A Conditional Access System with Efficient Key Distribution and Revocation for Mobile Pay-TV Systems

LO-YAO YEH and JIUN-LONG HUANG, National Chiao Tung University, Taiwan, R.O.C.

Current mobile pay-TV systems have two types of Conditional Access Systems (CAS): group-key-based and public-key systems. The best feature of group-key-based systems is the ability to enjoy the broadcast nature in delivery multimedia contents, while the major advantage of public-key systems is consolidating the security foundation to withstand various attacks, such as collusion attacks. However, the problems of group-key-based systems include collusion attacks, lack of nonrepudiation, and troublesome key distribution. Even worse, the benefit of broadcast efficiency is confined to a group size of no more than 512 subscribers. For public-key systems, the poor delivery scalability is the major shortcoming because the unique private key feature is only suitable for one-to-one delivery. In this article, we introduce a scalable access control scheme to integrate the merits of broadcasting regardless of group size and sound security assurance, including fine-grained access control and collusion attack resistance. For subscriber revocation, a single message is broadcast to the other subscribers to get the updated key, thus significantly boosting subscriber revocation scalability. Due to mobile subscribers' dynamic movements, this article also analyzes the benefit of retransmission cases in our system. Through the performance evaluation and functionality comparison, the proposed scheme should be a decent candidate to enhance the security strength and transmission efficiency in a mobile pay-TV system.

Categories and Subject Descriptors: K.6.5 [**Computing Milieux**]: Security and Protection—*Authentication*; K.4.4 [**Computing Milieux**]: Electronic Commerce—*Distributed commercial transactions*

General Terms: Security

Additional Key Words and Phrases: Digital video broadcasting, nonrepudiation, multimedia delivery, sophisticated access control.

ACM Reference Format:

Yeh, L.-Y. and Huang, J.-L. 2013. A conditional access system with efficient key distribution and revocation for mobile pay-TV systems. ACM Trans. Multimedia Comput. Commun. Appl. 9, 3, Article 18 (June 2013), 20 pages.
DOI: http://dx.doi.org/10.1145/2487268.2487271

1. INTRODUCTION

With the rapid growth of hardware, software, and network technologies, mobile multimedia services are envisioned to dominate the market over the next decade. Many handheld devices, including smart phones and tablet PCs, are becoming increasingly popular. These handheld devices are conducive to mobile pay-TV services. Consequently, demands for scalable transmission protocols for multimedia

This work was supported in part by the National Science Council under grant NSC 101-2221-E-492-030 and NSC 101-2221-E-492-025.

Author's address: L.-Y. Yeh and J.-L. Huang (corresponding author), Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan, R. O. C.; email: jlhuang@cs.nctu.edu.tw.

DOI: http://dx.doi.org/10.1145/2487268.2487271

content are also emerging. In a pay-TV system, security is an important issue, which ensures that only authorized subscribers can access the video contents. To handle security issues, researchers have proposed some Conditional Access Systems (CASs) [ITU; Huang et al. 2004; Sun et al. 2008; Wang and Laih 2008; Zhu 2008; Sun and Leu 2009; Yeung et al. 2005]. Most CASs are based on the broadcast encryption [Fiat and Naor 1994] and group-key-based symmetric cryptosystems to enjoy broadcast efficiency. All subscribers are divided into several groups according to their channel preferences or other policies. Subscribers in the same group share a group key. To transmit a requested video to multiple subscribers in different groups, the video server first determines which group keys are used to encrypt the video content and broadcasts the encrypted video to all requesting subscribers. However, group-key-based systems [Huang et al. 2004; DVB-SPP; Wang and Laih 2008; Sun et al. 2008] suffer from problems related to troublesome key distribution [Sun and Leu 2009], collusion attacks [DVB-SPP] and a lack of nonrepudiation. The troublesome key distribution problems may also lead to another puzzle: the iterative revocation process (or key update process). In Wang and Laih [2008] and Sun et al. [2008], the authors also have analyzed the detailed storage and communication overhead in the key update process. When a subscriber orders 120 channels, he/she must store at least 605 secret keys in Sun et al. [2008] and 3480 ones in Huang et al. [2004]. When a subscriber wants to change his preference group, the service provider delivers messages to 4 to 12 groups, according to the location of the group the departing subscriber inhabits. There are approximately 256 users, that is, subscribers, in a group, which requires approximately 1024 to 3072 subscribers to update their keys. Group-key-based schemes earn a broadcast advantage during content transmissions by sacrificing revocation efficiency and security strength.

Conversely, some works [Sun and Leu 2009; Yeung et al. 2005] have been based on public-key cryptosystems to consolidate security strength. Unfortunately, the public-key cryptosystems dedicate a public/private key pair to a specific subscriber, thus compromising broadcast efficiency. In Sun and Leu [2009], the authors attempt to repair the bandwidth waste problem using batch-based verifications. This system [Sun and Leu 2009] only keeps the benefits of broadcasting during the authentication phase but retains one-to-few transmission[1] during video content transmissions. The bandwidth cost of the authentication phase is less than that of video content transmissions. Some works [Sun and Leu 2009; Yeung et al. 2005] have even yet considered the subscriber revocation problem [Staddon et al. 2002].

An ideal mobile pay-TV system should encompass the following properties.

- Security aspects:
  - Fine-grained access control: A mobile pay-TV system should offer various videos to subscribers, but children should not be able to access a sexual or violent movie. Determining a subscriber's identity and his/her access rights is thus an extremely important issue.
  - Nonrepudiation: It is essential for commercial transactions to provide the nonrepudiation property. When disputes between subscribers and a service provider occur, this property is useful evidence in court.
  - Backward secrecy: A mobile pay-TV system must ensure that a revoked subscriber cannot obtain services.
- Efficiency:
  - Storage overhead: Several pay-TV systems [[Zhu 2008]; DVB-SPP; Wang and Laih 2008; Sun et al. 2008] adopt a tree structure to support key management strategies for efficiency and flexibility. Each subscriber may receive some extra keys, which is a type of storage overhead.

[1] In Section 5.2.6-2, we will classify transmissions into three kinds of delivery types for precise comparisons.

- —Retransmission efficiency: A “mobile” pay-TV system should allow subscribers to download videos using mobile devices, for example, Tablet PCs and smart phones, which may result in a high probability for packet retransmissions. The importance of the retransmission efficiency should thus gain more attention.
- —Scalability: Two types of scalability can impact a pay-TV system. One is user preference scalability, and the other is revocation scalability.
  - —User preference scalability: A pay-TV system should allow each subscriber to arrange his/her own channels according to his/her preferences. In a traditional group-key-based system, several subscribers may need to update their keys to guarantee that security issues will not occur if a preference group member has changed his/her preference, which causes poor user preference scalability.
  - —Revocation scalability: subscribers often join and leave. An ideal pay-TV system should incur little cost when a single subscriber joins or leaves. In current pay-TV systems, the other subscribers must update their group keys when a subscriber in the same group has left.

To the best of our knowledge, no mobile pay-TV systems possesses the preceding properties. Group-key-based pay-TV systems [Huang et al. 2004; Wang and Laih 2008; Sun et al. 2008; Zhu 2008; DVB b; a] may hold the properties of fine-grained access control, backward secrecy, and medium transmission efficiency, but they do not have revocation scalability or are of high storage overhead. Even worst, group-key-based pay-TV systems cannot attain the important nonrepudiation property because symmetric cryptosystems do not have digital signatures. In contrast, public-key-based pay-TV systems [Yeung et al. 2005; Sun and Leu 2009; Roh and Jung 2011] are of nonrepudiation, lightweight storage overhead, and better revocation scalability, but they are deficient in fine-grained access control and have extremely poor transmission efficiency. Each user can usually be classified into different groups to achieve fine-grained access control. The existing public-key-based pay-TV systems [Yeung et al. 2005; Sun et al. 2008] usually choose a random authorization key to encrypt multimedia content. Fine-grained access control is thus not easy to implement in public-key-based pay-TV systems. In Section 5, Table III compares the functionality of several schemes.

This article proposes a scalable conditional access scheme to fulfill the aforesaid requirements. The proposed scheme not only enjoys the benefit of broadcast delivery (the advantage of group-key-based pay-TV systems) but also offers solid security strength (the advantage of public-key-based pay-TV systems). Furthermore, when a subscriber is revoked, the proposed scheme can efficiently update the other subscribers using a broadcast message. The Attribute-Based-Encryption (ABE) concept [Sahai and Waters 2005] is employed as the underlying cryptosystem to support the nonrepudiation property. In our system, each subscriber is endowed with an n-bit unique Revocation Number (RN) for efficient revocation procedures and several granted attributes for fine-grained access control. Subscribers do not store a group key, and pay-TV systems do not maintain a tree structure. Our pay-TV system only uses the appropriate public RN keys (i.e., attributes) to encrypt update messages during revocation procedures. One unique virtue of the proposed scheme is retransmission efficiency, which is extremely suitable for “mobile” pay-TV systems. As each encrypted update message is not bound to any specific group or subscriber, the middle proxy servers that have received the encrypted messages can directly retransmit it without the intervention of the centralized multimedia server.

