Key Management for Versatile Pay-TV Services

Kazuto Ogawa[1](✉), Sakurako Tamura[2], and Goichiro Hanaoka[3]

[1] Japan Broadcasting Corporation, Tokyo, Japan
ogawa.k-cm@nhk.or.jp
[2] NTT Secure Platform Laboratories, Tokyo, Japan
tamura.sakurako@lab.ntt.co.jp
[3] National Institute of Advanced Industrial Science and Technology, Tokyo, Japan
hanaoka-goichiro@aist.go.jp

Abstract. The content of pay-TV services is encrypted and each subscriber has a security module that holds a decryption key. When subscribers want to receive the same pay-TV services that they receive at home outside their homes, they have to bring the security module with them. However, it is not easy to take the module out of the TV set. To enrich current and conventional pay-TV services and to make it easier for subscribers to obtain pay-TV services outside their homes, we propose a key management system using a temporary key, an attribute-based encryption (ABE) scheme, and a mobile terminal. The temporary key is not a conventional key, but has a backward compatibility. The ABE is used to restrict the time and location when and where the temporary key can be used. The mobile terminal has a role to take secret data related to the temporary key and ABE. In this system, a certain decryption key sk_t is stored in the mobile terminal. sk_t is used to decrypt a content key. Since sk_t is stored in a mobile terminal, it is vulnerable to being leaked. To protect services from such key leakage, we add a function to control when and where sk_t can be used. To introduce such a restriction, we employ an ABE scheme. The system uses ABE to exchange certain secret data between broadcasters and subscribers through communication networks. This key management system is secure against key leakage and enables subscribers obtain pay-TV services their homes.

Keywords: Pay-TV services · Functional encryption · Attribute · Valid period · Mobile terminal

1 Introduction

1.1 Background

Broadcasting and cable TV services encrypt their content before distributing it to subscribers for the purpose of copyright protection. Each subscriber needs a decoder with a security module for decrypting the content. In Japan, a smart card is used as a security module in broadcasting, and a decryption key is generated in the card [27]. Pay-TV services use the card to control the subscriber's

G. Livraga and C. Mitchell (Eds.): STM 2017, LNCS 10547, pp. 3–18, 2017.
DOI: 10.1007/978-3-319-68063-7_1

access to their content. In particular, the card holds the subscriber's contract information, and decryption keys are generated from the information in the card.

If the card can be taken out of the TV receiver or set-top box, in principle, subscribers can get services outside the home. However, it is not easy to take the card out of receiver; in fact, breakage of cards is a concern.

On the other hand, if the decryption key(s) could be stored in mobile devices such as mobile phones and tablet PCs, subscribers would not need to take the card out or bring it with them. In this way, quality of service would be improved.

Nowadays, people can use hybrid systems, such as youview [32], HbbTV [30], Hulu [31], and Hybridcast [29], to obtain both broadcasting services through the air and network services through the Internet. In these systems, TV receivers and mobile terminals cooperate. This means that it becomes easy to transmit data from a receiver to a mobile terminal. However, when a third party can use the data transmitted into the mobile terminal, illegal use becomes a potential problem; particularly, copyrights may be infringed. Hence, when the data can be transmitted into the mobile terminal, countermeasures against illegal use of that data should be taken. Ogawa, Hanaoka, and Imai (OHI07) [20] proposed a method in which a decryption key is updated periodically and a temporary decryption key can be carried outside in order to enrich the current and conventional services. That is, the subscriber can obtain the same service outside as he or she would receive at home only during a limited period. Thus, even if the decryption key is leaked, the damage it causes would not extend beyond the valid period of the key.

1.2 Contributions

OHI07 controls a time during which a decryption key can be used. We extend this control and propose a key management system that can control when and where the key can be used. OHI07 cannot control the location of use and it is difficult to add a control function to it for this purpose.

First, we consider a situation in which a subscriber carries decryption keys and obtains the same services outside that they receive at home, e.g., someone travelling on business or sightseeing. In such a situation, where the subscriber stays during the period is likely decided before leaving home. Here, let us suppose that the subscriber would want to obtain services while staying at a hotel. Furthermore, the time during which the subscriber obtains the services at the hotel is limited. Then, generating a decryption key that can be used at the hotel and at the time and storing the key in the mobile terminal electronically makes it possible to obtain the expected services at the time and location the subscriber wants.

