

# Practical Key Distribution Schemes for Channel Protection

Yu-Lun Huang  
*Department of Computer  
Science and Information  
Engineering,  
National Chiao-Tung  
University, Taiwan*  
ylhuang@csie.nctu.edu.tw

Shiuh-Pyng Winston Shieh  
*Director, Computer and Network Center  
&  
Professor, Department of Computer  
Science and Information Engineering,  
National Chiao-Tung University, Taiwan*  
ssp@csie.nctu.edu.tw

Jian-Chyuan Wang  
*Department of Computer  
Science and Information  
Engineering,  
National Chiao-Tung  
University, Taiwan*  
jcwang@csie.nctu.edu.tw

**Abstract** – This paper presents three key distribution schemes for channel protection. With the proposed schemes, encryption keys of the ordered programs can be distributed to the authorized subscribers efficiently and securely. In these schemes, for key updates, at most two messages are transmitted and simpler computation functions, including one-way hash function and XOR operation, are used to reduce the computation cost compared to existing solutions. With our key distribution schemes, only the authorized subscribers can decrypt the ordered programs. Thus, the service provider in a Pay-TV system can charge his subscribers according to their subscriptions and the intelligent property rights of TV programs can be protected by the proposed schemes.

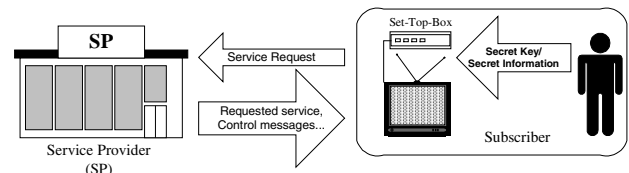
**Index Terms-** Pay-per-view, channel protection, network security, and key distribution scheme

## I. INTRODUCTION

Advance of modern network technologies makes digital distribution of TV programs increasingly popular. To protect TV programs from illicit copying, encryption algorithms are commonly used for channel protection. The encryption keys should be distributed to all subscribers to decrypt the ordered contents. Traditional key distribution

schemes [1-6] result in high computational costs and poor quality of service. To provide real-time services, efficient and secure key distribution schemes are necessary. Figure 1 shows the basic components of a typical Pay-TV system.

The basic components of a Pay-TV system are service providers (SP) and subscribers. Before a subscriber can receive programs from SP, he must first register with the SP and get a secret key and secret information. The secret key is used for subscribing and viewing programs.



**Figure 1. Basic components of a Pay-TV system**

The characteristics of TV programs are: (1) higher data transmission rate, and (2) lower information value [6]. Normally, a scramble function is acceptable for TV channel protection [7]. A scramble function is a high-speed but low-security encryption method compared to other general purpose symmetric key cryptosystems. A program is scrambled to make it unintelligible and only authorized subscribers can get the descramble key/control word (CW) of the scrambled program from the SP. To avoid the illicit guess of these CWs, frequent update of the CWs is

necessary. The secret key and secret information held by subscribers is used for the CWs updates. The secret key and secret information can be stored in a tamper-proof device to avoid disclosure. In addition, to ensure that only the authorized subscribers can descramble the program, the CW is encrypted using other encryption keys, such as authorization keys (AK).

Channels can be classified into two types in Pay-TV system: *subscription channels* and *pay-per-view (PPV) channels* [8-13]. On subscription channels, subscribers subscribe a channel for a period of time while subscribe a program on the PPV channels once a time. In this paper, three low-computational-cost schemes are proposed for channel protection: two for subscription channels, and one for PPV channel protection.

This paper is organized as follows. In Section II, the related works for Pay-TV channel protection are discussed. Then, in Section III, we propose two key distribution schemes to periodically update the encryption keys of the CWs for subscription channels. In Section IV, we propose a key distribution scheme to dynamically update the encryption keys of the CWs for PPV channels. The proposed schemes are compared with the related researches in Section V. And finally, the conclusions are given in Section VI.

## II. RELATED WORK

Hierarchical key management schemes are proposed in ITU Rec. 810 [4] and some real Pay-TV system such as EUROCRYPT [5][6] for channel protection. In these systems, subscription channels are partitioned by content providers. The channels provided by the same content provider use the same distribution key (DK) for authorization key (AK) updates. When AKs need to be

updated, the SP encrypts the new AKs with the corresponding DKs and then transmits the encrypted AKs to subscribers. However, there are no discussions about key distribution on PPV channel protection in ITU standard and EUROCRYPT systems.

