by means of secure over-air credit transmissions having a short cycle time," Proc. of Int. Broadcasting Convention, pp. 282-288, Sep.1984