In summary, the contributions of the proposed scheme are: (1) integrating the merits of both group-key- and public-key-based pay-TV systems, (2) supporting efficient subscriber revocation, (3) reducing the storage overhead for group keys, (4) enjoying real one-to-many broadcast facilities in both the authentication and video content transmission phase, (5) assisting packet retransmissions, and (6) meeting the imperative security requirements, for example, nonrepudiation and preventing collusion attacks. As mentioned before, the aspects of efficiency and scalability are important for a mobile pay-TV system. In this article, we also have done three experiments in terms of: (1) storage overhead (Section 5.2.1), (2) retransmission efficiency (Section 5.2.2), and (3) revocation waiting time (Section 5.2.3) to demonstrate the efficiency and scalability advantages our scheme earns. The subscriber revocation function and dynamic attribute update concept introduced in the Appendix section are new properties for the original attribute-based encryption.

To be practical, we show that the proposed scheme can be compatible with the current booming digital video broadcast standards, DVB-H [DVB a] and DVB-SH [DVB b]. In the following section, we enforce the proposed scheme in the DVB-H or DVB-SH architectures. The proposed scheme can be easily implemented in other multimedia transmission architectures with some modifications.

The rest of the article is outlined as follows. Section 2 briefly surveys the related work. In Section 3, we introduce the complexity assumptions and security objectives. Section 4 presents the proposed access control scheme. Section 5 demonstrates the security analysis and performance evaluations. Finally, Section 6 presents the conclusion.

2. RELATED WORK

In this section, we introduce the broadcast encryption that group-key-based systems often use. The Appendix presents the related popular digital video broadcast standards, DVB-H and DVB-SH, and the security mechanism (SPP) specified in the two standards.

2.1 Key Hierarchy

Here, we explain the broadcast encryption scheme used in SPP, called Zero Message Broadcast encryption (ZMB). As mentioned earlier, the SPP system contains four layers: the registration, rights management, key stream, and traffic encryption layers. Figure 8(b) illustrates the key hierarchy [DVB-SPP] used in SPP. SPP supports both the interactive and broadcast modes, but this article is dedicated to the broadcast mode. The details of key materials in each layer are described next.

—Registration layer. Several keys used for authentication and decryption as parts of a Device Registration Data (DRD) are protected by the device's public key and delivered to the device. These keys include the Unique Group Key (UGK), Subscriber Group Key (SGK), Broadcast Domain Key (BDK), Unique Device Key (UDK), and Right Issuer Authentication Key (RIAK). The UGK, SGK, BDK, and UDK are used for addressing, while the RIAK is designed for authentication. Section 2.2 explains the detailed addressing by keys.

—Rights management layer. Depending on which device or group receives the Right Object (RO), the Right Issuer (RI) determines which Inferred Encryption Key (IEK) is used to encrypt/decrypt the Service Encryption Key (SEK)[2]. The Right Object (RO) is a collection of permissions, keys, and other attributes for the requested content or service. The Right Issuer (RI) is an entity that registers devices and provides ROs, thus allowing devices to receive the protected services. If the RO is addressed to a domain, the IEK is the BDK.

—Key stream layer. As the SEK is determined in the right management layer, the SEK is used to encrypt the Traffic Encryption Key (TEK), which protects real traffic packets.

[2] In SPP [DVB-SPP], there is another business model, pay-per-view-based subscription, and the protection method of which is similar as the service-based subscription introduced in this article. For simplicity, we only discuss the keys hierarchy used in the service-based subscription (pay-per-channel).

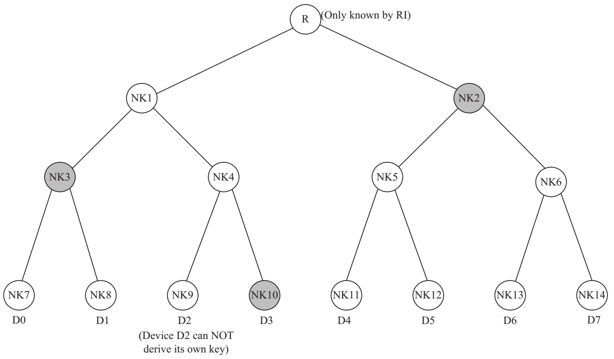


Fig. 1. Example of a zero message tree (group size $N = 8$).

—Content/service protection layer. In this layer, video contents are encrypted using IPsec, SRTP, or ISMACryp. The key used to encrypt the traffic is TEK, and the C represents the video content. The TEK changes frequently, ranging from once per minute to once per second.

The SPP recommends that AES [Daemen 2002] be the symmetric encryption cryptosystem.

2.2 Addressing by Keys

To achieve broadcast encryption, several keys sent to a device in the registration layer are designed for addressing. How to use these keys is explained next.

—Unique Group Key (UGK): A unique group contains all devices in a group, which is the largest group in the broadcast encryption scheme. Considering the revocation efficiency, SPP suggests that a group size be fewer than 256 or 512.

—Subscriber Group Key (SGK): A subscriber group can be smaller than or equal to the unique group, for example, sports can be a subscriber group.

—Broadcast Domain Key (BDK): A device can join a domain in the registration layer using a join domain response.

—Unique Device Key (UDK): Each device holds a unique device key, which is used to address only one device.

The UGK, SGK, and BDK are designed to achieve efficient broadcast encryption. These keys are used to distinguish the relationships among all devices to reduce the number of transmissions.

2.3 Zero Message Broadcast Encryption Scheme

After device registration, a zero message broadcast encryption [Fiat and Naor 1994] is adopted to create a privileged set within a group of devices. The ideal case is that no more data must be transmitted to the unique device, thus creating a Zero Message Broadcast (ZMB) scheme.

ZMB is based on a set of group keys provisioned to the device during registration [DVB-SPP]. Depending on the group size N, the number of required group keys l is calculated as $l = log_2(N)$. Each device must derive $N - 1$ keys. Figure 1 shows a simple example of a zero message tree. The group size of the example is 8, $N = 8$, and the required group keys for each device is 3, $l = 3 = log_2(8)$. The root key in the zero message broadcast encryption key tree is only known by the Right Issuer (RI). In this case, device D2 must keep the keys {NK2, NK3, NK10} to derive the keys {NK11, NK12, NK13, NK14} from NK2 and the keys {NK7, NK8} from NK3. The derivation function is thus

$$NK2i + 1 = AES\{NKi\}(2i + T1), NK2i + 2 = AES\{NKi\}(2i + T2),$$

where i is the parent key index, $T1$ is the timestamp when the RO became active, and $T2$ is the timestamp when the RO is due to expire. The Inferred Encryption Key (IEK) comprises the keys {NK7, NK8, NK10, NK11, NK12, NK13, NK14}.

Considering Figure 8(b), device D2 should hold the group keys {NK2, NK3, NK10} in the registration layer. If D2 does not have the group keys, the interactive channel must acquire all group keys. After gaining IEK, D2 can derive both the SEK from the RO message and the TEK from the key stream messages. Finally, the TEK can decrypt the encrypted traffic. The TEK should be frequently changed for security considerations.

In the ZMB scheme, the recommended group size is no more than 512. Although the ZMB scheme tries to gain the broadcast encryption advantage, the small group size restricts it, because it is rare that all requesting devices belong to the same group, as in Appendix C. Due to several considerations, including collusion attacks and the key derivation process complexity [DVB-SPP], small group size is preferred. A more serious consequence may occur with a larger size, for example, the reregistration of all devices. In this article, we determine a novel access control scheme tailored for broadcast transmission to eliminate the group size limitation. Collusion attacks are withstood, and complicated key derivation processes are omitted.

3. PRELIMINARY CONDITIONS

3.1 Complexity Assumptions

The following underlying assumptions [Sahai and Waters 2005] exist for the security foundations of the proposed protocol.

(1) *Elliptic Curve Decisional Bilinear Diffie-Hellman (ECDBDH)*. Suppose a challenger chooses a, b, c, d, $z \in Z_q$ at random. The decisional ECDBDH assumption is that no polynomial-time adversary should be able to distinguish the tuple $(A = aP, B = bP, C = cP, Z = e(P, P)^{abc})$ from the tuple $(A = aP, B = bP, C = cP, Z = e(P, P)^z)$ with more than a negligible advantage.