W. Lee proposes a key distribution scheme [1] for subscription channels. A four-level key hierarchy is used: *Control Word (CW)*, *Direct Entitlement Key (DEK)*, *Distribution Key (DK)* and *Master Private Key (MPK)*. However, the computation of encryption and transmission in Lee's scheme are too heavy for PPV services.

Tu et al. [2] classified all subscribers are into charging and receiving groups in 1998. In this scheme, subscribers with the same charging period are in the same charging group and subscribers subscribe the same subscription channels are in the same receiving groups. The maximum number of the receiving group in Tu's scheme is the total number of channels and is still a very large number. Besides, key updates in this scheme require large messages. Neither Lee's and Tu's scheme are efficient enough for the periodical and frequent key updates.

## III. KEY DISTRIBUTION SCHEMES FOR SUBSCRIPTION CHANNEL PROTECTION

In this section, two key distribution schemes are proposed for subscription channel protection. These schemes are also a four-level key hierarchy: *Control Word (CW)*, *Authorization Key (AK)*, *Distribution Key (DK)* and *Secret Key (SK)*. The key for each level is used to encrypt the keys for the former level. CW is used to scramble programs on channels. Each channel has a unique CW at a specific time. Vector  $\langle CW \rangle$  denotes the CWs of all channels. The CWs are updated frequently for security.

AK is used to encrypt CW. Each channel also has an AK

at a specific time. Vector  $\langle AK \rangle$  is used to denote the AKs of all channels. SP encrypts the CW using AK and then transmits the encrypted CW to all authorized subscribers. Generally, AKs are update periodically less frequent than CWs. It is usually daily updated because subscribers may be expired from the charging period in the next day.

DK is used to derive AK. Each channel also has a DK at a specific time. Vector  $\langle DK \rangle$  is used to denote the DKs of all channels. DK is designed to reduce messages for AK updates. DKs are usually updated monthly for the basic unit of the charging period is normally one month. SK, the secret key held by the subscriber, is used to encrypt/decrypt the DK. SK is distributed to the subscriber while registering and is used to distribute private messages. SK is hardly changed for it is undisclosed. Keys of the last three levels are never disclosed while CW is used to descramble the program.

## A. Group-Oriented Key Distribution Scheme

Assume that there are  $N$  subscribers, and  $M$  groups of subscription channels. Every subscription group has its own AK and DK. AK is used to encrypt/decrypt the CWs of the channels of the group. DK is designed as secret information to derive the AK. Vector  $\langle DK_{SP} \rangle$  held by the SP is used to generate the vector  $\langle DK_i \rangle$  for each subscriber  $S_i$ . Vector  $\langle AK_{SP} \rangle$  contains the AKs of all subscription groups.  $\langle DK_i \rangle$  is used to derive  $\langle AK_i \rangle$ . In  $\langle AK_i \rangle$ , only the AKs of the subscribed groups equal the corresponding AKs in  $\langle AK_{SP} \rangle$ . Thus, every subscriber can only correctly derive the AKs of the groups he subscribed. In this scheme, AK is derived in ascending order of group identity, regardless of the dependency of groups.

The update procedure of AK consists of two phases: initial phase and update phase. In the initial phase, the SP

generates the vector  $\langle DK_{SP} \rangle$ , and uses  $\langle DK_{SP} \rangle$  to generate  $\langle DK_i \rangle$  for each subscriber  $S_i$ .  $\langle DK_{SP} \rangle$  is also used to derive the AKs of all groups, while  $\langle DK_i \rangle$  of is used to derive the AKs of the subscribed groups for  $S_i$ . In this phase, SP randomly generates  $\langle DK_{SP} \rangle$ , where  $\langle DK_{SP} \rangle = [dk_1, dk_2, \dots, dk_M]$ . For each subscriber  $S_i$ ,

- (1) SP generates the vector  $\langle DK_i \rangle$ , where
  - (i)  $dk_j^i$  is randomly generated for group  $j$ , which is not the subscribed groups.
  - (ii)  $dk_j^i = (dk_1 \oplus \dots \oplus dk_j) \oplus (dk_1^i \oplus \dots \oplus dk_{j-1}^i)$ , if group  $j$  is the subscribed group.
- (2) SP encrypts  $\langle DK_i \rangle$  using the secret key  $SK_i$  of  $S_i$ .
- (3) SP transmits  $\{\langle DK_i \rangle\}_{SK_i}$  to  $S_i$ .

