Efficient Key Distribution Schemes for Secure Media Delivery in Pay-TV Systems

Yu-Lun Huang, Shiuhpyng Shieh, *Senior Member, IEEE*, Fu-Shen Ho, and Jian-Chyuan Wang

***Abstract*—To provide secure media delivery in pay-TV systems, a large number of messages are exchanged for key updates in the conventional key distribution schemes. This is inefficient and costly when the client side (set-top box) uses a smart card with limited computing power. In this paper, we present three key distribution schemes for channel protection and secure media delivery in pay-TV systems. With the proposed schemes, encryption keys of the subscribed programs can be efficiently and securely distributed to the authorized subscribers. Only one message is needed to renew key in the key distribution schemes for subscription channel protection. In addition, we use simpler computation functions, including one-way hash function and exclusive-OR operation, for key updates to reduce the computation cost. With our key distribution schemes, only authorized subscribers can watch the subscribed programs correctly. Unauthorized subscribers have no information to retrieve the correct programs over the networks. Thus, service providers can charge their subscribers according to their subscriptions, and the illegal access of the media and video programs from networks can be prevented, based on the proposed schemes.**

***Index Terms*—Channel protection, conditional access system, key distribution scheme, secure media delivery.**

I. Introduction

THE ADVANCE of modern network technologies has made digital video broadcasting available throughout the world. Broadcasters and media service providers introduce the conditional access systems (CAS) for pay channels and transfer the burden of paying for subscribed media and video programs to the viewers. Charges for pay/encrypted channels should be paid by viewers at rates chargeable by content providers based upon hours of watching per set-top box. The pay-TV service provider who covers cost of collection and remittance should retain a portion of such receivables.

To ensure the access rights of the authorized subscribers who pay for the content watched and prevent media/video programs from unauthorized access, scramble and encryption algorithms are commonly used for secure media delivery and channel protection. The encryption keys should be distributed to all subscribers so that they can receive and decrypt the subscribed video programs or media streams. For large amounts of subscribers in a conditional access system, traditional key distribution schemes [1]–[6] result in high computational costs and poor quality of service. To provide real-time video services, an efficient and secure key distribution scheme is a necessary and important requirement. Fig. 1 shows the basic components of a typical pay-TV system.

A conditional access system is an essential system to facilitate the charge for video subscription in a pay-TV system. Existing conditional access TV modes are [4]

- Subscription channel: a subscriber subscribes a channel for a period of time.
- Pay-per-view (PPV) channel: a subscriber pays for each single program.

The basic components in a CAS in pay-TV system are a service provider (SP) and large amount of subscribers. Before receiving video programs from the service provider, a subscriber must first register with the service provider and get his own secret key and along with other secret information. For the reasons of higher transmission rate, lower information value, and security requirements [6], a scrambling/descrambling function is usually used for channel protection in CAS [7]. A scramble function scrambles the video programs by modifying the synchronization part or the active part of the video signal, or by altering the audio waveform with the help of a pseudo-random sequence. The scramble keys/control words (CW) initialize the generation of the pseudo-random sequence. The descramble function recovers the original video programs at the receivers with the help of the CW and the pseudo-random sequence. Generally, the scramble and descramble functions are higher speed and lower security strength encryption methods compared to other general purpose symmetric key cryptosystems [8]–[10].

Before transmission, video programs are scrambled to make it unintelligible. Only the authorized subscribers can receive the CW of the scrambled program from the SP. To avoid the illicit guess of these CWs, we can enforce a strong encryption mechanism on the access control data (e.g., CWs). Furthermore, we should also update the CWs frequently enough (e.g., 5–20 s) to minimize the risk of key compromising attack. The secret key and secret information held in the subscriber's smart card could be used to prevent the renewed CWs from being altered during its transmission over the networks. Since a smart card is a tamper-proof device, the secret key and secret information held in the smart card will not be disclosed anytime.

On designing key distribution schemes in a broadcasting system, the compromise of a single key should not result in the compromises of the subsequent keys. Besides, the conspiracy

Manuscript received June 22, 2000; revised March 6, 2002. This work was supported in part by Ministry of Education, National Science Council of Taiwan, R.O.C., and by the Lee & MTI Center, National Chiao-Tung University, Hsinchu, Taiwan. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Minerva Yeung.

The authors are with the Department of Computer Science and Information Engineering, National Chiao-Tung University, Hsinchu 30050, Taiwan, R.O.C. (e-mail: ylhuang@csie.nctu.edu.tw, ssp@csie.nctu.edu.tw; fsho@csie.nctu.edu.tw; jcwang@csie.nctu.edu.tw).

Digital Object Identifier 10.1109/TMM.2004.834861

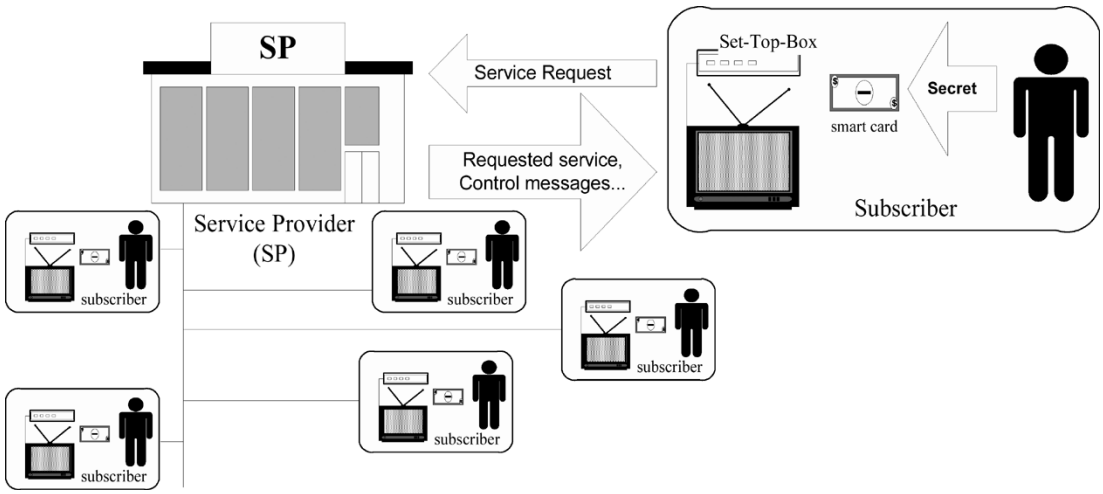

Fig. 1. Basic components of a typical pay-TV system.

of subscribers should not compromise the system, either. Third, the time, computation power, and transmission cost required for key updates should be deterministic in a real-time broadcasting system.