(2) *Elliptic Curve Decisional Modified Bilinear Diffie-Hellman (ECMBDH)*. Suppose a challenger chooses $a, b, c, d, z \in Z_q$ at random. The decisional ECMBDH assumption is that no polynomial-time adversary should be able to distinguish the tuple $(A = aP, B = bP, C = cP, Z = e(P, P)^{\frac{ab}{c}})$ from the tuple $(A = aP, B = bP, C = cP, Z = e(P, P)^z)$ with more than a negligible advantage.

3.2 Security Objectives

To achieve scalable and robust video content delivery, an access control scheme for pay-TV systems should meet the following requirements.

(1) Fine-grained Access Control: Due to the various video content properties, a secure video delivery scheme is desirable for the sophisticated authorization or fine-grained access control, which provides a strategy to specify different subscribers' capabilities.

(2) Resistance to Collusion Attacks: A subscriber cannot cooperate with other subscribers to promote his own privileges.

(3) Nonrepudiation: To ensure video content validity and quality, the video server should not deny that the video contents are delivered from it.

(4) Backward Secrecy: For subscriber revocation, an access control scheme should guarantee that revoked subscribers cannot access video content after the subscribers' privileges have been revoked.

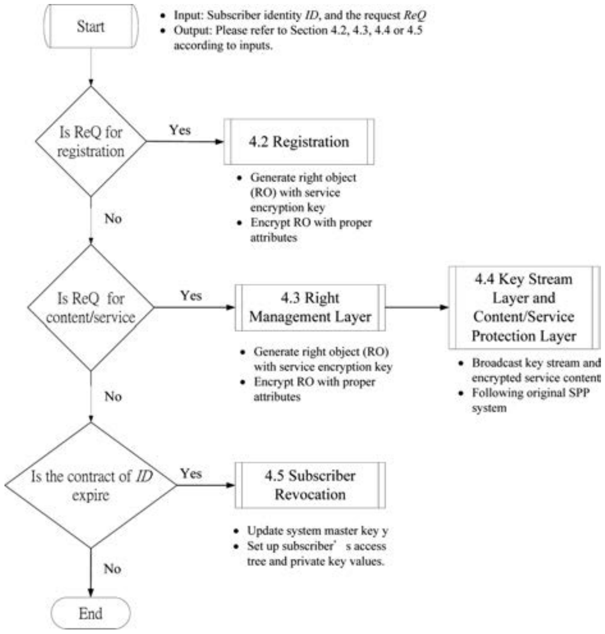

Start
• Input: Subscriber identity ID, and the request ReQ
• Output: Please refer to Section 4.2, 4.3, 4.4 or 4.5 according to inputs.
Is ReQ for registration
Yes
4.2 Registration
• Generate right object (RO) with service encryption key
• Encrypt RO with proper attributes
No
Is ReQ for content/service
Yes
4.3 Right Management Layer
• Generate right object (RO) with service encryption key
• Encrypt RO with proper attributes
4.4 Key Stream Layer and Content/Service Protection Layer
• Broadcast key stream and encrypted service content
• Following original SPP system
No
Is the contract of ID expire
Yes
4.5 Subscriber Revocation
• Update system master key y
• Set up subscriber' s access tree and private key values.
No
End

Fig. 2. Flowchart of proposed scheme.

4. THE PROPOSED SCHEME

The promising merit of the DVB-H/SH standards is delivering video content and services to a subscriber group using a broadcast. Due to the security considerations, the benefits of broadcasting are significantly diminished. In this section, we propose a scalable access control scheme to enjoy the benefits of broadcasting without compromising security considerations. For commercial businesses, the proposed scheme further provides the nonrepudiation property and supports fine-grained access control, including film rating systems and subscriber classes.

Figure 2 shows a flowchart of the proposed scheme for a better view. Conceptually, based on attribute-based encryption cryptosystems [Goyal et al. 2006; Sahai and Waters 2005], the Right Issuer (RI) or service provider enumerates the universal attributes $\mathcal{A}$, that is, five film ratings, and subscriber classes. RI then generates the (public key, private key) pair for each attribute. For subscriber revocations, the RI assigns each subscriber a unique Revocation Number (RN) using the centralized flat table method [Waldvogel et al. 1999] to efficiently update the keys.

In the registration layer, each subscriber is granted some attributes, such as $\{\text{subscriber class} = \text{VIP}\}$ and $\{\text{film ranking} = \text{NC-17}\}$, associated with a unique access structure. Based on the access structure, the subscriber's private key values are generated using his/her authorized attributes. In the rights management layer, while receiving requests for the same video content, the RI can directly choose a SEK encrypted using the public key of the proper attributes and disseminate the encrypted SEK in a broadcast. Only subscribers with the attached attributes can derive the SEK. For subscriber revocations, each subscriber is assigned a unique n-bit revocation number RN, which serves as a unique identifier and is irrelevant to a subscriber's attributes and access tree. Each bit is bound with two bit attributes with the bit values 1 and 0. When a subscriber with $RN = X_{n-1}X_{n-2\dots}X_0$ is revoked, the RI can update the master key of the other subscribers by encrypting the update message with the bit attributes $\overline{RN} = \bar{X}_{n-1}\bar{X}_{n-2\dots}\bar{X}_0$. All subscribers but the revoked one can thus retrieve the update

Table I. Notations and Parameters

Notation	Description
RI	Right issuer or service provider
$\mathcal{A}$	Universal attributes
SA	Subscriber's attributes
VA	Video's attributes
$RN_{i,X}$	Revocation number and the i-th bit with X value, where $X = 0\|1$
$RNA_{i,X}$	Revocation number attribute for the i-th bit with X value
PK	Set of system's public keys
$W, T_j, h_{i,X}$	Components of PK
MK	Set of system's master keys
y, τ, t_j, c_i, d_i	Components of MK
AT	Subscriber's access tree
RK	Set of subscriber's private keys
WD, D_i, DR_{j,X_j}	Components of RK
RO, ERO	Right object and encrypted right object
SEK	Service encryption key
UM	Update message for subscriber revocation.

message to renew the master key. Table I provides descriptions of the important notations used in our scheme.

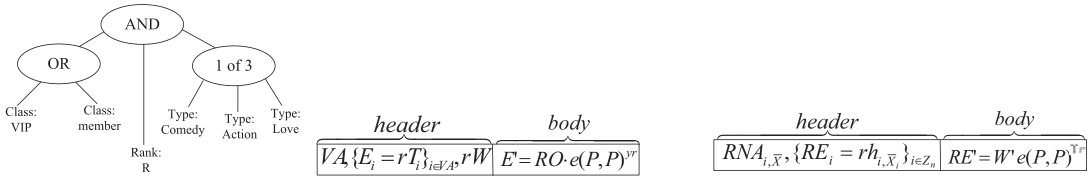
The proposed scheme endows the SEK and update message with some attributes to enforce fine-grained access control and delivers the encrypted SEK and updates messages regardless of the group keys to be used. Moreover, the encrypted SEK and update messages are only transmitted once, while the ZMB scheme [DVB-SPP] may be delivered multiple times to subscribers with different groups. For security, the collusion attack, which means two subscribers share their attributes, can be prevented because the RI selects different polynomials associated with the subscribers' access structures and the private key values are related to those polynomials.

To enforce fine-grained access control, RI constructs an access structure for each subscriber according to his/her preference. RI first defines a public key/private key for each attribute, and each subscriber is granted an authorized attribute and the corresponding keys. The access structure is implemented using an access tree AT, where each leaf node is labeled with an attribute and the interior nodes are threshold gates, for example, AND, OR, and t-of-n threshold gate. Figure 3(a) shows how a subscriber can only access the video content with attributes {Class = VIP or member} and {Ranks: R} and {Type = Comedy or Action or Love}. The access structure can represent sophisticated logic expressions to achieve fine-grained access control for each subscriber.

4.1 Registration Layer

4.1.1 *System Initialization.* RI first establishes the public parameters and private key values for subscribers in the registration layer. Let G be a cyclic additive group generated by P, where P is a generator of G, and G_T a cyclic multiplicative group with the same order q. In addition, let e: $G \times G \rightarrow G_T$ denote the bilinear map of prime order q. According to the purchase contract, each subscriber is entitled to some subscriber attributes $SA \subseteq \mathcal{A}$, where $\mathcal{A}$ represents the universal attributes. RI randomly selects $t_i \in Z_q^*$ for each attribute $i \in \mathcal{A}$ and chooses two random numbers $y, \tau \in Z_q^*$.