The DKs in  $\langle DK_i \rangle$  are generated in the ascending order of the group. If group  $j$  is subscribed,  $dk_j^i$  is generated to satisfy the formula  $dk_1^i \oplus \dots \oplus dk_j^i = dk_1 \oplus \dots \oplus dk_j$ . Otherwise,  $dk_j^i$  is randomly generated.  $(dk_1 \oplus \dots \oplus dk_j)$  is used to generate the  $ak_j$  for group  $j$ .  $dk_j^i$  is generated to equal  $(dk_1 \oplus \dots \oplus dk_j) \oplus (dk_1^i \oplus \dots \oplus dk_{j-1}^i)$  for deriving correct  $ak_j$ .

In update phase, SP first generates a random number  $R$  and broadcasts  $R$  to all subscribers.  $R$  is use to derive the new AKs. The SP then uses  $\langle DK_{SP} \rangle$  to derive the new  $\langle AK_{SP} \rangle$ , which contains the AKs of all groups. Each subscriber  $S_i$  uses his  $\langle DK_i \rangle$  to derive the new  $\langle AK_i \rangle$ , which contains the AKs of the subscribed groups. When updating AKs, SP randomly generates  $R$  and broadcasts  $(R, h(R))$  to all subscribers:

- (1) SP derives new  $\langle AK_{SP} \rangle$ :
  - (i)  $ak_1 = R \oplus dk_1$  and (ii)  $ak_j = ak_{j-1} \oplus dk_j$ ,  $2 \leq j \leq M$
- (2) On receiving  $R$ ,  $S_i$  checks  $h(R)$  and derives new  $\langle AK_i \rangle$ :
  - (i)  $ak_1^i = R \oplus dk_1^i$  and (ii)  $ak_j^i = ak_{j-1}^i \oplus dk_j^i$ ,  $2 \leq j \leq M$

The new AKs in  $\langle AK_{SP} \rangle$  and  $\langle AK_i \rangle$  are generated in the ascending order of the group identity. For  $S_i$ , if group  $j$  is subscribed,  $ak_j^i$  is derived and is equal to  $ak_j$ , then  $S_i$  can use  $ak_j^i$  to decrypt the CWs of the channels of the

subscribed group  $j$ . To verify the integrity of  $R$ , SP broadcasts  $(R, h(R))$ .  $h(R)$  is treated as a checksum of  $R$ .

## B. Level-Oriented Key Distribution Scheme

Sometimes, channels are partitioned into several levels. A subscriber watches the program of levels lower than the subscribed level. The higher level a subscriber subscribed, the more levels of channels he can receive programs from. In our scheme, channels of the same level use the same AK and DK. The DK of lower level channels can be generated from that of higher level. Whichever the level the subscriber subscribed, only one DK is needed for viewing programs. In this scheme, only one message is broadcast to all subscribers for updating AKs of all levels, which are not higher than the level they subscribed.

The update procedure consists of two phases: initial phase and update phase. If there are  $N$  subscribers and  $M$  channel levels in a Pay-TV system. In the initial phase, SP generates  $\langle DK_{SP} \rangle = [dk_1, dk_2, \dots, dk_M]$ , where

(1)  $dk_1$  is randomly generated

(2)  $dk_j = f(dk_{j-1})$ ,  $2 \leq j \leq M$

For each subscriber  $S_i$ , SP transmits  $\{\langle DK_i \rangle\}_{SK_i}$  to  $S_i$ , where  $\langle DK_i \rangle = [dk_k]$ , for  $L_k$  is the subscribed level for  $S_i$ . Upon receiving  $\langle DK_i \rangle$ ,  $S_i$  derive  $[dk_{k+1}, \dots, dk_M]$ , where

$$dk_j = f(dk_{j-1}), k+1 \leq j \leq M.$$

In this scheme,  $dk_j$  is generated from  $dk_{j-1}$  using one-way function,  $f()$ . Only the DK of higher level can derive that of the lower level. Besides, only one DK is needed for receiving programs of all subscribed channels. In update phase, a new  $\langle AK_{SP} \rangle$  is generated by  $\langle DK_{SP} \rangle$ . Only one  $R$ ,  $\{AK_{\text{lowest\_level}}\}DK_{\text{lowest\_level}}$ , is broadcast to all subscribers. Each subscriber  $S_i$  uses his  $\langle DK_i \rangle$  to derive the new  $\langle AK_i \rangle$  that contains the AKs of the levels not higher than the subscribed level. In this phase, SP

generates  $\langle AK_{SP} \rangle = [ak_1, ak_2, \dots, ak_M]$ , where

(1)  $ak_1$  is randomly generated.