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, two key distribution schemes for channel protection are discussed. Then, in Section III, we propose two key distribution schemes that can 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. These proposed schemes are compared with the related research in Section V. Finally, the conclusions are given in Section VI.

II. Related Work

In this section, we discuss the past work related to the key distribution schemes proposed for conditional access systems in pay-TV systems. In 1992, hierarchical key management schemes were proposed in ITU Recommendation 810 [4], in which a three-level key hierarchy is defined: Control Word (CW), Authorization Key (AK), and Distribution Key (DK). CW is used to initialize the generation of a pseudo-random sequence for scrambling/descrambling of video programs. AK is used to encrypt the CW for each subscriber. DK is used to securely transmit the AK and the entitlement messages corresponding to the subscribed video program. However, the transmission of DK is not discussed in ITU recommendation. The revealment of DK results in the compromise of AK when updating the AK.

As an improvement, some pay-TV systems, such as Eurocrypt conditional access systems [5], [6], use one more level of key hierarchy than the ITU recommendation [4] for channel protection: the Unique Key (UK). UK is used to transmit the DK securely. UK is unique to each subscriber, and is directly distributed to the subscriber upon registration. In Eurocrypt conditional access systems, subscription channels are grouped according to their content providers. Channels in the same group use the same DK for AK updates. When AKs need to be updated, the service provider encrypts the new AKs with the corresponding DKs and then transmits the encrypted AKs to all authorized subscribers. However, the way for key distribution in PPV channel is not discussed in Eurocrypt conditional access systems. In other words, video programs in PPV channels are not protected in these systems.

In 1996, J. W. Lee proposed a key distribution scheme [1] for subscription channels. A four-level key hierarchy is used in Lee's scheme: CW, Direct Entitlement Key (DEK), DK, and Master Private Key (MPK). CW and DEK perform the same functions as the CW and AK in the ITU recommendation, respectively. The DK consists of a Private Key (PK) and a Group Key (GK) and is used to encrypt the DEK. PK is used uniquely for each subscriber and GK is used as a group key for each group of channels. MPK is used to encrypt the entitlement management message and DK and is stored in a smart card-based device. Keys of the last three levels are never revealed outside the smart card-based device, while the CW is sent out to descramble the subscribed programs. The computation of encrypting and broadcasting keys in Lee's scheme are too heavy to provide PPV services. In addition, the PK is unnecessary, since MPK can be used to identify the subscriber.

To improve Lee's scheme, Tu *et al.* [2] modified DEK in Lee's scheme and replace DK with a newly proposed key, Receiving Group Key (RGK). The RGK is used for subscription channels only. Subscribers whose authorization is expired will not receive the new RGK and can no longer view video programs. In Tu's scheme, all subscribers are classified into charging and receiving groups, where subscribers with the same charging periods are put in the same charging group and subscribers with the same set of subscription channels in the same receiving groups. Tu's scheme is efficient for subscription management and has the advantages to distribute the heavy daily work. However, the maximum number of the receiving group becomes the total number of subscription channels and is still a very large number. Besides, DEK updates in Tu's scheme require large amount of package broadcasting. In summary, the aforementioned schemes may introduce high computation and transmission costs for key updates. This is inefficient and costly

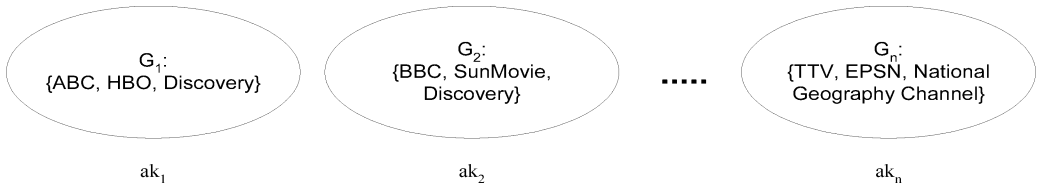

Fig. 2. Example of subscription channel groups.

when the client side is using a smart card with low computing power.

III. Key Distribution Schemes for Subscription Channel Protection

The goals of channel protection are to ensure that only authorized subscribers can descramble the programs correctly and that channel protection schemes must be efficient enough. In this section, two efficient key distribution schemes for key updates are proposed for subscription channel protection. The first scheme, *group-oriented key distribution scheme*, is used for subscription channels, which are divided into groups. The second scheme, *rating-oriented key distribution scheme*, is used for subscription channels classified by video program ratings.

The proposed two schemes are also based on a four-level key hierarchy: CW, AK, DK, and Secret Key (SK). The key for each level is used to encrypt/decrypt the keys for the previous level. CW is used to scramble/descramble programs on channels. Each channel has a unique CW at a specific time. Vector $\langle CW \rangle$ is used to denote the CWs of all channels. The CWs are updated frequently for higher security.

AK is used to encrypt and decrypt CW. There is also an AK for each channel 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 message to all authorized subscribers. Generally, AKs are updated periodically (e.g., daily) less frequent than CWs (e.g., 5–20 s). AK is usually updated daily because an authorized subscriber may be expired from the charging period in the next day.

DK is used to derive AK. There is also a DK for each channel 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, because the basic unit of a charging period is normally one month. SK, the secret key held by the subscriber, is used to encrypt and decrypt the DK. SK is distributed to the subscriber upon registration and stored on the subscriber's smart card. SK is used to distribute private messages for subscription and PPV channels. Keys of the last three levels (e.g., AK, DK, and SK) are never disclosed with the assistance of smart card. Only CW is sent out while descrambling the subscribed program. In the following sections, we explain each scheme in more detail based on the four-key hierarchy.

A. Group-Oriented Key Distribution Scheme

In the group-oriented key distribution scheme, customers subscribe to channels by groups, as shown in Fig. 2. Assume that there are n subscribers and m groups of channels in a CAS in the pay-TV system. Each group of subscription channels has its own AK and DK. AK is used to encrypt/decrypt the CWs of the channels in the group. DK is the secret information to derive the AK.