In the proposed system, we introduce a temporary work key k_{w_t} and a functional encryption scheme (FE) [1,3,7,18,21], and use a mobile terminal. Particularly, FE is an efficient tool to restrict the time and location. More concretely, we use an attribute-based encryption scheme (ABE) [4,6,12,15] that is a kind of FE and that can control each subscriber's access to content (data) according to the subscriber's attribute.

We will use the following travel situation as an example:

- travel destination (hotel location): XYZ hotel in Oslo, Norway
- travel duration: 9/11–15.

These data are used as attributes in the ABE scheme. However, it is impossible to substitute the current encryption schemes with the ABE scheme, since there are a lot of subscribers who have receivers that only work the current encryption scheme. To have backward compatibility, we need to add functions to the current systems. That is, the new system should not supersede the current system. It should use ABE to encrypt certain personal data of the subscriber. Hence, the ABE-encrypted data should not be transmitted through the air, because the capacity of broadcasting channels is not so large. Here, we introduce a temporary work key k_{w_t}, which plays a similar role as the current work key k_w and which has a valid period. A function to encrypt a content key k_s by using k_{w_t} is added to the current system. k_s is encrypted by using k_w and k_{w_t} simultaneously, and two versions of the ciphertext of k_s are transmitted simultaneously.

A function to encrypt k_{w_t} by using ABE is added to the current system. Before a subscriber gets k_{w_t}, the decryption key sk_t of ABE is generated under conditions of the above attributes. The subscriber obtains it through the communication networks, stores sk_t in the mobile terminal, and brings it to the travel destination. The data stored in the mobile terminal is sk_t, not a ciphertext of k_{w_t}, because the broadcasters mind that the k_{w_t} is extracted from the ciphertext and sk_t does not include any information on k_{w_t}. A ciphertext of k_{w_t} is necessary at the hotel; in this case, it is transmitted through communication networks to the mobile terminal just before it receives the services. The capacity of the broadcasting channel is not large, and using the communication networks enables the real-time property to be kept.

The proposed system uses two time and location data: data collected when the subscriber is at home and data when the subscriber measures at the hotel. Naturally, there are errors in these data, and then, we chose an ABE scheme that can specify the range of attributes carefully among a lot of ABE schemes.

By these techniques, the subscriber uses sk_t and the ciphertext of k_{w_t} to enjoy the enriched services.

1.3 Related Work

Our key management system uses time and location data as attributes of the key to control the access to the content. As far as we know, there has not been any related proposal except for OHI07 regarding access control to Pay-TV services and OHI07 cannot control the location where the decryption key is used.

However, a position based cryptography scheme (PBC) [9,11,14,23], which controls the decryption of a ciphertext according to the location the message sender specifies, and time released encryption scheme (TRE) [5,13,16,17, 19,22,26], which controls the decryption of a ciphertext according to the time the message sender specifies, can be used for the same purpose. That is, by considering position data as an attribute, PBC can be viewed as a kind of ABE, and because the time data be considered an attribute, TRE can also be viewed as a kind of ABE.

For PBC, a correct and unmodified position should be used, or else the security of the ciphertext cannot be guaranteed. For this reason, position authentication has been studied [9,23]. The basic idea involves a measurement of the response. That is, the speed of the response depends on the distance between the sender and receiver, and hence, the measurement of the response speed is an effective method against spoofing of the position. The concept was first proposed by Brands and Chaum [8]. Chandran et al. used a query challenge for this measurement [10]. Dziembowski and Zdanowicz's scheme [14] assumes a noisy measurement channel. Chandran et al. later proposed a scheme using a bounded storage model [11].

By considering position data as an attribute, PBC can be viewed as a kind of ABE. Although studies on PBC schemes are on the decline for this reason, a lot of protocols that control something using position data, including ones for RFIDs, car security, applications using GPS, etc., have been developed.

May proposed the first TRE [19]. Hwang et al. scheme [16] decrypts the ciphertext before the appointed time by using an additional release key. Baek, Safavi-Naini, and Susilo proposed a scheme [5] that generates a decryption key by using a token published periodically by a trusted third party (TTP). Yoshida et al. [26] improved Baek et al.'s scheme; their scheme can generate a decryption key at a later time than the appointed one. Dent and Tang [13] revised the security model of Hwang et al.'s scheme and proposed a new approach using KEM-DEM frameworks. Paterson and Quaglia' scheme can specify a certain time range [22]. Kasamatsu et al. proposed a scheme [17] whose computational cost and data sizes are small and that has forward security.