(2)  $ak_j = \{dk_{j-1}\}_{dk_{j-1}}$ ,  $2 \leq j \leq M$

SP broadcasts  $(R, h(R))$  to all subscribers, where  $R = \{ak_M\}_{dk_M}$ . After receiving  $(R, h(R))$ ,  $S_i$  verifies  $h(R)$  and derives new  $\langle AK_i \rangle = [ak_k, ak_{k+1}, \dots, ak_M]$ , where

(1)  $ak_M = \{R\}_{dk_M}^{-1}$

(2)  $ak_j = \{ak_{j+1}\}_{dk_{j+1}}^{-1}$ ,  $k \leq j < M$

For SP, the new AKs in  $\langle AK_{SP} \rangle$  are generated in the descending order of level  $j$ . For each subscriber  $S_i$ , the new AKs in the  $\langle AK_i \rangle$  are derived in the ascending order of level  $j$ . That is,  $ak_{j-1}$  is derived from  $ak_j$  by decrypting  $\{ak_j\}_{dk_j}$  using  $dk_j$ . The number of levels of AKs a subscriber can derive depends on the level he subscribed. Only the DK of the subscribed level is held for generating DKs of levels lower than the subscribed one.

## IV. KEY DISTRIBUTION SCHEME FOR PAY-PER-VIEW CHANNEL PROTECTION

On PPV channels, programs are broadcast according to the subscription requests. In this scenario, subscribers may request the same video program simultaneously. The join and leave actions occur frequently during the playback period. Without privilege revocation, the left subscribers can keep watching the programs without payment. To help alleviate this problem, a dynamic key distribution scheme for AK update is proposed.

The proposed scheme for PPV channel protection also uses four-level key hierarchy: *Control Word (CW)*, *Authorization Key (AK)*, *Dynamic Secret Set (DSS)* and *Secret Key (SK)*. The key for each level is used to encrypt the key for the former level. DSS is dynamically assigned when requesting for subscription. In PPV scheme, subscribers dynamically keep secret information for driving new AK

when other subscriber leaves. With the secret information, no keys are needed to be sent for privilege revocation.

In this scheme, when subscriber  $S_i$  joins, SP randomly generates a secret information  $P_i$  for all subscribers except  $S_i$ . Then, SP transmits  $\{S_i \text{ Join}, P_i\}_{AK}$  to all subscribers except  $S_i$ , updates new AK to  $AK_{new}=AK \oplus P_i$  and transmits  $\{AK_{new}, P_1, P_2, \dots, P_{i-1}\}_{SK_i}$  to  $S_i$ . If there are  $n$  subscribers viewing the same program, SP randomly generates  $n$  secrets,  $P_1, P_2, \dots, P_n$  when join. Each subscriber keeps all secrets except the one generated when he joined. When  $S_j$  leaves, SP broadcasts  $\{S_j \text{ Leave}\}_{AK}$  to all subscribers, updates new AK to  $AK_{new}=AK \oplus P_j$  and discards  $P_j$ . Since  $S_j$  doesn't know  $P_j$ , he cannot derive  $AK_{new}$  after leaving.

## V. COMPARISON

In this section, the number of transmitted messages and the cost of computations are discussed. Table 1 shows the number of message transmitted and the cost of computation for AK updates. When update is needed, SP encrypts the new AKs with the corresponding DKs and then transmits the encrypted AKs to subscribers. Therefore, the number of encrypted message and the number of the transmitted message equal the number of channel groups.

**Table 1. Comparison of message transmitted.**

	Subscription Channels	Pay-Per-View Channels	
	Update operations	join	Leave
Eurocrypt	p/p (encrypt)	N/A	N/A
Lee	m/m (encrypt)	N/A	N/A
Tu	m/m (encrypt)	1/1 (encrypt)	1/1 (encrypt)
Our scheme	Group 1/p (XOR)	2/2 (encrypt)	1/1 (XOR)
	Level 1/q (encrypt)	1 (XOR)	

**m:** # of subscriber groups; **p:** # of channel groups; **q:** # of channel levels

In Lee's scheme, only subscription channel protection is discussed. Subscribers in the same group use the same DK to update AKs. When AKs need to be updated, the SP

encrypts the new AKs with the DK of each subscriber group respectively and then transmits to the subscribers. Therefore, the number of message encryption and the number of message transmissions are equal to the number of the subscriber groups.