The notations used in this scheme are defined in Table I. In this scheme, AK is derived one by one in the ascending order of the group identity regardless of the group dependency. Besides, every subscriber can only correctly derive the AKs of the subscribed channel groups.

The distribution of AK consists of two phases: initial phase and update phase. In the initial phase, a service provider generates the vector $\langle DK_{SP} \rangle$, and uses the generated $\langle DK_{SP} \rangle$ to derive the AKs of "ALL" channel groups. Upon subscribing channel groups, the service provider uses $\langle DK_{SP} \rangle$ to generate $\langle DK_i \rangle$ for each subscriber S_i. Upon receiving the $\langle DK_i \rangle$, subscriber S_i is able to derive the AKs of the "SUBSCRIBED" groups. The key generation performed in the initial phase is described as follows.

[Initial Phase] For service provider (SP):

1) SP randomly generates $\langle DK_{SP} \rangle$, where $\langle DK_{SP} \rangle = [dk_1, dk_2, \ldots, dk_m]$.

2) SP derives new $\langle AK_{SP} \rangle$ by performing the following procedures:

- $ak_1 = D \oplus dk_1$, where D is a random number. (A.1)
- $ak_j = ak_{j-1} \oplus dk_j, \quad 2 \le j \le m.$ (A.2)

[Initial Phase] For each subscriber ($\mathbf{S_i}$):

1) SP generates the vector $\langle DK_i \rangle$ for each subscriber S_i, where

- dk_j^i *is randomly generated*, for $G_j \notin SG_i$.
- $dk_j^i = (dk_1 \oplus \cdots \oplus dk_j) \oplus \left(dk_1^i \oplus \cdots \oplus dk_{j-1}^i\right)$, for $G_j \in SG_i$. (A.3)

2) After generating $\langle DK_i \rangle$, the SP encrypts $\langle DK_i \rangle$ using the secret key SK_i of S_i.

3) SP transmits $\{\langle DK_i \rangle, D\}_{ski}$ to S_i, where D is the random number used to generate $\langle AK_{SP} \rangle$.

4) Subscriber S_i derives new $\langle AK_i \rangle$ by performing the following procedures:

- $ak_1^i = D \oplus dk_1^i.$ (A.4)
- $ak_j^i = ak_{j-1}^i \oplus dk_j^i, \quad 2 \le j \le m.$ (A.5)

The distribution keys in $\langle DK_i \rangle$ are generated one by one in the ascending order of the group. For example, dk_j^i is generated after dk_{j-1}^i. In the initial phase, if group j is subscribed, dk_j^i is generated to satisfy the formula $dk_j^i = dk_1^i \oplus \cdots \oplus dk_j^i = dk_1 \oplus \cdots \oplus dk_j = dk_j$, which is held by SP. Otherwise, if group

TABLE I
NOTATIONS USED IN GROUP-ORIENTED KEY DISTRIBUTION SCHEME

Notation	Description
G_j,	Channel group of identity j, where $j = 1, 2, ..., m$
S_j	Subscriber j, where $j = 1, 2, ..., n$
SG_i	Channel groups ordered by subscriber S_i.
$H()$	One-way hash function.
dk_j	The DK for channel group j, held by SP.
ak_j	The AK for channel group j, held by SP.
dk^i_j	The DK for channel group j, held by subscriber S_i.
ak^i_j	The AK for channel group j, held by subscriber S_i.
$<DK_{SP}>=[dk_1, dk_2, ..., dk_m]$	A vector of DKs and is held by SP. The vector is used to generate $<DK_i>$ and $<AK_{SP}>$.
$<AK_{SP}>=[ak_1, ak_2, ..., ak_m]$	A vector of AKs of all channel groups and is held by SP.
$<DK_i>=[dk^i_1, dk^i_2, ..., dk^i_m]$	A vector of DKs and is held by subscriber S_i. The vector is used to derive $<AK_i>$.
$<AK_i>=[ak^i_1, ak^i_2, ..., ak^i_m]$	A vector of AKs held by subscriber S_i. Only AKs of the subscribed channel groups equal to the AKs in $<AK_{SP}>$.

j is not subscribed, the corresponding dk^i_j will be randomly generated and will not equal to the dk_j, held by SP.

[Update Phase] For service provider (SP):

1) SP generates a random number R.
2) SP derives new $\langle AK_{SP}\rangle$ by performing:

- $ak_1 = R \oplus dk_1.$ (A.6)
- $ak_j = ak_{j-1} \oplus dk_j, \quad 2 \le j \le m.$ (A.7)

3) SP transmits $(R, h(R))$ to all subscribers.

[Update Phase] For each subscriber $(\mathbf{S_i})$:

1) After receiving $(R, h(R))$, S_i checks $h(R)$ for the integrity of R.
2) S_i derives new $\langle AK_i\rangle$ by performing:

- $ak^i_1 = R \oplus dk^i_1.$ (A.8)
- $ak^i_j = ak^i_{j-1} \oplus dk^i_j, \quad 2 \le j \le m.$ (A.9)

The new AKs in the vector $\langle AK_{SP}\rangle$ and the vector $\langle AK_i\rangle$ are generated one by one in the ascending order of the group identity. For example, dk^i_j is generated after dk^i_{j-1}. To verify the integrity of the received R, SP broadcasts R together with its digest, $(R, h(R))$, where $h()$ is a one-way hash function known to SP and subscribers' smart cards. In the update phase, if channel group j is subscribed, the dk^i_j, held by subscriber S_i, is equal to the dk_j, held by SP. Thus, subscriber S_i is able to derive an ak^i_j that is equal to ak_j held by SP.

Fig. 3 shows an example of the initial phase of group-oriented key distribution scheme. In this example, subscription channels are divided into four groups, G_1, G_2, G_3, and G_4. In the initial phase, the service provider (SP) randomly generates four distribution keys, dk_1, dk_2, dk_3 and dk_4. The SP then derives the four authorization keys, ak_1, ak_2, ak_3 and ak_4 by performing the schemes described in Section II.

In this example, the subscriber S_1 subscribes subscription channel groups, G_1, G_3 and G_4. The distribution keys held by subscriber S_1 are derived as follows.

1) dk^1_1 is the same as the distribution key (dk_1) held by SP.
2) dk^1_2 is randomly generated for G_2 is not subscribed.
3) dk^1_3 and dk^1_4 are derived by using formula (A.3), as shown in Fig. 3.