For subscriber revocations, each subscriber is assigned a n-bit unique revocation number (RN), denoted $X_{n-1}X_{n-2...}X_0$, where $X_i = 0|1$, $i \in Z_n$. The RN can be regarded as an unique index for updating


AND
OR
1 of 3
Class: VIP
Class: member
Rank: R
Type: Comedy
Type: Action
Type: Love
header
body
$VA, \{E_i = rT_i\}_{i\in VA}, rW$
$E' = RO \cdot e(P,P)^{yr}$
header
body
$RNA_{i,\overline{X}}, \{RE_i = rh_{i,\overline{X}_i}\}_{i\in Z_n}$
$RE' = W' e(P,P)^{\Upsilon r}$

(a) an example access control for a subscriber

(b) the encrypted right object

(c) the update message

Fig. 3. Access structure and formats of transmitting messages.

keys when the other subscribers are revoked. We use $RN_{i,X}$, where $X = 0|1$, to indicate that "the i-th bit is X." Each bit is thus associated with two attributes: $RNA_{i,0}$ and $RNA_{i,1}$, $i \in Z_n$. RI also randomly picks a number Υ from Z_q^* as the revocation master key. Let h_{i,X_i} be the corresponding element in group G of attribute RNA_{i,X_i}. We thus have

$$h_{i,0} = c_i P, h_{i,1} = d_i P,$$

where c_i and d_i are random numbers generated from Z_q^*. The public parameter values are

$$PK =< G, G_T, q, P, e, W = \tau P, \forall j \in \mathcal{A} : T_j = t_j P, \forall i \in Z_n : h_{i,0}, h_{i,1} >$$

and the master key values for RI are

$$MK = (y, \tau, \forall j \in \mathcal{A} : t_j, \forall i \in Z_n : c_i, d_i).$$

4.2 Subscriber Registration

According to the subscriber's attributes SA, RI constructs the corresponding access tree AT and computes private key values for the subscriber. Following the top-down manner starting from the root node r of AT, RI use Lagrange interpolation to generate a random polynomial q_x of degree $d_x - 1$, where d_x is the degree of node x, for each node x in AT. For a non-root node y in AT, RI sets $q_y(0) = q_{parent(y)}(index(y))$, where $parent(y)$ is the parent of node y and node y is the $index(y)$-th child of its parent. RI sets $q_r(0) = \Psi$, where q_r is the polynomial for root node r and Ψ is a random number from Z_q^*. The private key values RK for the subscriber contain

$$RK = \left\langle WD = \frac{y - \Psi}{\tau} P, \left\{ D_i = \frac{q_i(0)}{t_i} P \right\}_{i \in SA}, \left\{ DR_{j,X_j} = \begin{Bmatrix} \frac{q_1(0)\cdot\Upsilon}{c_i} P & \text{if } X_j = 0 \\ \frac{q_1(0)\cdot\Upsilon}{d_i} P & \text{if } X_j = 1 \end{Bmatrix} \right\}_{j \in Z_n, X = 0|1}, q_1(0)^{-1} \right\rangle.$$

$DR_{j,X}$ and $q_1(0)^{-1}$ (mod q) are used to update keys, and X_j is the j-th bit of the subscriber's RN. Finally, RI preloads the corresponding private key values RK to the subscriber. The delivery channel can follow that of the registration layer stated in SPP [DVB-SPP].

4.3 Rights Management Layer

When receiving requests for a video content/service, the RI can simplify the right management layer process as follows.

(1) Generate the right object (RO) $\in G_T$ containing the SEK and related parameters such as the timestamp, and assign the proper video attributes $VA \subseteq \mathcal{A}$ to associate with the RO.
(2) Select a unique random number r from Z_q^*, and calculate items $E_i = rT_i$ for each attribute $i \in VA$.
(3) Compute $E' = RO \cdot e(P, P)^{yr}$ and the encrypted RO is $ERO = (VA, \{E_i = rT_i\}_{i \in VA}, E', rW)$. Figure 3(b) shows the encrypted right object (ERO) format.

RI delivers the following message ERO to subscribers using a broadcast.

$$RI \rightarrow Subscribers : \langle ERO = (VA, E_{i \in VA}, E', r\tau P) \rangle$$

After receiving $\langle ERO \rangle$ from RI, each subscriber with his own AT and corresponding subscriber attributes SA performs the following procedures to retrieve the SEK.

(1) The decryption procedure begins from the leaf nodes and moves in a bottom-up manner. The subscriber calculates the temporal value TV_i for each leaf node i in his own AT.

$$TV_i = \begin{cases} e(D_i, E_i) = e(P, P)^{rq_i(0)}, & \text{if } i \in SA; \\ \perp, & \text{otherwise.} \end{cases} \tag{1}$$

For node x implemented as a d_x-of-n gate[3], if more than $n - d_x$ children nodes return $\perp$, TV_x is set to $\perp$. Otherwise

$$\begin{aligned} TV_x &= \prod_{i \in C_x} TV_i^{\varphi_{j,C'_x}(0)}, \text{ where } {}^{\text{j=index(i)}}_{\text{C}'_{\text{x}}\text{=\{index(i):i}\in\text{C}_{\text{x}}\text{\}}} \\ &= \prod_{i \in C_x} \left(e(P, P)^{rq_i(0)}\right)^{\varphi_{j,C'_x}(0)} \\ &= \prod_{i \in C_x} \left(e(P, P)^{r \cdot q_{parent(i)}(index(i))}\right)^{\varphi_{j,C'_x}(0)} \quad \text{(by construction)} \\ &= \prod_{i \in C_x} \left(e(P, P)^{r \cdot q_x(i)}\right)^{\varphi_{j,C'_x}(0)} \\ &= e(P, P)^{r \cdot q_x(0)} \quad \text{(using polynomial interpolation)} \end{aligned}$$

where C_x is the set of x's children nodes and $\varphi_{i,C'_x}(0)$ is the Lagrange coefficient. The subscriber can obtain $TV_r = e(P, P)^{r\Psi}$ if the subscriber's AT "accepts" the video attributes VA, which means the subscriber holds enough attributes SA to access the video content. Otherwise, the decryption procedure fails. After acquiring $e(P, P)^{r\Psi}$, the subscriber decrypts the messages as follows.

$$RO = \frac{E'}{e(WD, rW) \cdot TV_r} = \frac{RO \cdot e(P, P)^{yr}}{e(\frac{y-\Psi}{\tau}P, r\tau P)e(P, P)^{r\Psi}} = \frac{RO \cdot e(P, P)^{yr}}{e(P, P)^{ry-r\Psi}e(P, P)^{r\Psi}} \tag{2}$$

(2) After obtaining the RO, the subscriber can retrieve the SEK.

4.4 Key Stream and Content/Service Protection Layers

Because the key stream and content/service protection layers in the original SPP can enjoy the broadcast benefit, we do not modify the layers in SPP for better compatibility.

4.5 Subscriber Revocation

For subscriber revocations, all subscribers except the revoked subscriber should update the master key y embedded in WD. To revoke a subscriber with $RN = \{X_{n-1}X_{n-2...}X_0\}$, where $X_i = 0|1$, $i \in Z_n$, the RI executes the following procedures to efficiently update the master key.

(1) Choose a random number $y' \in Z_q^*$ to replace the old master key y, compute the incremental value as $\triangle y = y' - y$, and generate the new public parameter $W' = \frac{\triangle y}{\tau}P$ to replace W.

(2) Pick a random number $r \in Z_q^*$ and generate $RE' = W'e(P, P)^{\Upsilon r}$, $\{RE_i = rh_{i,\bar{X}_i}\}_{i \in Z_n}$, where $\bar{X}_i$ is the reverse i-th bit of the revoked subscriber's RN.

[3] The extreme examples are AND gate (n-of-n) and OR gates (1-of-n).

(3) Disseminate the update message $UM =< \{RNA_{i,\bar{X}}, RE_i = rh_{i,\bar{X}_i}\}_{i \in Z_n}, RE' = W'e(P,P)^{\Upsilon r} >$ as in Figure 3(c) using a broadcast.

After receiving the UM, each subscriber except the revoked one can update his secret key as follows.

(1) Determine the decryption keys by checking whether one of his/her DR_{i,X_i} can correspond to $RNA_{i,\bar{X}}$, where $i \in Z_n$, which means the i-th bit of the subscriber's RN differs from that of the revoked subscriber's.

