Using a New Structure in Group Key Management for Pay-TV

Shih-Ming Chen[1], Ching-Rong Yang[1], and Min-Shiang Hwang[1,2]
(Corresponding author: Min-Shiang Hwang)

Department of Computer Science and Information Engineering, Asia University[1]
No. 500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan
(Email: mshwang@asia.edu.tw)
Department of Medical Research, China Medical University Hospital, China Medical University[2]
No. 91, Hsueh-Shih Road, Taichung 40402, Taiwan
(Received May 17, 2015; revised and accepted Aug. 21 & Sept. 8, 2015)

Abstract

This paper studies a key management problem for a conditional access system with a control word, an authorization key, a distribution key and the master private key. Using a new key store structure and multiple select groups, we can reduce the memory request size and update time. This problem is considered with a large memory for a matrix of group key store structure of four key distributions, and only one group has select right of four key distributions in a free select channel.

Keywords: Conditional access system (CAS), pay-TV, key management, four-key distribution

1 Introduction

Pay-TV is the best business way to distribute a mass of information program to a large number of people simultaneously. Because of already established free payment by users, television has become a widespread communications medium. A Pay-TV system channel provider charges the subscriber fee for receiving the broadcasting program. In real business applications, a Pay-TV system can be a digital broadcasting system (DBS) [3, 14], or a digital cable TV system such as the local cable TV system (CATV) [7, 11]. In an industry society, scheduled programming does not always offer what television receivers desire. Therefore, additional video services provided by CATV network have enjoyed enormous successes during the last decade. A Pay-TV system has many broadcasting channels to provide its subscriber, and these channels can be classified into two classes [15, 20]. The first kind of channel is the basic channel available to all the subscribers of the system. Second kind of channel is the pay-channel that charges the subscriber for the receiving fee. The pay-channel can be classified into two subclasses (See Table 2). The first subclass is Pay Per Channel (PPC) [18], receiving fee for each channel counted according to a time unit. Second subclass is Pay Per View (PPV) [2, 5], counted for each program.

Table 1: The class of broadcasting channels

program	Subscription	PPV	Fee
Basic subscriber	×	×	√
PPC subscriber	√	×	√
PPV subscriber	√	√	√

Where, ×: has no viewing right; √: has viewing right. From Table 1, there exist a lot of charge fee problems on CATV. In technology, registered subscribers could be sufficiently authorized by taking advantage of conditional-access system (CAS) reference upon table [6, 12, 17]. It can follow upon table to permit only the authorized subscribers to watch the CATV program. Thus, CAS constructs a key distribution and management rule for Pay-TV services. The management rules include encryption and decryption keys to refresh those keys periodically and then distribute those keys to authorized subscribers secretly so that unauthorized receivers cannot get the correct keys [13].

This paper is organized as follows: Section 2 discusses a secure message module. Section 3 discusses the basic key for CAS management. Section 4 discusses the proposed key distribution models. Section 5 discusses proposed store structure of the key distribution model and multiple select group police. Section 6 concludes the paper.

2 Secure Message Module

Between the transmitters and receivers, these have two secure message modules multiplexed with the signal itself.

These two modules are introduced as follows:

1) Entitlement Control Module:
The Entitlement control module is a route Entitlement Control Message (ECM) to microprocessor of the smart card of set-top-box (STB) [1, 8] with the received control parameters. If passing the comparison, authorized receivers can decrypt control word (CW) by an authorized key in the smart card. Thus, the ECM consists of an access parameter and enciphered CW.

2) Entitlement Management Module:
The Entitlement Management Message (EMM) [19] carries the information of the receiving program to the STB. The Entitlement management includes access rights and updates the AK for the channel subscriber. Mail or a specific channel without the program simultaneously in a batch process can transfer this EMM.

3 Basic Keys

We will describe four elements about CAS management subscriber and key distribution in this section. We discuss their characteristics about control word, authorization key, group key, and master private key for CAS control.

1) Control Word:
It is used to scramble and descramble broadcasting programs in each charged channel. Each charged channel has a unique control word (CW). Thus, n charge channels have $cw_1 \sim cw_n$. The control word should be updated within a short time period of 5-10 seconds.

2) Authorization Key:
It is used to encipher the control word and access the ECM. Each charged channel has a unique Authorization key. Thus, n charge channels have $AK_1 \sim AK_n$. The control word should be updated within a day or month period of time.