Because the time data can be considered an attribute, TRE can also be viewed as a kind of ABE. Currently, the studies are included in that on ABE.

A combination of PBC and TRE can realize the access control to the content, which allows the subscribers obtain outside the home identical services to those inside the home. However, two distinct encryption schemes would have to be used in both encryption and decryption, and this is inefficient.

2 Preliminaries

2.1 Current Broadcasting System

There are a lot of pay-TV services in North America, Europe, and Asia. The systems in North America and Europe are various from broadcaster to broadcaster, and their details are not disclosed. Although the Common Descrambling System of Digital Video Broadcasting (DVB-CSA) [28] is standardized in Europe, non-disclosure agreement is necessary to see its details, and naturally, the details cannot be disclosed. On the other hand, Japanese broadcasting system is disclosed. Figure 1 shows the current broadcasting system used in Japan [27].

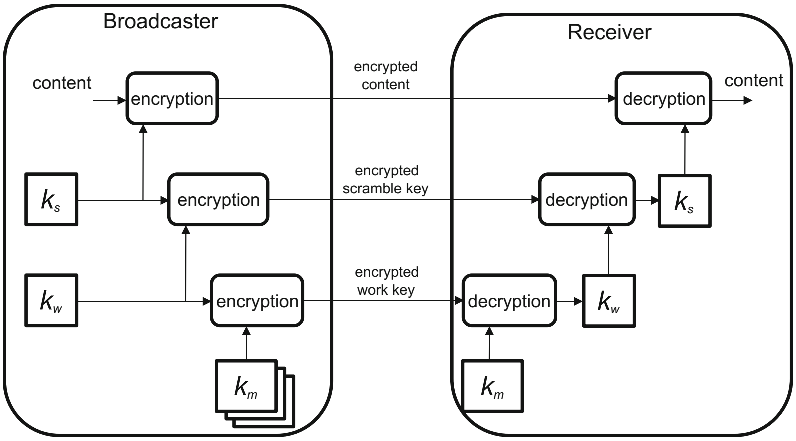

Fig. 1. Current broadcasting system: k_s is a content (scramble) key, k_w is a work key, and k_m is a master key.

The broadcaster encrypts the content M by using a scramble key k_s. It broadcasts the encrypted content $C_M = Enc(k_s, M)$. $Enc(k, M)$ denotes that the plaintext M is encrypted by using a key k. k_s is encrypted by using a work key k_w, and the broadcaster generates an encrypted scramble key $C_{k_s} = Enc(k_w, k_s)$. In addition, k_w is encrypted by using a master key k_m, and the broadcaster generates an encrypted work key $C_{k_w} = Enc(k_m, k_w)$. C_M, C_{k_s}, and C_{k_w} are multiplexed and transmitted to the subscribers.

There are multiple symmetric encryption schemes in the Japanese system. That is, the scrambling scheme used for content encryption is different from the encryption scheme used for k_s and k_w encryption. This difference does not affect the proposed system. Hence, we use the same notation $Enc(\cdot, \cdot)$ as in symmetric encryption.

Each receiver needs a smart card as a security module that holds a k_m. It should be noted that each smart card has a distinct k_m and the broadcasters can transmit private contract information to each subscriber (receiver) by using this k_m. C_M, C_{k_s}, and C_{k_w}, which are transmitted through the air, are demultiplexed in the receiver. k_w is decrypted by using k_m in the smart card as follows: $k_w = Dec(k_m, C_{k_w})$. $Dec(k, C)$ denotes that a ciphertext C is decrypted by using a key k. k_s is decrypted by using k_w: $k_s = Dec(k_w, C_{k_s})$. k_s is sent to the receiver, and M is decrypted (descrambled) by using k_s: $M = Dec(k_s, C_M)$ in the receiver.

Since all the encryption schemes are symmetric, their encryption and decryption keys are identical. Regarding decryption, the descrambling scheme used for content decryption is different from that of k_w and k_s decryption in the actual Japanese broadcasting system, but this difference does not affect the proposed system. Hence, we use the same notation $Dec(\cdot, \cdot)$.