In Tu's scheme, subscribers are grouped by subscribed channels. The subscribers in the same group use the same DK for AK updates. Therefore, the number of encrypted message and of transmitted message equal the number of the subscriber groups. For PPV, SP uses the subscribers' SKs to distribute AKs. When a subscriber leaves, the SP encrypts the new AK with other subscribers' SKs and transmits it for privilege revocation. Thus, the number of encrypted message and of transmitted message equal the number of subscribers.

In our group-oriented scheme, only one random number is broadcast to all subscribers for AK updates. Each subscriber derives the AKs of all subscribed channel groups using the vector of DK and the random number. Only XOR function is performed to derive the AKs. In addition, the cost of computation equals to the number of channel groups, which is fewer than the number of the subscriber groups in Lee's and Tu's scheme.

In our level-oriented scheme, only one message is broadcast to subscribers for AK updates. Each subscriber can derive the AKs of the levels lower than the subscribed one. To generate the AKs of all channel levels, the number of message encrypted equals that of the channel levels, and is also less than that in Lee's and Tu's scheme.

In PPV key distribution scheme, each subscriber keeps all randomly generated secrets except the one generated when he joins. When a subscriber joins, the SP encrypts the new AK and the secrets generated before with the subscriber's SK, and then transmits to the subscriber. The SP also encrypts the new secret with the current AK, and

then broadcasts to subscribers watching the same program for AK update. Although one more encryption and transmission is needed when joining, only one message is transmitted for privilege revocation. In additions, only XOR function is used for deriving the new AK.

## VI. CONCLUSION

In this paper, three key distribution schemes are proposed for Pay-TV channel protection. The group-oriented and level-oriented key distribution schemes are used for subscription channel protection, and the dynamic key distribution scheme is used for PPV channel protection. Compared with the existing solutions, fewer messages are transmitted and simpler computing functions are used in our schemes.

With our schemes, only the authorized subscribers can view the subscribed programs and SP can charge the subscribers according to their subscriptions. Thus, the illicit viewing of TV programs can be avoided by the proposed key distribution schemes.

## REFERENCES

- [1] W. Lee, "Key Distribution and Management for Conditional Access System on DBS," Proceedings of International Conference on Cryptology and Information Security, pp. 82-86, 1996.
- [2] F. K. Tu, C. S. Laih and S. H. Toung, "Key Distribution Management for Condition Access System on Pay-TV System," Proceedings of the 8<sup>th</sup> National Conference on Information Security, pp. 369-387, 1998.
- [3] H. Sakakibara, et al. "The ID-based Non-interactive Group Communication Key Sharing Scheme using Smart Cards," Proceedings, International Conference on Network Protocols, pp. 91-98, 1994.
- [4] ITU Rec. 810, 1992
- [5] E. Cruselles, J. L. Melus and M. Soriano, "An Overview of Security in Eurocrypt Conditional Access System," IEEE Global Telecommunications Conference, vol. 1, pp. 188-193, 1993.
- [6] B. M. Macq and J. J. Quisquater, "Cryptology for Digital TV Broadcasting," Proceedings of the IEEE, 83(6), pp. 944-57, June 1995.
- [7] W. H. Kim, K. J. Chen and H. S. Cho, "Design and Implementation of MPEG-2/DVB Scrambler Unit and VLSI Chip," IEEE Transaction on Consumer Electronics, 43(3), pp. 980-985, August 1997.
- [8] T. D. C. Little and D. Venkatesh, "Prospects for Interactive Video-on-demand," IEEE multimedia, pp. 14-23, Fall 1994
- [9] L. Golubchik, C. S. Lui and R. Muntz, "Adaptive Piggyback: A Novel Technique for Data Sharing in Video-on-demand Storage Servers," Multimedia Systems, 4(3), pp. 140-155, 1996
- [10] H. Woo and C. K. Kim, "Multimedia Scheduling for VOD Services," Multimedia Tools and Applications, 2(2), pp. 157-71, March 1996.
- [11] K. C. Almeroth and M. H. Ammar, "The Use of Multicast Delivery to Provide a Scalable and Interactive Video-on-demand Service," IEEE Journal on Selected Areas in Communications, 14(6), August 1996.
- [12] S. Viswanathan and T. Imielinski, "Metropolitan Area Video-on-demand Service Using Pyramid Broadcasting," Multimedia Systems, 4(4), pp. 197-208, 1996.
- [13] L. S. Juhn and L. M. Tseng, "Staircase Data Broadcasting and Receiving Scheme for Hot Video Service," IEEE Transaction on Consumer Electronics, 43(4), pp. 1110-1117, November 1997.