After deriving the distribution keys, the subscriber S_1 continues derives the authorization keys for the subscribed channel groups as follows.

1) $ak^1_1 = D \oplus dk^1_1$
$= ak_1$, where D is the random number used to generate the authorization keys for S_1.

2) $ak^1_2 = ak^1_1 \oplus dk^1_2$
$\neq ak_2$, for dk^1_2 is randomly generated and is not equal to dk_2.

3) $ak^1_3 = ak^1_1 \oplus dk^1_2 \oplus dk^1_3$
$= ak^1_1 \oplus dk^1_2 \oplus \left(dk_2 \oplus dk_3 \oplus dk^1_2\right)$
$= ak^1_1 \oplus dk_2 \oplus dk_3$
$= ak_1 \oplus dk_2 \oplus dk_3$
$= ak_3.$

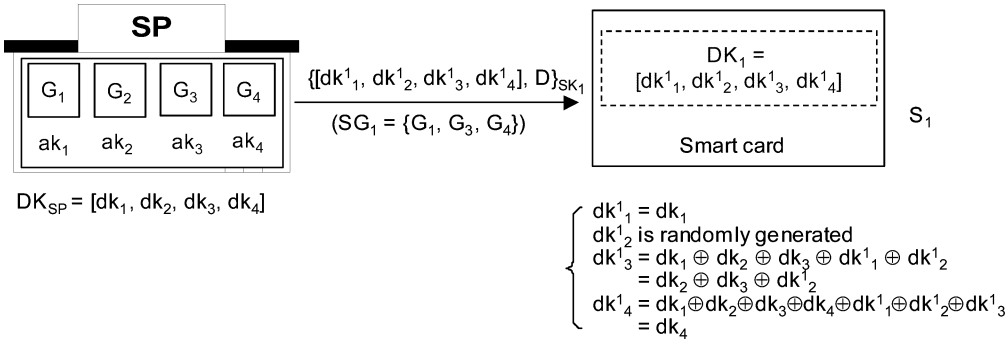

Fig. 3. Example of group-oriented key distribution scheme—initial phase.

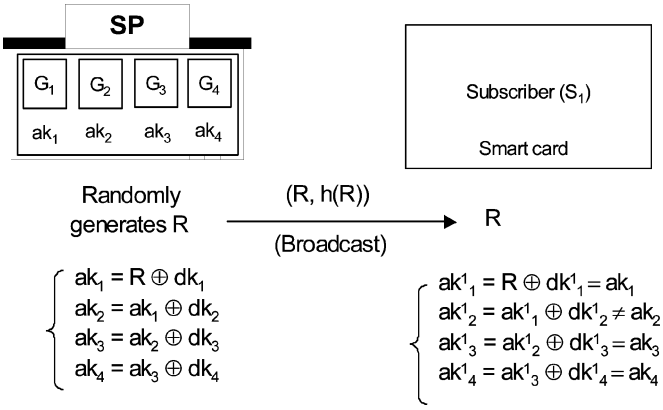

Fig. 4. Example of group-oriented key distribution scheme—update phase.

$$\begin{aligned} 4)\quad ak_4^1 &= ak_1^1 \oplus dk_2^1 \oplus dk_3^1 \oplus dk_4^1 \\ &= ak_1^1 \oplus dk_2^1 \oplus \left(dk_2 \oplus dk_3 \oplus dk_2^1\right) \oplus dk_4^1 \\ &= ak_1^1 \oplus dk_2 \oplus dk_3 \oplus dk_4 \\ &= ak_1 \oplus dk_2 \oplus dk_3 \oplus dk_4 \\ &= ak_4. \end{aligned}$$

Upon updating the authorization keys, the SP broadcasts a random number R to all subscribers. Then, SP and all subscribers update their authorization keys by performing formula (A.6)–(A.9), as shown in Fig. 4.

B. Rating-Oriented Key Distribution Scheme

In rating-oriented key distribution scheme, subscription channels are grouped by ratings. According to the definition in Motion Picture Association of America (MPAA), channel ratings are divided into five ratings: G (general), PG (parent guidance suggested), PG-13 (parent strongly cautioned), R (restricted) and NC-17 (no one 17 under admitted), as shown in Fig. 5.

In this scheme, a subscriber can watch the program on channels, which are not higher than the subscribed rating. The higher rating the subscriber subscribed, the more channels he can watch. For example, if a subscriber subscribes channels with a PG-13 rating, then the subscriber is able to watch video programs from channels with ratings of G, PG, and PG-13. We now describe the proposed rating-oriented scheme.

Assume that there are n subscribers and m ratings in a conditional access system. In the rating-oriented scheme, channels that belong to the same rating use the same AK and DK. The DK of lower rating channels can be generated from the DK of channels belong to higher rating. No matter which rating the subscriber belongs to, only one DK is needed for receiving video programs from these channels. In this scheme, only one message is broadcast to all subscribers for updating AKs of channels, which belong to the ratings lower than the subscribed rating. The notations used in rating-oriented key distribution scheme are defined in Table II.

The distribution of AK consists of two phases: initial phase and update phase. In the initial phase, a service provider generates the vector $\langle DK_{SP}\rangle$, and uses the generated $\langle DK_{SP}\rangle$ to derive the AKs of "ALL" channel ratings. Upon subscribing a channel rating, the service provider uses $\langle DK_{SP}\rangle$ to generate $\langle DK_i\rangle$ for each subscriber S_i. Upon receiving the $\langle DK_i\rangle$, subscriber S_i is able to derive the AKs of the channels lower than the "SUBSCRIBED" rating. The key generation performed in the initial phase is described as follows.

[Initial Phase] For service provider (SP):

SP generates $\langle DK_{SP}\rangle = [dk_1, dk_2, \ldots, dk_m]$, where

1) dk_1 is randomly generated. (B.1)

2) $dk_j = f(dk_{j-1})$,
where $2 \le j \le m$ and m is the lowest rating. (B.2)

[Initial Phase] For subscriber ($\mathbf{S_i}$):

1) SP transmits $\{\langle DK_i\rangle\}_{SKi}$ to subscriber S_i, where

$$\langle DK_i\rangle = [dk_k], \text{ for } SR_i = R_K. \tag{B.3}$$

2) S_i derives $[dk_{k+1}, \ldots, dk_m]$, where

$$dk_j = f(dk_{j-1}), \quad k+1 \le j \le m. \tag{B.4}$$

In this scheme, dk_j is generated from dk_{j-1} by using the one-way function, $f()$. Therefore, only the DK of higher rating can generate the DK of lower rating. Besides, only one DK need to be held for receiving video programs from these channels. DK of lower rating channel is derived by its ancestor.