2.2 Functional Encryption (Attribute-Based Encryption)

FEs [4,6,12,15] are public key encryption schemes that have advanced functionalities. ABEs are included in the FEs and can prescribe the logic of encryption or decryption by embedding attributes or conditions of attributes into a ciphertext or a decryption key. Arbitrary functions, described as combinations of AND gates, OR gates, NOT gates, and threshold gates, are possible conditions.

Ciphertext-policy ABE is a kind of ABE that embeds attribute data into a decryption key and a policy (condition), such as Boolean formula, into a ciphertext. It consists of the following four algorithms ($\mathsf{ABE\_Setup}$, $\mathsf{ABE\_Gen}$, $\mathsf{ABE\_Enc}$, $\mathsf{ABE\_Dec}$).

- $\mathsf{ABE\_Setup}(1^\lambda) \rightarrow (msk, pk)$: The set-up algorithm takes a security parameter 1^λ as an input and outputs a master key msk and a public key pk.
- $\mathsf{ABE\_Gen}(msk, S) \rightarrow sk$: The decryption key generation algorithm takes msk and attributes of a decryption key S as inputs and outputs a decryption key sk.
- $\mathsf{ABE\_Enc}(pk, \beta, M) \rightarrow C$: The encryption algorithm takes pk, attributes and its condition β, such as a Boolean function, and a message M as inputs and outputs a ciphertext C.
- $\mathsf{ABE\_Dec}(sk, C, \beta) \rightarrow M$: The decryption algorithm takes sk, C, and β as inputs and outputs M.

The proposed system uses the above ciphertext-policy ABE, more specifically, one in [4] that can assign an attribute with a range. The range is included in β.

3 Proposal: Key Management System

There are two kinds of broadcasting service: through the air (via the broadcasting satellite, communication satellite, or terrestrial station) and through communication cable networks. The ones through the air provide the same services to subscribers in a wide area, while the ones through cables provide services in a limited area.

In this paper, we consider a situation in which a subscriber travels to a certain destination and wants to obtain services there that are identical to ones he or she receives at home. That means wider service area is preferable. Hence, we will focus on services through the air. In addition, we assume that the subscriber signed a contract with a certain broadcaster and can obtain services at home. In the proposed system, this services are extended and the subscribers can obtain services outside the home.

Below, we explain how to apply the system to the Japanese broadcasting system as an example.

3.1 Discussion: Bringing Current Keys

The simplest way to obtain the same services outside the home is to bring a security module from the home to the destination. However, it is difficult to dismount the security module even if it is a smart card.

Let us consider the way to take out the keys, k_s, k_w, and k_m, used in the current system. If the subscriber takes them out from the security module electronically, stores it in his/her mobile terminal, and transmits the key from the mobile terminal to the receiver at the hotel electronically, he or she can easily obtain the desired services outside the home.

k_s is updated every two seconds and it is not practical to bring all k_s's used during travel, as the number of keys would be enormous.

k_w's update period varies from channel to channel and broadcaster to broadcaster, but the key is not updated as frequently as the change of on-air programs. That is, an update of k_w leads to an update of the subscriber's contract, and from the viewpoint of the service continuity, it is impossible for the contract to change as frequently as an on-air program. If the subscriber has a long-term contract, such as several months, with a broadcaster, it is easy for the broadcaster to continue to use the same k_w for several months. However, such long-term use leads to risk of key exposure and is not preferable from the viewpoint of security. Even if there is a long-term contract, k_w should be updated periodically; in practice, it is updated almost every month. Although it is possible to take out k_w and this might be practical in the sense that the number of keys that the subscriber should carry is small, its valid period is too long considering the potential damage caused by its exposure. Broadcasters would thus prefer shorter term keys.

k_m is used only when contract between a broadcaster and a subscriber is changed or updated or when k_w is updated. Hence, it is not appropriate to take out k_m to obtain services outside the home without any contract change.

From the above discussion, there is no adequate key among the three that can be taken out. Instead, what is required is a key that acts as a work key and that has a moderately long valid time.

3.2 Discussion: Key Transmission Through the Air

In the previous section, k_s should not be taken outside from the viewpoint of the number of keys and k_w should not be taken outside from the viewpoint of the valid term of keys. In this section, we show that an encrypted k_s or k_w should not be transmitted through the air for the private use of this extended service, either.