(2) Assume that DR_{j,X_j} can match $RNA_{j,\bar{X}}$, where $j \in Z_n$. The subscriber can decrypt the UM using the decryption keys DR_{j,X_j} as follows.

$$\begin{aligned} W' &= RE'/e(DR_{j,X_j}, q_1(0)^{-1} \cdot RE_j) \\ &= W'e(P,P)^{\Upsilon r}/e(\frac{q_1(0) \cdot \Upsilon}{c_j}P, \frac{rc_j}{q_1(0)}P) \text{ if } X_j = 0; \\ &\quad \text{or} \\ &\quad W'e(P,P)^{\Upsilon r}/e(\frac{q_1(0) \cdot \Upsilon}{d_j}P, \frac{rd_j}{q_1(0)}P) \text{ if } X_j = 1. \\ &= W'e(P,P)^{\Upsilon r}/e(P,P)^{\Upsilon r} \end{aligned}$$

(3) After retrieving $W' = \frac{\triangle y}{\tau}P$, the subscriber replaces his secret key WD with $WD' = WD + W' = \frac{y-\Psi}{\tau}P + \frac{\triangle y}{\tau}P = \frac{(y-\Psi)+(y'-y)}{\tau}P = \frac{y'-\Psi}{\tau}P$.

The revoked subscriber can no longer obtain the SEK.

5. SECURITY ANALYSIS AND PERFORMANCE EVALUATION

5.1 Security Analysis

The security of the proposed scheme is based on the Elliptic Curve Decisional Bilinear Diffie-Hellman (ECDBDH) and Elliptic Curve Decisional Modified Bilinear Diffie-Hellman (ECMBDH) assumptions, which are derived from the BDH and MBDH assumptions [Sahai and Waters 2005]. The proposed scheme follows the attribute-based encryption scheme [Sahai and Waters 2005; Yu et al. 2011], which has a detailed formal proof [Sahai and Waters 2005]. We evaluate the security of the proposed scheme by examining how the security requirements listed in Section 3.2 are fulfilled.

(1) Fine-grained Access Control: To achieve fine-grained access control, the proposed scheme realizes sophisticated access control policies using the access structure AT defined by logic expressions. Only when the subscriber attributes SA match the video attributes VA and the number of matched attributes conforms to the AT, the master secret key y can be retrieved to obtain the RO. Our scheme's encryption corresponds to the attribute-based encryption [Goyal et al. 2006], which is provably secure using the ECMBDH assumption.

(2) Resistance to Collusion Attacks: To analyze collusion attacks, we assume that there is a video content with the 1st, 3th, and 4th attributes, $i = 1, 3, 4 \in VA$, and two clients SS_1 with the 1st and 5th attributes, $i = 1, 5 \in SA$ and SS_2 who possesses the 4th attribute $i = 4 \in SA$. If SS_1 colludes with SS_2 to decrypt the video content, the proposed scheme can still protect the video content, as each subscriber's private key RK is derived from its AT containing random polynomials q_i for each node i. SS_1 can collect $D_1 = \frac{q_i^{SS_1}(1)}{t_1}P$ and $D_5 = \frac{q_i^{SS_1}(5)}{t_5}P$ from himself and $D_3 = \frac{q_i^{SS_2}(3)}{t_3}P$ from SS_2, where $q_i^{SS_1}(x)$ and $q_i^{SS_2}(x)$ are the polynomials of node i in SS_1's AT and SS_2's AT, respectively. The RO cannot be correctly derived using the formula (2) because $TV_x \neq \prod_{i \in C_x} TV_i^{\varphi_{j,C'_x}(0)}$. For key

updating security, key $DR_{j,a}$ is also bound with each subscriber's polynomial $q_1(0)$. Each client keeps unique node polynomials q_i that are used to derive important keys, including RK, SEK, and the updating key. As a result, collusion attacks can thus be withstood.

(3) Nonrepudiation: In essence, the ERO is generated using elliptic curve-based ElGamal encryption [Sahai and Waters 2005] to ensure RO security. Only the RI knows both the master private key y and random number r because only the RI can offer the encrypted ERO. Assume that q is the number of elliptic curves E, the bit length of q is $b = log(q)$, and $e : G \times G \rightarrow G_T$, the number of G_T group elements: $|G_T| = 2^b$. To impersonate the RI sending the encrypted ERO, an attacker must pass the formula $e(D_i, E_i) = e(P, P)^{rq_i(0)} = e(P, P)^{r\check{y}}$ if $i \in SA$, where $\check{y}$ is the parameter chosen by the attacker to replace y. The compromise complexity is approximately $|G_T|/\mathrm{C}_2^{|G_T|} = 2/(|G_T| - 1) = 2/(2^b - 1)$, where $\mathrm{C}_2^{|G_T|}$ is the mathematic combination operation. When updating keys in the subscriber revocation, the master private key Υ and random number r are also only known by the RI. The compromised complexity is also at least $|G_T|/\mathrm{C}_2^{|G_T|} = 2/(2^b - 1)$ because $W'e(P, P)^{\Upsilon r} = W'e(P, P)^{\check{\Upsilon} r}$ must hold. Only the legal RI can thus disseminate the valid ERO and UM. When a commercial dispute occurs, the third party can take the ERO or UM with the subscriber's RK to validate formula $RO = \frac{E'}{e(WD,rW)\cdot TV_r} = \frac{RO\cdot e(P,P)^{yr}}{e(\frac{y-\Psi}{\tau}P,r\tau P)e(P,P)^{r\Psi}}$ or $W' = \frac{W'e(P,P)^{\Upsilon r}}{e(P,P)^{\Upsilon r}}$. If the RO or W' can be correctly derived from ERO or UM, then the RI cannot disclaim that the ERO or W' is not sent by him. The transmitted messages ERO or UM contain timestamps that can be used to withstand replay attacks.

(4) Backward Secrecy: In our scheme, the KP-ABE encryption [Goyal et al. 2006; Sahai and Waters 2005] protects parameter W', which is used to update the master key and ensures that all subscribers but the revoked subscriber can extract W' to calculate the new secret key WD'. To ensure that no information leaks to the revoked subscriber, we employ the attributes $\{RNA_{i,\bar{X}}\}_{i \in Z_n}$, where $\bar{X}_i$ is the i-th reverse bit of the revoked subscriber's RN. Each subscriber's RN is unique, so other subscribers have at least one RN bit that differs from the revoked subscriber's. The other subscribers thus have at least one $\{DR_{i,X}\}_{i \in Z_n}$ corresponding to $\{RNA_{i,\bar{X}}\}_{i \in Z_n}$ to extract W'. Without knowing the master private key Υ, the attacker realizes the formula $W'e(P, P)^{\Upsilon r} = W'e(P, P)^{\check{\Upsilon} r}$ with the complexity about $|G_T|/\mathrm{C}_2^{|G_T|} = 2/(2^b - 1)$ [Sun and Leu 2009].

5.2 Performance Evaluation

In this section, we have done three experiments to evaluate: (1) storage overhead, (2) retransmission efficiency, and (3) revocation waiting time. Then, a theoretical scalability analysis is presented in Appendix C.

5.2.1 *Storage Overhead.* In this section, we evaluate the storage overhead of a subscriber in our system and related works [Huang et al. 2004; DVB-SPP; Sun et al. 2008]. In our system, a subscriber is endowed with a set of attribute private keys, a set of revocation private keys, and an access structure for fine-grained access control. Related works widely adopt tree structures to attain transmission efficiency and revocation flexibility. Unfortunately, extra storage costs are demanded for security considerations. For example, the storage cost for the D2 in Figure 1 is $log(N)$, where N is the number of subscribers in only one preference group.

We discuss the following situations to compare the storage cost of a subscriber and assume the following parameters.

—SA_{Avg}. This is the average number of subscriber attributes (including channel attributes) used for access control.

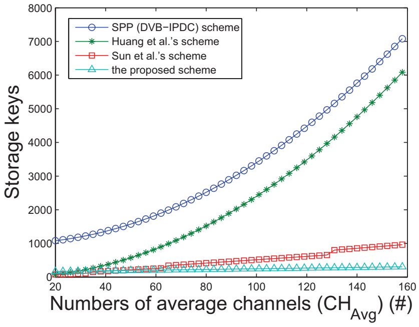


Fig. 4. Storage key comparisons.

—*B*. This is the bit number of a revocation number.

—CH_{Avg}. This is the average number of channels for a receiving (preference) group [Huang et al. 2004; DVB-SPP; Sun et al. 2008].

—G_{Avg}. This is the average number of receiving groups in a system.

—Tol_{ch}. This is the total number of channels.

—Tol_G. This is the total number of receiving groups in a pay-TV system.