[Update Phase] For service provider (SP):

In update phase, a new vector $\langle AK_{SP}\rangle$ is generated by vector $\langle DK_{SP}\rangle$. Only one message, which is the encrypted AK of the lowest rating, is broadcast to all subscribers.

- ak_1 is randomly generated. (B.5)

- $ak_j = \{dk_{j-1}\}_{dk_{j-1}}, \quad 2 \le j \le m.$ (B.6)

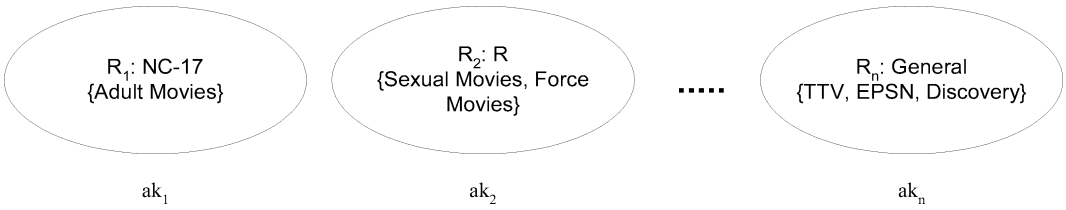

Fig. 5. Example of subscription channel ratings.

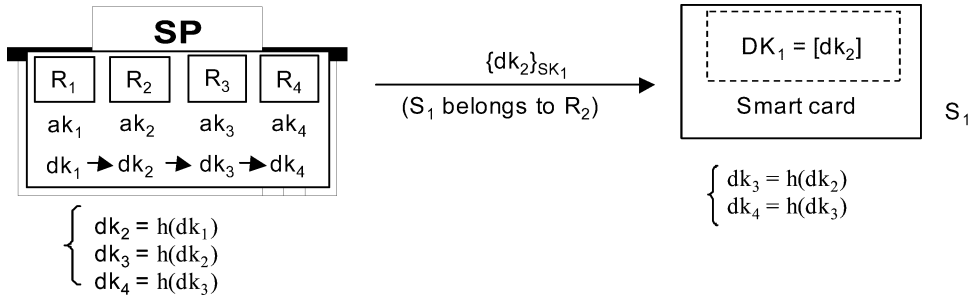

Fig. 6. Example of rating-oriented key distribution scheme—initial phase.

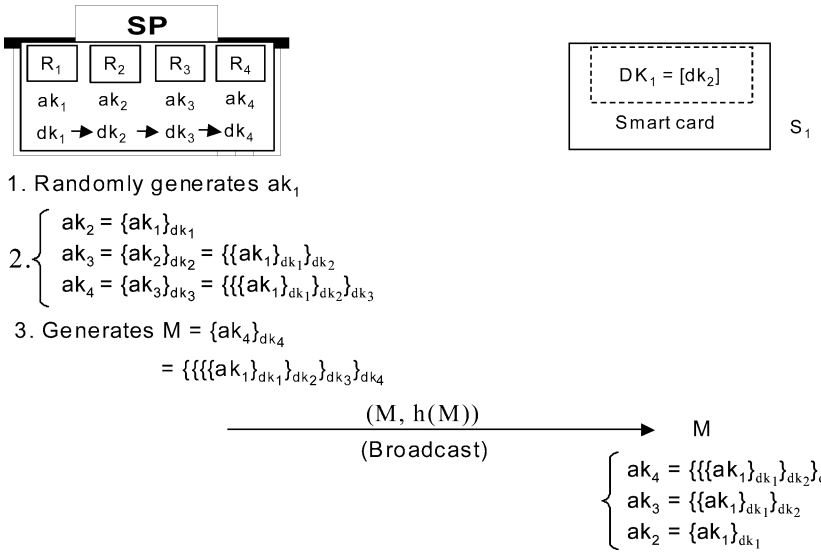

Fig. 7. Example of rating-oriented key distribution scheme—update phase.

[Update Phase] For subscriber (S_i):

Each subscriber S_i uses his vector $\langle DK_i \rangle$ to derive the new vector $\langle AK_i \rangle$ that contains the AKs of the ratings not higher than the subscribed rating. In this phase:

- After receiving $(M, h(M))$, S_i checks $h(M)$.
- S_i derives new $\langle AK_i \rangle = [ak_k, ak_{k+1}, \ldots, ak_m]$, where
  - $ak_m = \{M\}^{-1}_{dk_m}$. (B.7)
  - $ak_j = \{ak_{j+1}\}^{-1}_{dk_{j+1}}, \quad k \leq j < m.$ (B.8)

The new AKs are generated one by one in the descending order of channel ratings. For example, ak_{j-1} is derived from ak_j by decrypting with the decryption key dk_j. The AKs a subscriber can derive depends on the rating he subscribes. A subscriber only holds one DK of the rating he subscribes, and can only derive the DKs of the lower ratings. These derived DKs are used to derive the AKs of the ratings that are not higher than the subscribed rating.

Fig. 6 shows an example of the initial phase of rating-oriented key distribution scheme. In this example, subscription channels are divided into four ratings, R_1, R_2, R_3 and R_4. In the initial phase, the service provider (SP) randomly generates four distribution keys, dk_1, dk_2, dk_3, and dk_4. The SP then derives the four authorization keys, ak_1, ak_2, ak_3, and ak_4 by performing the formula (B.1) and (B.2) described in the Section III-A. In this example, the subscriber S_1 subscribes channel rating, R_2. The distribution keys held by subscriber S_1 are derived as follows.

1) S_1 receives $\{dk_2\}_{SK1}$ from SP.
2) S_1 derives dk_3 by performing $dk_3 = h(dk_2)$.
3) S_1 derives dk_4 by performing $dk_4 = h(dk_3)$.