3) Group Key:
It is used to encipher the authorization key. Each charge group and receive group have a unique group key [4, 9]. Thus, i charge groups and j receive groups have $RGK_1 \sim RGK_{ij}$. The row of group key should be updated once per month. One row of group key should be updated once per day. Therefore, each row is updated per month. In Tu et al.'s propose, the group key of four-level key management uses a matrix to store [16].

4) Master Private Key:
It is used to encipher the group key and is unique store in the smart card for each subscriber. Each Master Private Key (MPK) is never charged during the life cycle of the smart card. Thus S subscribers have $MPK_1 \sim MPK_s$.

4 Relate Key Distribution Models

There are many proposed schemes for charge-fee programs of Pay-TV at last. That key management is to use a hierarchy key management method in the proposed scheme. In this section, we will discuss briefly about proposed key distribution models' shortcoming. We assume S subscribers and C channels in Pay-TV system. It will be basic assume in follow methods.

4.1 Two-Key and Three-Key Distributions

The two-key scheme uses an MPK to distribute CW. Thus, The CAS needs to compute CW of every charge channel using only subscribers' MPK. There is $S \times C$ message-packages encrypted and broadcasting within 5 to 20 seconds. In real application, Pay-TV may have hundreds of channels and millions of subscribers. The total broadcasting message package will to be huge load for CAS. The profit of this scheme is simple to implement. But it is not suitable for a large Pay-TV system.

The three-Key distribution scheme [10] is focused on two Key distribution shortcomings. It will reduce a huge load in every update and retransmission. The scheme adds AK between in CW and MPK. The AK is a time variant and unique in every channel. The system encrypts the CW by using the AK. The AK is encrypted by the MPK. The AK is updated every month. Therefore, Total CW only uses S times to encrypt and retransmission message package within 5 to 20 seconds. However, it must refresh AK about $S \times C$ every month. It will be a huge load system in one day of every month. Therefore, the scheme is not suitable for a large system. It is only suitable for a PPV program with a few of channels and few of subscriber.

4.2 Four-key Distribution

We will describe two schemes about Tu et al. [16]. The proposed scheme for CAS management subscribers and key distributions in this section. We will discuss their characteristics and flow about the key transform, encrypted and decrypted for CAS control.

4.2.1 Simple Model

The scheme development is focused on three Key distribution shortcomings. It will reduce a huge load in every update and retransmission. The scheme adds RGK between in AK and MPK. The RGK is a time variant and unique in each receiving channel group. The system encrypts the CW by using the AK. The AK of channels in same receiving channel group is distributed by RGK. The

receiving channel group by combining those authorizations keys together is encrypted by RGK of this group. The AK and RGK are updated periodically about one month. The EMM package includes encrypted AK and RGK. The scheme assumes N receiving group for classifications of subscribers. Define the receiving group key matrix as follows.

$$RGK = [rgk_1, rgk_2 \cdots rgk_N]$$

Thus, it must refresh Aks of channels about $S \times C$ to $S + N$ in every month. It will reduce a huge load system in one day each month, so the scheme is not suitable for a dynamic system.

4.2.2 Complete Model

The four-key complete model architecture is used to implement the CAS to provide PPC service for a Pay-TV dynamic key management system. The scheme is focused on a simple model and a charge group for dynamic key management. Therefore, it combines two assuming M charging groups and N receiving groups for the classifications of subscribers. The set S of all subscribers of the system is classified into $M \times N$ classes of the disjoint subscribing class s_{ij} where $1 \leq i \leq M$, $1 \leq j \leq N$:

$$S = \begin{bmatrix} s_{11} & s_{12} & \cdots & s_{1N} \\ s_{21} & s_{22} & \cdots & s_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ s_{M1} & s_{M2} & \cdots & s_{MN} \end{bmatrix}$$

Each row of S matrix is the same charging groups and each column of S matrix is the same receiving groups. Thus, we can mirror to the receiving group key matrix (RGK) as following:

$$RGK = \begin{bmatrix} rgk_{11} & rgk_{12} & \cdots & rgk_{1N} \\ rgk_{21} & rgk_{22} & \cdots & rgk_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ rgk_{M1} & rgk_{M2} & \cdots & rgk_{MN} \end{bmatrix}$$