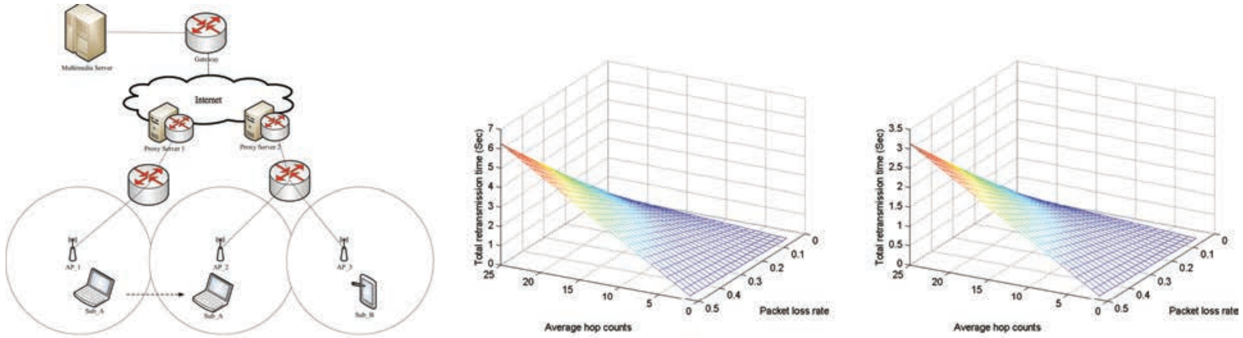
As a result, the storage costs in schemes are listed as follows.

Our scheme	[Sun et al. 2008]	[Huang et al. 2004]	[DVB-SPP]
$SA_{Avg} + B_{Avg}$	$CH_{Avg} \times log(G_{Avg}) + log(N)$ $= CH_{Avg} \times \lceil log((Tol_G/Tol_{ch}) \times CH_{Avg})\rceil$ $+ \lceil log(N)\rceil$	$CH_{Avg} \times (G_{Avg} - 1)$ $= CH_{Avg} \times ((Tol_G/Tol_{ch})$ $\times CH_{Avg} - 1)$	$(N \times Tol_G)/10000 + CH_{Avg} \times$ $((Tol_G/Tol_{ch}) \times CH_{Avg} - 1)$

For easier comparisons, we simply assume that 10000 subscribers set one BDK. Instead of group keys, our scheme can directly make a channel attribute key for each channel to distribute video content.

We take the following numerical example. Assume that a pay-TV system has 1000000 subscribers, 256 receiving groups ($Tol_G = 256$), 1024 channels ($Tol_{ch} = 1024$), and the revocation number (*RN*) is 128 bits. When $CH_{Avg} = 160$, the storage cost of our scheme is 20 (subscriber attribute keys) + 128 (revocation keys) + 160 (channel attribute keys) = 308 keys, and that of Sun et al.'s scheme is $160 \times \lceil log(0.25 \times 160)\rceil + \lceil log(10000000/256)\rceil = 160 \times 6 + 16 = 976$ keys. For Huang et al. and SPP schemes, the storage keys are $160 \times (0.25 \times 160 - 1) = 6240$ and $160 \times (0.25 \times 160 - 1) + 10000000/10000 = 7240$, respectively. Figure 4 compares our systems and other works. As a subscriber orders more channels, our scheme provides more advantages.

5.2.2 *Retransmission Efficiency.* For retransmission efficiency, our system can use buffer technology in some proxy servers to reduce retransmission overhead. Proxy servers [Yeung et al. 2005] may belong to cooperative companies to help buffer popular multimedia content, but they cannot handle key distribution tasks. Due to the prevalence of mobile devices, such as PDAs, tablets, and notebooks, subscribers may download video content from a pay-TV system anywhere at any time. Let us consider the situation shown in Figure 5(a). Two mobile subscribers, sub_A and sub_B, are classified into different groups and download the same popular video, that is, the Olympic Games. The video content is encrypted using a TEK, which is frequently changed on a 2–10 seconds basis [Wang and Laih 2008]. In traditional pay-TV systems [Huang et al. 2004; DVB-SPP; Sun et al. 2008], if sub_A moves into the communication area of AP_2, sub_A must ask the multimedia server to retransmit his specific KMM



(a) an example of mobile subscribers (b) traditional pay-TV system (c) the proposed system

Fig. 5. Retransmission scenario and time evaluation (RS = 100000, $Size_{KMM}/BW = 0.5$ sec).

to acquire the correct TEK. In our scheme, Proxy Server_2 can directly send the KMM, which has been sent to sub_B, to sub_A without using the multimedia server, because the KMM in our scheme is encrypted without depending on any subscriber's receiving group.

To demonstrate the benefit of our lightweight transmission overhead, we use the following assumptions to calculate the time saved.

—Let λ be the KMM packet loss rate [Qi et al. 2010], RS be the number of requested subscribers, hop represent the average hop counts in the transmission path, $Size_{KMM}$ indicate the KMM packet size, and BW denote the available network bandwidth.

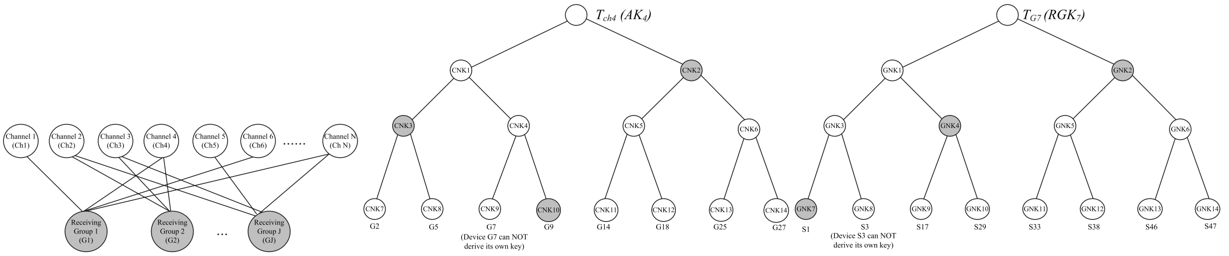
—Assume that our scheme can reach a proxy server in only half the number of hops.

—The total retransmission time for a pay-TV system in a short period is

$$RS \times \lambda \times hop \times \frac{Size_{KMM}}{BW}.$$

Figure 5 shows the retransmission time of our system and a representative traditional pay-TV system, which is DVB-SPP [DVB-SPP] in our case. In the traditional pay-TV system, the remote multimedia server has to resend the encrypted KMM to Sub_A, while our scheme takes advantage of proxy servers to retransmit the encrypted KMM to any subscriber. In general, the distance between subscribers and proxy servers is shorter than that between subscribers and the multimedia server. As a result, the total retransmission time in our scheme can be mitigated. As shown in Figure 5(b) and 5(c), when the downloading hop counts is 15 and packet loss rate is about 0.3, the total retransmission time in our scheme is 0.7 seconds and that in the traditional pay-TV one is 2.7 seconds. Note that the TEK is regularly updated in a short period, approximately 2–10 seconds [Wang and Laih 2008], so the ratio of KMM retransmissions for mobile subscribers should be high. Our scheme can effectively reduce the retransmission burden of a multimedia server, thus becoming a more suitable candidate for a "mobile" pay-TV system.

5.2.3 *Revocation Waiting Time.* In this subsection, we analyze the revocation cost of our system and group-key-based systems [Huang et al. 2004; DVB-SPP; Sun et al. 2008]. To accommodate the different preferences of subscribers, group-key-based systems classify several receiving groups into different channels. Each subscriber can then freely join a favorable receiving group. To manage those subscribers, receiving groups, and channels, the SP maintains two types of trees, as in Figure 6. When subscriber S3 classified into receiving group G7 leaves, the following steps are performed [Sun et al. 2008].



(a) relationship between channels and receiving group

(b) receiving group tree

(c) subscriber tree

Fig. 6. Example for group-key-based systems.

(1) SP broadcasts the {LEAVE, $G7$, $S3$} message.

(2) The subscribers in the other receiving groups, for example, $G2$, $G5$, $G9$, $G14$, $G18$, $G25$, and $G27$ in our example, who subscribe to the same channel T_{ch4} must update their shared channel key AK_4.

(3) The subscribers in the same $G7$ must first update their shared group key RGK_7. SP then encrypts the new channel key AK'_4 using the updated group key RGK'_7 and broadcasts the encrypted AK'_4 to the subscribers in the same $G7$.

Our scheme requires only one broadcast message to update the other subscribers' keys. We assume the following assumptions to measure the waiting time for each subscriber.

—M is the number of total subscribers,

—N denotes the number of subscribers in a group,

—I_{ch} represents the number of groups who subscribe to the same channel,

—CH_{Avg} this is the average number of channels for a receiving (preference) group in systems.

Some messages can be transmitted to multiple subscribers in parallel. Table II summarizes the revocation costs of group-key-based systems and of ours. Group-key-based systems require M messages for step (1), $CH_{Avg} \times (I_{ch} \times N)$ messages for step (2), and $N - 1$ messages for step (3). In our scheme, M messages are transmitted to broadcast the leaving messages that contain update parameters. As a practical experiment, we conduct a simple simulation[4] using NS2 [ns 2] according to the topology shown in Figure 5(a).