Upon updating the authorization keys, SP randomly generates ak_1(B.5) and derives ak_2, ak_3 and ak_4 by performing formula (B.6). Then, SP generates M by encrypting ak_4 with dk_4 $(M = \{ak_4\}_{dk4})$ and broadcasts M to all subscribers. After receiving M, subscribers perform formula (B.7) and (B.8) to derive the authorization keys for the subscribed channels, as shown in Fig. 7.

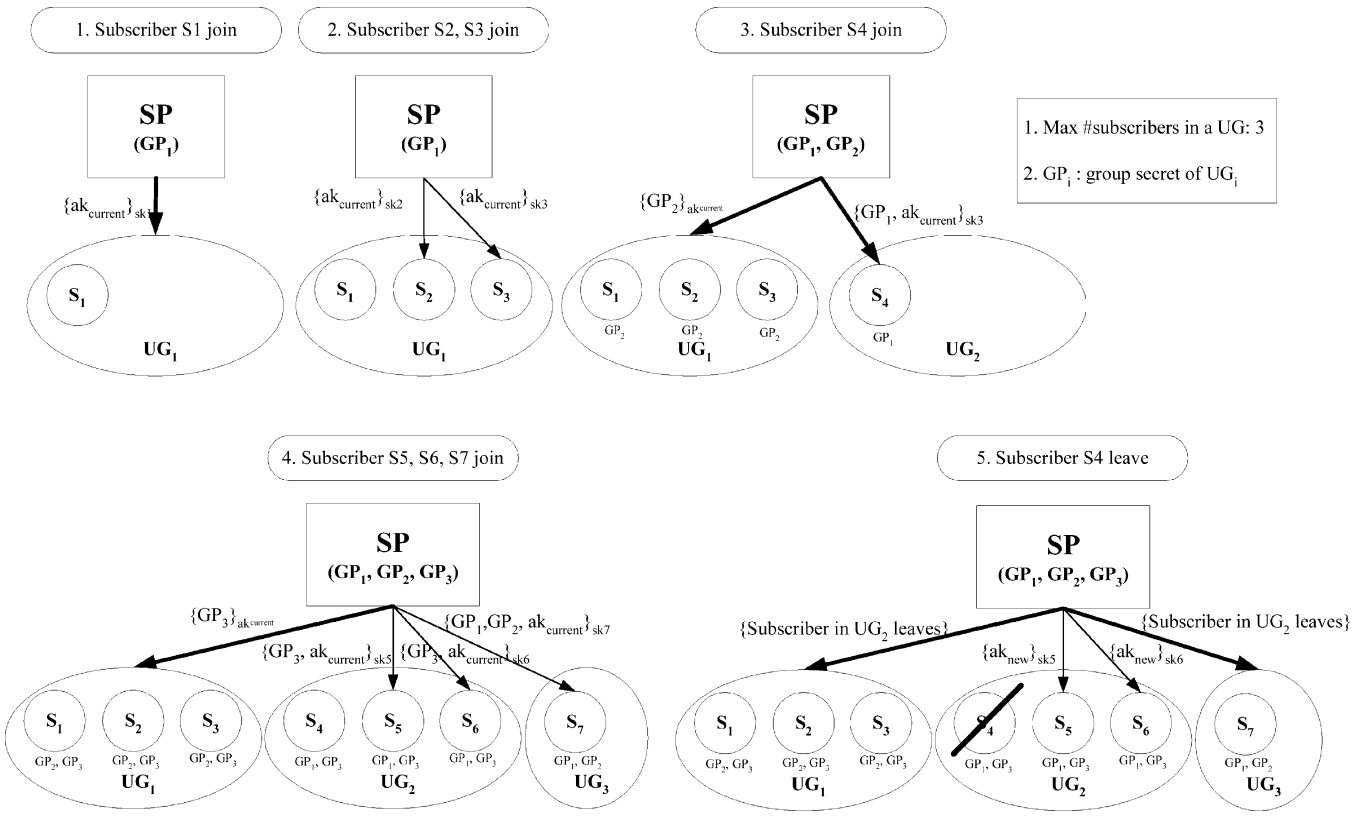

Fig. 8. Example of key distribution scheme for PPV channel protection.

i) S_1 decrypts M with dk_4 and gets ak_4.
ii) S_1 derives ak_3 by decrypting ak_4 with dk_3.
iii) S_1 derives ak_2 by decrypting ak_3 with dk_2.
iv) S_1 cannot derive ak_1 because S_1 does not know dk_1.

IV. Key Distribution Scheme for PPV Channel Protection

On PPV channels, video programs are broadcast according to the requests of subscribers. In this scenario, many subscribers may request the same popular video program simultaneously [11]–[13]. Some may participate and some others may leave during the playback period. Without privilege revocation, the leaving subscribers can keep watching the video programs without payment. For privilege revocation, AK updating operation is necessary and may occur very frequently. The behavior of the AK updating operation is similar to that of the rekeying operation in multicast communication [14], [15]. Once a member is leaving the multicast group, the keys known by the leaving member should be changed. The new keys are encrypted with users' private keys and the node keys shared by the users and then distributed to the users who need them. However, the encryptions and decryptions of the new keys take times in real-time applications, such as the broadcast of video streams. To help alleviate this problem, in this section we propose an efficient dynamic key distribution scheme for AK updating operation.

The key distribution scheme that we propose for PPV channel protection is a three-level key hierarchy: CW, AK, and SK. The key for each level is used to encrypt/decrypt the keys for the previous level. AK is dynamically assigned when subscribers request for video programs on the PPV channels. In the following, we describe the proposed key distribution scheme for PPV channel protection:

- Subscriber $S_{(m-1)k+1}(m \geq 1)$ joins
  - SP creates subscriber group UG_m of max k members.
  - SP randomly generates a group secret GP_m for UG_m.
  - SP broadcasts $\{UG_m \text{ Create, } GP_m\}_{ak}$ to all subscribers.
  - SP transmits $\{ak\}_{sk}(m-1)k+1$ to subscriber $S_{(m-1)k+1}$.
- Subscriber $S_{(m-1)k+i}$ ($m \geq 1$ and $2 \leq i \leq k$) joins
  - SP transmits $\{ak\}_{sk_{(m-1)k+i}}$ to subscriber $S_{(m-1)k+i}$ ($m \geq 1$ and $2 \geq i \geq k$).