The receiving group key is unique for each subscribing class in S matrix. Therefore, we can easily understand rgk_{ij} is the receiving group key of the subscribing class s_{ij}. Each row of RGK matrix is refreshed in a day each month. And each key of column of each row of RGK matrix is encrypted with each subscriber's MPK of s_{ij}. The AKs of PPC channels are updated daily. The AKs of PPV channels are updated per program. Therefore, any subscriber that is out of authorization date will not receive the renewed keys in RGK, so they would not be able to watch programs. If a new subscriber is added to the system, the subscriber must follow the above rule to be classified into a receiving group key class and broadcasted to the new subscriber. If one subscriber wants to move into a new receive class for-vacation, and the CAS wants to delete the subscriber from a receiving class, the receiving group key of this class should be updated and re-broadcast to other subscribers within this class. The moved subscriber without the new receiving group key cannot get the AK and loses the receiving authentication.

5 The Propose Scheme

We propose a new key store structure and multiple select group police for a key distribution scheme from the complete model of four-key distribution. Because the four-key distribution is a good scheme for the key distribution of PPC channels. However, it uses two matrixes of a very large size of memory to store receive and charge a group key and the group of all subscribers. Because the system may have millions of subscribers and hundreds of channels, the potential amount of group to be classified is very large for store receiving group key and the group of all subscriber information in the free selective channel police. These large matrixes have a lot of empty space because subscribers have the same selecting channels or CAS supporter offers channels of discount for a viewing group. We propose a new structure and multiple-select group police to solve a waste of memory space. There are two kinds of structures presented for store key and one new multiple select group police as follows.

5.1 Link-List Structure for a Group Key

In Tu et al.'s proposed scheme is to use two matrices to store a receiving group key and the group of all subscribers. It let matrices have many empty spaces for selecting. First, we propose a new store structure that is the receiving group key Link-List to replace a receiving group key matrix as shown in Figure 1.

$LL_1 \sim LL_M$ charge a group and $N_1 \sim N_M$ receiving group, but $N_1 \sim N_M$ may be not equal. Because it only stores a subscribed group that has an empty space to waste, the scheme refreshes one Link-List daily, and each Link-List is refreshed once per month. The other thing is the same as Tu et al.'s complete model of four-level key distribution. It assumes the CAS has C channels, S subscribers, M charge group and N receiving group. If CAS supports free-select channel police for subscribers, we can easily obtain MAX$M = 31$ and $N = 2^C - 1$ in Tu et al.'s complete model. Thus, In Tu et al.'s matrixes, the complete model of four-key distribution model will request $31 \times 2^C - 1$ memory space for receiving group key matrixes. The system may have millions of subscribers and hundreds of channels, so the potential amount of group to be classified is very large to store a receiving group key and the group of all subscriber information in free-selective channel police. We only needs $2 \times M \times N$ memory in my proposed structure. We can easily obtain $1 \leq M \leq 31$, $1 \leq N \leq 2^C - 1$ for Link-List structure. In the worst, Link-List structure is equal to the matrix for memory request. In Link-List structure scheme, this problem never happens. The scheme can solve the draw-

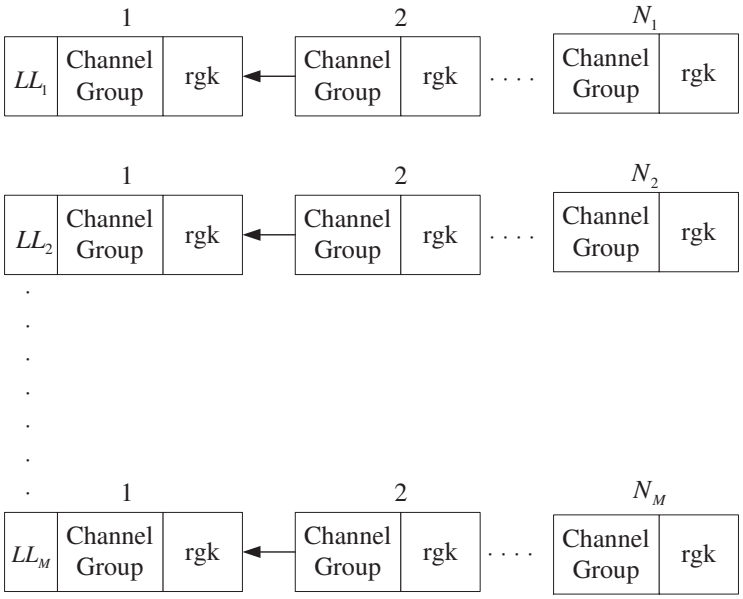

Figure 1: Link-List structure

back of the Tu et al.'s of four-levels key distribution that needs a very large system memory for a group key store matrix.