The average waiting time including transmission and verification delay for a subscriber is shown in Figure 7. When the number of channels in a receiving group is plenty, the waiting time is longer since more receiving groups and subscribers have to update their keys. Fortunately, our scheme consumes less waiting time than Sun et al.'s scheme does, because the number of message transmissions in our scheme is reduced. The extra cost of our scheme is to slightly increase the packet length of the leaving message. Thanks to the fewer bit advantage of elliptic curve cryptography, the increment can be small.

5.2.4 *Scalability Analysis.* Please refer to Appendix C.

5.2.5 *Performance Comparison with Group-Key-Based Systems.* In this section, we examine the detailed performance evaluation of the proposed system compared to that of group-key-based systems including the SPP system [DVB-SPP] adopted by DVB-IPDC, Sun et al. [2008], and Wang and Laih [2008] in Table II.

[4] The wired channel capacity is set to 100 Mb/s, and wireless channel capacity is 6 Mb/s, the delay for T_{pair} is 4.5 ms, the delay for T_{mul} is 0.6 ms [Zhu et al. 2009], and the delay for T_{symm} is 0.005 ms.

1.21.3

Table II. Performance Comparisons

	Group-key-based systems	Our system
Security foundation	Zero message tree Symmetric encryption	Attribute-based encryption Symmetric encryption
Security properties	Confidentiality Integrity Authentication	Confidentiality\integrity Authentication\authorization Nonrepudiation
Key distribution	One-to-group*	One-to-many
Computational cost for key distribution	RI: $(1T_{search} + 1T_{sym}) \times Num(groups)$ Subscriber: $N \cdot T_{sym}$	RI: $(Num(VA) + 1) \cdot T_{mul}$ Subscriber: $d \cdot T_{pair} + 1T_{mul}$
Bandwidth cost	$\lceil \frac{M}{N} \rceil \times Size_{KMM}$	$22 \times i + Size_{KMM}$
Number of messages for user revocation	$M + CH_{Avg} \times (I_{ch} \times N)) + N - 1$	M

*: Depending on the number of groups of requested subscribers, M: The number of all subscribers, N: the number of subscribers in a group, i: The number of attributes of a video content (usually no more than 10).

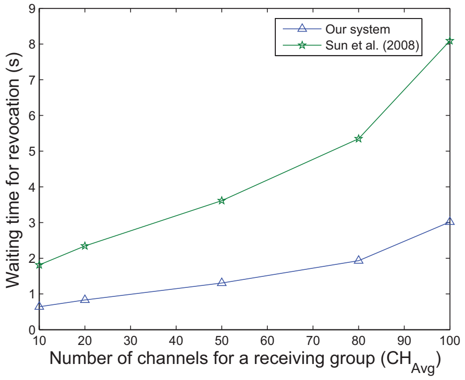


Fig. 7. Average waiting time for a subscriber in user revocation.

(1) Security foundation. Most group-key-based systems adopt the symmetric encryption cryptosystem to deliver the Key Management Messages (KMMs), while our proposed system is based on Attribute-Based Encryption (ABE), a variant of public-key-based encryption. The advantages of symmetric encryptions are lower computational costs and broadcast efficiency. However, it does have some weaknesses, including collusion attacks [DVB-SPP], no nonrepudiation property, and small group sizes, which limit the broadcast virtues in DVB-H/SH standards. To overcome these disadvantages, the proposed scheme adopts attribute-based encryption. For commercial businesses, the vital nonrepudiation property is provided, and collusion attacks can be withstood in the proposed scheme. The key distribution is independent of the number of requested subscribers, which fully brings the benefit of DVB-H/SH. To reduce the ABE computational costs, the elliptic curve-based ABE is developed for fewer computational bytes without compromising security strength.

(2) Security properties. For security properties, the SPP system focuses on data confidentiality, integrity, and authentication. To further enhance the important security properties for commercial businesses, the proposed scheme also provides the nonrepudiation properties and sophisticated authorization (or fine-grained access control).

(3) Key distribution. In SPP, the distribution of KMMs containing *SEK* depends on the number of groups of requested subscribers. If all requesting subscribers belong to the same group, only one broadcast transmission is demanded. However, the probability of this case is extremely low, as shown in Appendix C. We categorize this key distribution in a one-to-group fashion. In the proposed scheme, the KMM distribution can always enjoy the one-to-many advantage regardless of the requesting subscribers.

(4) Relevant to the number of key transmissions. Let $Size_{KMM}$ be the length of a Key Management Message (KMM), M be the number of all subscribers, and N be the number of subscribers in a group. The number of groups is then $\lceil \frac{M}{N} \rceil$. According to the scalability analysis, if the number of requesting subscribers is large, the KMM may be delivered as many times as there are groups. The SPP bandwidth cost is thus $\lceil \frac{M}{N} \rceil * Size_{KMM}$. Our scheme requires extra attribute parameters for the requested video content, although the KMM must only be broadcast once. Let i be the number of attributes of a video content. In the proposed scheme, each item E_i spends 21 bytes[5], and the index of each attribute is 1 byte. The bandwidth cost of the proposed scheme is thus $22 \times i + Size_{KMM}$.

(5) Computational cost. Here, we consider the computational cost of delivering a KMM to the requesting subscribers. Let T_{sym} be the time required to perform an encryption/decryption operation for a symmetric cryptosystem, T_{search} be the time to locate the proper group keys using the IEK key, T_{mul} be the time to perform one point multiplication over an elliptic curve, and T_{pair} be the time to perform a pairing operation. We only consider the dominant operations and ignore the lightweight ones, including hash functions and polynomial operations. In group-key-based systems, the computational cost is $(1T_{search} + 1T_{sym}) \times Num(groups)$, where $Num(groups)$ is the number of groups of requesting subscribers, where RI and $(N - 1 + 1) \cdot T_{sym} = N \cdot T_{sym}$ for each subscriber. Here, $(N - 1) \cdot T_{sym}$ is the time required to derive keys, as discussed in Section 2.2. The computational cost of the proposed scheme is $(Num(VA) + 1) \cdot T_{mul}$, where $Num(VA)$ is the number of video attributes of the requested video content, for RI and $d \cdot T_{pair} + 1T_{mul}$, where d is the number of attribute set overlap, that is, $d = Num(SA \cap VA)$, for each subscriber. If the number of requesting subscribers is not large, the proposed scheme may not perform as quickly as the SPP system in DVB-IPDC. Considering the overall bandwidth cost and security properties, including nonrepudiation, sophisticated authorization and collusion attacks resistance, the extra computational cost is worth spending. Moreover, according to Moore's law, the computational power continues growing, although the bandwidth is fixed. The computational cost thus cannot obscure the virtues of the proposed scheme.

5.2.6 *Qualitative Comparisons.* In this section, we compare the proposed scheme to some recent related works using the qualitative analysis in Table III.

(1) Cryptosystem. Group-key-based symmetric cryptosystems are used to ensure the security of encryption key distribution and video content delivery [DVB-SPP; Wang and Laih 2008; Sun et al. 2008]. In a previous study [Sun and Leu 2009], the Elliptic Curve Cryptosystem (ECC) is adopted for subscriber authentication, and it uses a symmetric cryptosystem for video content delivery. Our scheme employs attribute-based encryption for encryption key distribution and a symmetric cryptosystem for video content delivery.

(2) Authentication message delivery. Previous studies [Wang and Laih 2008; Sun et al. 2008] consider an Entitlement Management Message (EMM), which is similar to the Key Management Message (KMM) in SPP scheme [DVB-SPP], an authentication message. Because each subscriber's unique

[5] The security level of 160-bit key length in Elliptic Curve Cryptography (ECC) is strong as that of 1024-bit key length in RSA.

Table III. Functionality Comparisons

	[Wang and Laih 2008]	[Sun et al. 2008]	[DVB-SPP]	[Sun and Leu 2009]	Ours
Cryptosystem	GK^1 symmetric	GK^1 symmetric	GK^1 symmetric	ECC^2 + symmetric	ABE^3 + symmetric
Authentication message delivery	One-to-one	One-to-one	One-to-one	One-to-few^4	One-to-many
Key Distribution	One-to-group^5	One-to-group	One-to-group	One-to-few	One-to-many
Nonrepudiation	No	No	No	Yes	Yes
Fine − grained access control	No	No	No	No	Yes
Subscriber revocation	Yes	Yes	Yes	No	Yes
Resistible colluision attack	No	No	No	Yes	Yes
Resistible authentication failure	Yes	Yes	Yes	No	Yes

1: Group-Key-based, 2: Elliptic Curve Cryptography, 3: Attribute-based Encryption, 4: multiple subscribers arriving in little time, 5: Depending on the number of groups of requested subscribers.