If there are n subscriber groups, each group has k subscribers (totally nk subscribers) viewing the same video program, then $n-1$ secrets should be stored in subscribers' smart cards. When subscriber $S_{(m-1)k+i}$ (belong to UG_m) leaves, the authorization key should be changed, as described in the following:

- SP broadcasts $\{$ Subscriber in UG_m Leaves $\}$ to all subscribers.
- SP and subscribers belong to GU_j (where $j \neq m$) update the current AK (ak_{current}) to new AK:
  - $ak_{\text{new}} = H(ak_{\text{current}}, GP_m)$, where $H()$ is a one-way hash function.
- SP transmits the new AK ($\{ak\}_{sk_{(m-1)k+j}}$, where $m \geq 1$, $2 \geq j \geq k$ and $j \neq i$) to subscribers $S_{(m-1)k+j}$ who belong to GU_m.

TABLE II
NOTATIONS USED IN RATING-ORIENTED KEY DISTRIBUTION SCHEME

Notation	Description
R_j,	Channels of rating j, where $j = 1, 2, ..., m$
S_j	Subscriber j, where $j = 1, 2, ..., n$
SR_i	The rating subscribed by subscriber S_i.
$f()$, $h()$	One-way hash function.
ak_j	The AK for channels of rating j.
dk_j	The DK for channels of rating j.
$<AK_{SP}> = [ak_1, ak_2, ..., ak_m]$	A vector of AKs of all channel ratings and is held by the service provider.
$<AK_i> = [ak^i_k, ak^i_{k+1}, ..., ak^i_m]$	A vector of AKs of channel ratings, which are lower than the subscribed channel. This vector is held by subscriber S_i. Only AKs of the subscribed channel ratings equal to the AKs in $<AK_{SP}>$.
$<DK_i> = [dk_k]$	A vector of DK of the subscribed rating k, and is held by subscriber S_i. The vector is used to derive $<AK_i>$.
$<DK_{SP}> = [dk_1, dk_2, ..., dk_m]$	A vector of DKs of all channel ratings and is held by SP. The vector is used to generate $<DK_i>$

Fig. 8 shows an example of the key distribution scheme for PPV channel protection. In this example, the maximum number of subscribers in a subscriber group is three. SP creates new subscriber group when the number of subscribers reaches the multiples of three. In this case, S_1, S_2, S_3, S_4, S_5, S_6, and S_7 request for the same PPV channel sequentially. Initially, SP randomly generates an authorization key (ak). SP then generates a secret (GP_1) for subscriber group UG_1 when S_1 request for a PPV channel. Later, when S_2 and S_3 requesting for the same PPV channel, SP sends the authorization key (ak) encrypted with SK_2 and SK_3 to S_2 and S_3, respectively. At that time, SP does not create new subscriber group for the maximum number of subscribers in UG_1 does not reach three. Upon joint of S_4, SP creates a new subscriber group UG_2 and broadcasts the group secret GP_2 to S_1, S_2 and S_3 in subscriber group UG_1. In this example, totally seven subscribers are requesting the same PPV program and three subscriber groups are created for these subscribers.

The key update performs when one of the subscribers leaves the channel. In this example, S_4 leaves the channel and SP updates authorization key used by the channel. When subscriber S_4 leaves, SP broadcasts $\{$ Subscriber in UG_2 leaves $\}$ to all other subscribers. SP and subscribers not belong to UG_2 update their authorization keys (ak_{current}) to a new one $(ak_{\text{new}} = H(ak_{\text{current}}, GP_2)$, where $H()$ is the one-way hash function shared by SP and all subscribers). Then, SP sends the new authorization key (ak_{new}) to the rest subscribers in UG_2, S_5 and S_6. The ak_{new} is encrypted with the secret keys of these subscribers, e.g., SK_5 and SK_6, respectively. The leaving subscriber, S_4, cannot derive ak_{new} because neither does he know the secret GP_2 nor receive the new key from SP. Thus, S_4 cannot access that channel after he left.

In this scheme, if n subscriber groups are created and there are maximum k subscribers in each subscriber group (totally nk subscribers), then each subscriber keeps $(n-1)$ group secrets in his own smart card. When a subscriber leaves the group, k messages are used for notifying the updates of the authorization key: one message is broadcast to all subscriber and $(k-1)$ messages encrypted with subscribers' secret key are distributed to the rest subscribers who belong to the same group as the leaving subscriber.

V. COMPARISON

In this section, we compare our schemes with related researches in terms of the number of message exchanges and the cost of computation. Table III shows the number of message transmitted and Table IV shows 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 messages and the number of the transmitted messages are equal to the number of channel groups.

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

TABLE III
COMPARISON OF MESSAGE TRANSMITTED

Action/Scheme	Subscription Channels		PPV Channels	
	AK Update		Join	Leave
Eurocrypt	p		N/A	N/A
Lee	m		N/A	N/A
Tu	m		1	mk
Our Scheme	Group-oriented	1	2	k
	Rating-oriented	1		

m: subscriber groups
p: channel groups
k: max number of subscribers in each subscriber group in PPV channel

TABLE IV
COMPARISON OF COMPUTATIONAL COST

Action/Scheme	Subscription Channels		PPV Channels	
	AK Update		Join	Leave
Eurocrypt	g encrypt		N/A	N/A
Lee	m encrypt		N/A	N/A
Tu	m encrypt		1 encrypt	mk encrypt
Our Scheme	Group-oriented	p XOR	2 encrypt	1 hash
	Rating-oriented	q encrypt		(k-1) encrypt

q: channel rating

new AKs with the DK of each subscriber group respectively and then transmits the new AKs 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 together according to their subscribed channels. The subscribers in the same group use the same DK to update AKs. Therefore, the number of encrypted messages and transmitted messages equal the number of the subscriber groups. For PPV channel, SP uses the subscribers' SKs to distribute AKs. When a subscriber leaves, the SP encrypts the new AK with other subscribers' SKs and transmits to these subscribers respectively for privilege revocation. Therefore, the number of encrypted messages and the number of transmitted messages equal the number of the subscribers.

In our schemes, the number of transmitted messages and the cost of computation are both less than the related researches. In the group-oriented scheme, each subscriber keeps a vector of DKs that contains the information of the subscribed channel groups. On updating AKs, only one random number is broadcast to all subscribers. Each subscriber derives the AKs of all subscribed channel groups using the vector and the random number. Only exclusive-OR function is used to derive the AKs. In addition, the cost of computation equals to the number of channel groups, fewer than the number of the subscriber groups in Lee's and Tu's scheme.