5.2 Array Structure for Subscribers

The structure is focused on all subscribers of the system for a store matrix. It let a matrix have many empty spaces to waste for subscribers. We propose one array structure to replace the matrix of all subscribers of the system as shown in Table 2. We assume the CAS has N receiver group, M charge group, L Link-List point address memory length and S subscribers. If CAS supports free-select channel police for subscribers, we can easily obtain MAX$M = 31$ and $N = 2^C - 1$ in Tu et al.'s complete model. In Tu et al.'s matrix of the complete model of a four-key distribution model will request $31 \times 2^C - 1$ memory space for the matrix of all subscribers in the system. We only need $S \times L$ memory space in my propose array structure. Thus, we can easily obtain $S \times L$ ¡ $31 \times 2^C - 1$. Let assume CAS have 10000 subscribers, and 4 bytes of memory for Link-List point address and 100 channels. We need $31 \times 2^{100} - 1$-matrix memory for Tu et al's proposed scheme. However, we can reduce memory request from $31 \times 2^{100} - 1$ down to 10000×4 for the array structure.

Table 2: Array structure

Subscriber	Link-List Point Address
⋮	⋮

5.3 Multiple Select Group Police

The scheme is focused on defining select group police for subscribes in all select possibly. In free-select channel police, that will request $31 \times 2^C - 1$ memory requests for the receiving group key of any methods. When this happen, we can choose the multiple select group police to reduce memory request.

The multiple select group police must be deleted including group of many channels that are replaced with some group of minor channel in CAS. However, it lets subscribers can multiple select channel group their want. It means that they can use multiple select to obtain one equal to old one group including many channels. When we use this police, the N receiver group is less than $2^C - 1$ receiver group. If CAS has 4 channels for subscribers to choose, we have 15 kinds of receiver groups for choice. And that will request 31×15 memory spaces for free-select channel police in worst time, if each subscriber selects including 4, 6, 7, 8 channels group to watch TV. However, we can choose two groups, 4, 6 and 7, 8, for multiple select group police. Therefore, receiver group including 4, 6, 7, 8 channels must to be deleted to reduce memory space request. If we can find so many this state and delete this receiver group, it will reduce many memory requests in any methods.

6 Conclusions

Efficient compression and modulation techniques have been implemented for a large-scale Pay-TV broadcasting. It uses a kind of key distribution and management for Pay-TV charge fee. We have discussed above many key distribution models for Pay-TV. We can find three-key distribution model is suitable for PPV programs, and

four-key distribution model is suitable for PPC programs for the no-free-select channel application environment.

We have proposed two schemes and one police are Link-List structure, array structure and multiple select police for memory space reduced. In fact, the conditional access control system can allow the Pay-TV for a free-select channel that is subscribers' wish and trend of the time. Thus, we apply the new structure and police for a four-key architecture of CAS to a Pay-TV. Originally, we can use Tu et al.'s four-key distribution architecture to implement, but under the consideration of memory matrix, the Link-List and array structure of four-key architecture are employed. Of course, we can obtain two profit and one shortcoming in my proposed scheme as follow.

Profit:

- The scheme only uses a minimum memory for CAS in Link-List and array structure of a four-key distribution scheme.
- It can select multiple channels in multiple select group police for CAS.

Shortcoming:

- It needs a more complex algorithm than Tu et al.'s complete model of a four-key distribution scheme.

All these issues are emerging; making Tu et al.'s complete model of a four-key distribution scheme concept is good than other proposed schemes. However, Tu et al.'s scheme has two shortcomings that requests a large memory in a complete scheme and lack multiple select groups for a free-select channel in CAS. The scheme we propose can solve these two shortcomings.

Acknowledgements

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: MOST 103-2221-E-468 -026, NSC 103-2622-E-468-001-CC2, and NSC 103-2622-H-468-001-CC2.

References

[1] N. Anwar, I. Riadi, A. Luthfi, "Forensic SIM card cloning using authentication algorithm," *International Journal of Electronics and Information Engineering*, vol. 4, no. 2, pp. 71–81, 2016.

[2] H. W. Chi, G. L. Li, M. J. Chen and J. R. Lin, "Efficient computation allocation algorithm for multi-view video coding," *International Journal of Electronics and Information Engineering*, vol. 3, no. 2, pp. 91–106, 2015.