Master Private Key (MPK) encrypts the EMM, the authentication message delivery using such schemes is only suitable for a one-to-one transmission. A previous study [Sun and Leu 2009] cleverly utilizes the homomorphic property of ECC parameters to simultaneously authenticate several subscribers' requests arriving in a short period of time, which can be classified into a one-to-few relationship. Our scheme associates the KMM with proper attributes, not a specific MPK, because the authentication message in our scheme can be delivered using a one-to-many relationship.

(3) Key distribution. The distribution of KMMs containing SEK has previously depended on the number of groups of the requested subscribers [DVB-SPP; Wang and Laih 2008; Sun et al. 2008]. If all requesting subscribers belong to the same group, only one broadcast transmission is demanded. The probability of this case is extremely low, as shown in Appendix C. We categorize this type of key distribution using a one-to-group relationship. In Sun and Leu [2009], SP will certify a group authorization key for multiple requests arriving in a short period of time, meaning that the key delivery uses one-to-group transmission. In the proposed system, the KMM distribution can always enjoy the one-to-many advantage regardless of the requesting subscribers.

(4) Nonrepudiation property. Previous studies adopt symmetric cryptosystems [DVB-SPP; Wang and Laih 2008; Sun et al. 2008]; they do not support the nonrepudiation property. Conversely, [Sun and Leu 2009] and our scheme are based on Elliptic Curve Cryptography (ECC) and Attribute-Based Encryption (ABE), which belong to public-key cryptosystems. The nonrepudiation property can thus be upheld.

(5) Fine-grained access control. Among these schemes, only our scheme offers fine-grained access control to satisfy sophisticated access policies such as customer classes, video types, and a film rating system. To support fine-grained access control, schemes [Wang and Laih 2008; Sun et al. 2008] may take the method used in a previous study [Huang et al. 2004]. However, that method may incur more complicated key management problems [Sun and Leu 2009].

(6) Subscriber revocation. To support the subscriber revocation function, a scheme must be able to update keys without leaking new keys to the revoked subscriber. Based on symmetric cryptosystems, schemes [Wang and Laih 2008; Sun et al. 2008; DVB-SPP] rely on a tree-based technique to update keys, which is similar to the ZMB scheme introduced in Section 2.3. Sun and Leu [2009] do not consider the subscriber revocation issue. The proposed scheme can efficiently execute the update key procedure, as depicted in Section 4.5. The update key transmission in our scheme can still enjoy the one-to-many facility.

(7) Resistible to collusion attacks. As mentioned in [DVB-SPP], group-key-based schemes [Wang and Laih 2008; Sun et al. 2008] are vulnerable to collusion attacks. Conversely, the pubic-key-based scheme [Sun and Leu 2009] can easily resist collusion attacks. Section 5 analyzes the collusion attack security of our scheme.

(8) Resistible to authentication failure. In previous schemes [Wang and Laih 2008; Sun et al. 2008; DVB-SPP], an authentication failure for a single subscriber does not affect the authentication for others because each subscriber is independently authenticated. However, in Sun and Leu [2009] an authentication failure for a single subscriber impedes the authentication for others due to parameter aggregations. Fortunately, our scheme also tolerates a single user's authentication failure because each subscriber authentication is also independent.

6. CONCLUSIONS

In this article, a scalable and fine-grained access control is proposed with not only essential security properties but also efficiency and scalability features. The proposed scheme is also compatible with the current popular digital video broadcast standards, including DVB-H/SH. Some elaborate merits such as nonrepudiation, fine-grained access control, and an efficient subscriber revocation procedure are offered. Based on a novel attribute-based encryption, the broadcast virtue is no longer confined to the group size limitation. Taking advantage of a unique revocation number, our scheme can efficiently update each subscriber's master key to shorten the revocation waiting time. To the best of our knowledge, this is the first attempt to combine the merits of group-key-based and public-key-based access schemes and support sophisticated authorization (e.g., fine-grained access control) in mobile pay-TV systems. The limitations of our scheme are a time-consuming registration procedure because of fine-grained permission assignments and some lightweight cryptographic operations used in mobile devices. Our future work is to dynamically support changes in subscribers' access rights.

REFERENCES

CONDITIONAL-ACCESS BROADCASTING SYSTEM. 1992. ITU-R rec. 810, itu recommendation. http://www.itu.int/dms_pubrec/itu-r/rec/bt/R-REC-BT.810-0-199203-W!!PDF-E.pdf.

DIGITAL VIDEO BROADCASTING (DVB-H). 2004. Transmission system for handheld terminals. ETSI en 302 304, dvb technical specification. http://www.dvb-h.org/technology.htm.

DIGITAL VIDEO BROADCASTING (DVB-SH). 2007. System specifications for satellite services to handheld devices below 3 ghz. ETSI ts 102 585, dvb technical specification. http://www.dvb-h.org/technology.htm.

DIGITAL VIDEO BROADCASTING (DVB-SPP). 2007. Ip datacast over dvb-h: Service purchase and protection. ETSI ts 102 474, dvb technical specification. http://www.dvb-h.org/technology.htm.

DVB-H. http://en.wikipedia.org/wiki/DVB-H.

FIAT, A. AND NAOR, M. 1994. Broadcast encryption. In *Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology.*

GOYAL, V., PANDEY, O., SAHAI, A., AND WATERS, B. 2006. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS'06)*. 89-98.

HUANG, Y.-L., SHISH, S., HO, F.-S., AND WANG, J.-C. 2004. Efficient key distribution schemes for secure media delivery in pay-tv systems. *IEEE Trans. Multimedia 6*, 5, 760–769.

DAEMEN, J. AND RIJMEN, V. 2002. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer.

KORNFELD, M. AND MAY, G. 2007. Dvb-h and ip datacast–broadcast to handheld devices. *IEEE Trans. Broadcast. 53*, 1, 161–170.

NS 2, T. N. S. Network Simulator. *ACM Trans. Appl. Percept. 2*, 3.

QI, Q., CAO, Y., LI, T., ZHU, X., AND WANG, J. 2010. Soft handover mechanism based on rtp parallel transmission for mobile iptv services. *IEEE Trans. Consum. Electron. 56*, 4, 2276–2281.

ROH, H. AND JUNG, S. 2011. An authentication scheme for consumer electronic devices accessing mobile iptv service from home networks. In *Proceedings of the IEEE International Conference on Consumer Electronics (ICCE'11)*. 717–718.

SAHAI, A. AND WATERS, B. 2005. Fuzzy identity-based encryption. In *Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Lecture Notes in Computer Science, vol. 3494, Springer, 457–473.

STADDON, J., MINER, S., FRANKLIN, M., BALFANZ, D., MALKIN, M., AND DEAN, D. 2002. Self-healing key distribution with revocation. In *Proceeding of the IEEE Symposium on Security and Privacy.*

SUN, H.-M., CHEN, C.-M., AND SHIEH, C.-Z. 2008. Flexible-pay-per-channel: A new model for content access control in pay-tv broadcasting systems. *IEEE Trans. Multimedia 10*, 6, 1109–1120.

SUN, H.-M. AND LEU, M.-C. 2009. An efficient authentication scheme for access control in mobile pay-tv systems. *IEEE Trans. Multimedia 11*, 5, 947–959.

WALDVOGEL, M., CARONNI, G., SUN, D., WEILER, N., AND PLATTNER, B. 1999. The versakey framework: Versatile group key management. *IEEE J. Select. Areas Comm. 17*, 9, 1614–1631.

WANG, S. Y. AND LAIH, C. S. 2008. Efficient key distribution for access control in pay-tv systems. *IEEE Trans. Multimedia 10*, 3, 480–492.

YEUNG, S. F., LUI, J. C. S., AND YAU, D. K. Y. 2005. A multikey secure multimedia proxy using asymmetric reversible parametric sequences: Theory, design, and implementation. *IEEE Trans. Multimedia 7*, 2, 330–338.

YU, S., REN, K., AND LOU, W. 2011. Fdac: Toward fine-grained distributed data access control in wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst. 22*, 4, 673–686.

ZHU, H., LIN, X., SHI, M., HO, P.-H., AND SHEN, X. 2009. Ppab: A privacy-preserving authentication and billing architecture for metropolitan area sharing networks. *IEEE Trans. Vehic. Technol. 58*, 5, 2529–2543.

ZHU, W. T. 2008. A cost-efficient secure multimedia proxy system. *IEEE Trans. Multimedia 10*, 6, 1214–1220.

Received February 2012; revised October 2012; accepted October 2012