In the rating-oriented scheme, each subscriber keeps a vector of DKs that contains the subscribed rating information. On updating AKs, only one message is broadcast to all subscribers, and each subscriber can derive the AKs of the ratings lower than the subscribed one, for example, a subscriber who subscribes channels of rating PG (parent guidance suggested) can receive both the channels of rating PG and of rating G (general). To generate the AKs of all channel ratings, the number of message encrypted equals the number of the channel ratings, and is less than the ratings in Lee's and Tu's scheme.

In PPV key distribution scheme, each subscriber keeps group secrets except the one he belongs to, for example, subscriber S_i (belongs to UG_m) keeps all group secrets P_j, where $j \neq m$. When a subscriber joins and SP creates a new subscriber group, SP first broadcasts the new secret encrypted with the current AK to all subscribers watching the same video program. Then, SP encrypts the AK and the group secrets of other groups with the subscriber's SK and transmits it to the newly joined subscriber.

Although one more encryption and transmission of the new secret is needed for subscriber joins, only k messages are needed to broadcast for privilege revocation of the leaving subscriber: one broadcast and $(k-1)$ encrypted messages. Only one-way hash function is used to derive the new AK. This is much more efficient than Tu's scheme.

VI. CONCLUSION

In this paper, three key distribution schemes have been proposed for channel protection in conditional access system. The group-oriented and rating-oriented key distribution schemes are used for key updates for subscription channel protection. The dynamic key distribution scheme is used on PPV channel protection. Compared with the existing solutions described in the related work, fewer messages are transmitted and simpler computing functions are used in our schemes. Considering the low computation power of smart cards, our schemes are more practical for implementation in a smart card-based conditional access system.

With our schemes, only the authorized subscribers can view the ordered programs and the service provider can charge the subscribers according to their subscriptions. Unauthorized subscribers cannot get the correct programs over the networks. Thus, service providers can charge their subscribers according to their subscriptions, and the illegal access of the programs during transmission can be prevented.

REFERENCES

[1] J. W. Lee, "Key distribution and management for conditional access system on DBS," in *Proc. Int. Conf. Cryptology and Information Security*, 1996, pp. 82–86.
[2] F. K. Tu, C. S. Laih, and S. H. Toung, "On key distribution management for condition access system on Pay-TV system," in *1998 IEEE Int. Symp. Consumer Electronics (ISCE'98).* , vol. 45, Taipei, Taiwan, R.O.C., pp. 151–159.
[3] H. Sakakibara *et al.*, "The ID-based noninteractive group communication key sharing scheme using smart cards," in *Proc. Int. Conf. Network Protocols*, 1994, pp. 91–98.
[4] "Conditional-Access Broadcasting Systems,", ITU-R Rec. 810, 1992.

[5] E. Cruselles, J. L. Melus, and M. Soriano, "An overview of security in Eurocrypt conditional access system," in *IEEE Global Telecommunications Conf.*, vol. 1, 1993, pp. 188–193.
[6] B. M. Macq and J. J. Quisquater, "Cryptology for digital TV broadcasting," *Proc. IEEE*, vol. 83, 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 Trans. Consumer Electron.*, vol. 43, pp. 980–985, Aug. 1997.
[8] *Data Encryption Standard*, NBS FIPS PUB 46-1, Jan. 1977.
[9] X. Lai and J. Massey, "A proposal for a new block encryption standard," in *Advances in Cryptology- Proc. EUROCRYPT '90*, 1991, pp. 389–404.
[10] M. J. B. Robshaw, "Block Ciphers," RSA Lab. LOCATION???, TR-601, 1994.
[11] T. D. C. Little and D. Venkatesh, "Prospects for interactive video-on-demand," *IEEE Multimedia*, pp. 14–23, Fall 1994.
[12] K. C. Almeroth and M. H. Ammar, "The use of multicast delivery to provide a scalable and interactive video-on-demand service," *IEEE J. Selected Areas Commun.*, vol. 14, Aug. 1996.
[13] S. Viswanathan and T. Imielinski, "Metropolitan area video-on-demand service using pyramid broadcasting," *Multimedia Syst.*, vol. 4, no. 4, pp. 197–208, 1996.
[14] L. S. Juhn and L. M. Tseng, "Staircase data broadcasting and receiving scheme for hot video service," *IEEE Trans. Consumer Electron.*, vol. 43, no. 4, pp. 1110–1117, Nov. 1997.
[15] D. Wallner, E. Harder, and R. Agee, "Key Management for Multicast: Issues and Architectures,", RFC 2627, 1999.

Yu-Lun Huang received the B.S. and Ph.D. degrees in computer science and information engineering from National Chiao-Tung University (NCTU), Hsinchu, Taiwan, R.O.C. in 1995 and 2001, respectively.

She is currently an Assistant Professor, Department of Electrical and Control Engineering, NCTU. Her research interests include electronic commerce, distributed systems, quality of services, network security, embedded systems and embedded software.

Ms. Huang a member of the Phi Tau Phi Society.

Shiuhpyng Shieh (SM'00) received his M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, in 1986 and 1991, respectively.

He is currently the Professor and Chairman of the Department of Computer Science and Information Engineering, National Chiao-Tung University (NCTU); the Vice Board Chairman of Chinese Cryptology & Information Security Association; Director of Cisco Internetworking Technology Laboratory; Director of GSN-CERT.

Prof. Shieh was on the organizing committees of numerous international conferences and published over a hundred of papers and patents. Recently, he has received two outstanding research awards, honored by NCTU and Executive Yuan of Taiwan, respectively. His research interests include internetworking, distributed systems, and network security.

Fu-Shen Ho received the B.S., M.S. and Ph.D. degrees in computer science and information engineering from National Chiao-Tung University, Hsinchu, Taiwan, R.O.C., in 1995, 1997, and 2003, respectively. He is currently the Software Manager of Alpha Networks, Inc., Hsinchu. His research interests include operating systems design, distributed systems, internetworking and network security.

Jian-Chyuan Wang received the M.S. degree in computer science and information engineering from National Chiao-Tung University, Hsinchu, Taiwan, R.O.C., in 1998. His research interests include electronic commerce, distributed systems and network security.