When the encrypted k_s is transmitted, a distinct encryption key must be used for each subscriber. When the number of subscribers is small, the broadcaster can transmit the encrypted k_s's through the air, but when the number is large, the limited transmission capacity of broadcasting makes this difficult. That is, the amount of additional transmitted data increases in proportion to the number of subscribers, since every encrypted k_s is different from that for the other subscribers. For example, it would take about one hour for the data to be sent to every security module in Japan. Although the number of people who spend time outside the home during the golden week, silver week, summer, and New Years holidays in Japan is smaller than the number of all security modules, it is still a huge number. Assuming that almost all vacationers would want to use the proposed system, it would take too long a time to transmit the encrypted k_s's; k_s changes every two seconds, so it would be impossible to transmit all encrypted k_s in real-time. As one of the strong points of broadcasting is that it provides identical services simultaneously to all subscribers, but the loss of the real-time property would eliminate it. Hence, it is not practical to transmit encrypted k_s's through the air.

Now let us consider transmitting an encrypted k_w through the air for the private use of the extended service. k_w is a long-term key, and it is not necessary to transmit an encrypted k_w or decrypt it in real-time. That is, although the subscriber has to wait until the encrypted k_w to be transmitted for the service to start, after it is decrypted, he or she can seamlessly obtain services in real-time. In this sense, k_w is more adequate than k_s. However, k_w is common for all subscribers. That is, once k_w is decrypted, it can be used at any time (sometimes for several months) and at any location even when and where the subscribers assigned before the travel. The damage caused by the leakage of k_w would thus be unacceptably large from the viewpoint of content copyright protection. Finer control of the time and location is required.

3.3 Discussion: Use of Mobile Terminal and Attribute-Based Encryption Scheme

If the mobile terminal of a subscriber stores a key, there is a risk that the key may be leaked unintentionally or intentionally. The leaked data can be easily copied, and a broadcaster cannot use a system that does not have any countermeasure against such leakage. It is difficult to sweep the anxious away, but it is important to take a measure not to extend the damage caused by the key leakage.

We need finer control of the key. In Sect. 3.1, we described that it is not preferable to take out k_s, k_w, and k_m because of their roles, importance to maintaining security, and number. The discussion in Sect. 3.2 indicates that it is not preferable to transmit k_s and k_w through the air for the private extended service to the subscriber because of the lack of transmission capacity and security. In addition, it was pointed out that keys that act together a work key and that have a moderately long valid time and fine control of when and where the subscriber receives services are required. We thus introduce a temporary work key k_{w_t} and the ABE scheme. In the following, we discuss how k_{w_t} can be used to realize a secure key management system.

The system we propose minimizes the damage caused by leak of data stored in the mobile terminal and can control when and where the data can be used. We employ an FE, especially an ABE. We use the location of the hotel, and the travel date as attributes of ABE. The attributes make it possible to control when and where a leaked key can be used and to lessen the value of the key to other people.

The easy way to use ABE is that a broadcaster encrypts k_w by using ABE and transmits the encrypted k_w. In this case, a subscriber carries a decryption key and decrypts k_w at the hotel. However, as described in Sect. 3.1, it is not preferable to have subscribers bring k_w with them, so this issue remains even if ABE is used.

To deal with this issue, we use a temporary work key k_{w_t} that has a valid period and is updated frequently. k_w is used to encrypt k_s, and k_{w_t} is used for the same purpose. However, the update period of k_{w_t} is shorter than that of k_w. The shorter update period makes finer control of the key possible. In this paper, we set the update period to one day. k_{w_t} is changed every day, so the damage caused by a leak of k_{w_t} is limited to one day.

If k_{w_t} cannot be used except for the assigned time period, security level of the system holds high. We thus need a way how for the subscriber to carry k_{w_t} securely and efficiently outside the home.

If the plaintext of k_{w_t} is stored in the mobile terminal, it is vulnerable, and thus, copyright of the content may be violated. While it is possible to encrypt k_{w_t} by using k_m, it is impossible to control the location at which k_{w_t} is used. ABE can be used to control the time and location, but as mentioned in Sect. 3.2, it takes time until k_{w_t} is obtained, and this threatens the real-time property. To deal with this problem, we modify the system that has real-time property. The modified system uses both communication networks and broadcasting channels, so that broadcasters can respond to each subscriber's request almost in real-time. Such real-time service cannot be realized without communication networks.

In addition, mobile terminals work effectively to respond each subscriber's request. People merely lend their mobile terminal and the terminal can be used for the owner's authentication.