[3] S. J. Crowley, *Capacity Trends in Direct Broadcast Satellite and Cable Television Services*, National Association of Broadcasters, Oct. 8, 2013. (`http://www.nab.org/documents/newsRoom/pdfs/100813_Capacity_Trends_in_DBS_and_Cable_TV_Services.pdf`)

[4] Z. Eslami, M. Noroozi, and S. K. Rad, "Provably secure group key exchange protocol in the presence of dishonest insiders," *International Journal of Network Security*, vol. 18, no. 1, pp. 33–42, 2016.

[5] D. L. Garcia, A. Nebot, A. Vellido, "Visualizing pay-per-view television customers churn using cartograms and flow maps," in *Proceedings of 21st European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning (ESANN'13)*, pp. 567–572, 2013.

[6] D. He, N. Kumar, H. Shen, J. H. Lee, "One-to-many authentication for access control in mobile pay-TV systems," *Science China Information Sciences*, pp. 1–14, Apr. 13, 2016.

[7] D. Hunter, J. Coder, J. Ladbury, "Effects of LTE signals on cable TV devices," in *2014 United States National Committee of URSI National Radio Science Meeting (USNC-URSI NRSM'14)*, 2014.

[8] J. Kim, E. S. Jung, Y. T. Lee, W. Ryu, "Home appliance control framework based on smart TV set-top box," *IEEE Transactions on Consumer Electronics*, vol. 61. no. 3, pp. 279–285, 2015.

[9] A. Kumar and S. Tripathi, "Anonymous ID-based group key agreement protocol without pairing," *International Journal of Network Security*, vol. 18, no. 2, pp. 263–273, 2016.

[10] J. W. Lee, "Key distribution and management for conditional access system on dbs," in *Proceedings of International Conference on Cryptology and Information Security*, pp. 82–88, 1996.

[11] R. Li, N.K. Chung, K.T. MO, D.M. Fisher, and V. Wong, "A flexible display module for dvd and set-top-box applications," *IEEE Transactions on Consumer Electronics*, vol. 43, no. 2, pp. 496–503, 1997.

[12] Y. Liu, X. Yang, H. Yao, and W. Gao, "Novel secure communication protocol for conditional access system," *International Journal of Network Security*, vol. 5, no. 2, pp. 121–127, 2007.

[13] B. M. Macq, J. J. Quisquater, "Cryptology for digital tv broadcasting," *Proceedings of the IEEE*, vol. 83, pp. 944–957, June 1995.

[14] H. Y. Seo, B. Bae, J. D. Kim, "Transmission model for next-generation digital broadcasting systems," in *International Conference on Information Networking (ICOIN'15)*, pp. 379–380, 2015.

[15] C. Y. Sun and C. C. Chang, "Cryptanalysis of a secure and efficient authentication scheme for access control in mobile pay-TV systems," *International Journal of Network Security*, vol. 18, no. 3, pp. 594–596, 2016.

[16] F. K. Tu, C. S. Laih, H. H. Tung, "On key distribution management for conditional access system on pay-tv system," *IEEE Transactions on Consumer Electronics*, vol. 45, pp. 151–158, Feb. 1999.

[17] R. Varalakshmi, V. R. Uthariaraj, "Huffman based conditional access system for key distribution in digital TV multicast," *Multimedia Tools and Applications*, vol. 74, no. 9, pp. 2899–2912, May 2015.

[18] Z. Wan, J. Liu, R. Zhang, R. H. Deng, "A collusion-resistant conditional access system for flexible-pay-per-channel pay-tv broadcasting," *IEEE Transactions on Multimedia*, vol. 15, no. 6, pp. 1353–1364, 2013.

[19] J. Wei, J. Liu, Y. Liu, C. Wei, "A novel entitlement management message distribution for conditional access system," in *Proceedings of 1st International Symposium on Computer Network and Multimedia Technology (CNMT'09)*, pp. 1–4, 2009.

[20] X. Zhao and F. Zhang, "A new type of ID-based encryption system and its application to pay-TV systems," *International Journal of Network Security*, vol. 13, no. 3, pp. 161–166, 2011.

Shih-Ming Chen received the B.S. degree in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 1999; the M.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 2003. He is currently pursuing his PhD degree in Computer Science and Information Engineering from Asia University. His current research interests include information security and Science & Technology of Chinese studies.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished Research Awards of the National Science Council of the Republic of China. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.