There are three key management methods for ABE schemes. The first is that the subscriber carries both an ABE-encrypted temporary work key $C_{k_{w_t}} = \mathsf{ABE\_Enc}(pk, \beta, k_{w_t})$ and sk_t stored in the mobile terminal. The second is that the subscriber carries only $C_{k_{w_t}}$ in the mobile terminal. The third is that the subscriber carries only sk_t in the mobile terminal.

In the first method, the subscriber has both a ciphertext and its corresponding decryption key, and he/she can decrypt the ciphertext and obtain k_{w_t} when desired. Hence, the method is as same as one in which the subscriber carries a plaintext k_{w_t}; that means it is vulnerable to key leakage. In the second method, the data the subscriber gets before its travel is deeply related to k_{w_t}. Compared with the third method, it has more chance of k_{w_t} being extracted from the data of the subscriber. That is, broadcasters would find the third method preferable to the second.

In addition, the operation related to k_{w_t} should be the same as that of k_w, since the broadcaster does not want any special operation. Hence, the broadcaster can generate k_{w_t} whenever it wants. If the broadcaster generates k_{w_t} just before k_{w_t} becomes valid, the subscriber may not obtain k_{w_t} before beginning the journey. That is, considering the timing at which the broadcaster generates k_{w_t}, the third method is preferable, because the subscriber carries only sk_t in the mobile terminal. In the following, we will assume that only sk_t is stored in the mobile terminal.

We show more details. The subscriber needs to obtain a decryption key $sk_t = \mathsf{ABE\_Gen}(msk, S)$ before beginning to travel, where S is the set of attributes and it includes the location data of the hotel (latitude, longitude) $= (p_{px}, p_{py})$ and travel period t_p. To obtain sk_t, the subscriber sends (p_{px}, p_{py}) and t_p to the key issuance center through communication networks. The key issuance center generates sk_t and returns it to the subscriber. The subscriber gets sk_t, stores it in the mobile terminal, and takes it with him/her.

For the subscriber to obtain services at the hotel, the key issuance center has to generate an ABE-encrypted k_{w_t} by using the subscriber's current location and current time. That is, when the mobile terminal requests k_{w_t} to the key issuance center, it sends its GPS data. This GPS data contains the current location data (p_{cx}, p_{cy}) and the current time t_c. The key issuance center generates an ABE-encrypted temporary work key $C_{k_{w_t}} = \mathsf{ABE\_Enc}(pk, \beta, k_{w_t})$ by using the data as attributes and the policy β. Errors are naturally contained in the GPS data. In addition, there would be differences between (p_{px}, p_{py}) and (p_{cx}, p_{cy}) and between t_p and t_c in principle. For this reason, we chose the ABE scheme, which can specify a range of attributes [4]. Concretely, the policy of ABE is as follows: $\beta = (p_{px} \in \{p_{cxl}, p_{cxu}\}) \wedge (p_{py} \in \{p_{cyl}, p_{cyu}\}) \wedge (t_p = t_c)$, where $p_{cxl} = p_{cx} - \epsilon_x$, $p_{cxu} = p_{cx} + \epsilon_x$, $p_{cyl} = p_{cy} - \epsilon_y$, $p_{cyu} = p_{cy} + \epsilon_y$, where ϵ_x, ϵ_y are acceptable error values with regard to latitude and longitude, and where $\wedge$ denotes an AND gate.

At the hotel, the subscriber obtains an ABE-encrypted temporary work key $C_{k_{w_t}}$ from Key issuance center through communication networks, decrypts a temporary work key $k_{w_t} = \mathsf{ABE\_Dec}(sk_t, C_{k_{w_t}})$ by using sk_t brought from the home, and obtains services at the hotel.

There is a limit to the transmission capacity if $C_{k_{w_t}}$ and sk_t are sent through the air, and the subscribers may have to wait a half an hour or more. However, in the above method, the subscriber can get services without having to wait a long time. That is, he or she can get k_{w_t} at the desired time, and the quality of services improves.

The key point of this key management system is the use of a temporary work key k_{w_t}. k_{w_t}'s role is different from that of k_w, so the new functions associated with k_{w_t} should be added to the conventional system. New data signal(s) must be transmitted from the broadcasting station. In particular, the operation of k_{w_t} should be the same as that of k_w; hence, the broadcaster encrypts k_s by using k_w and k_{w_t} simultaneously, generates $C_{ks} = Enc(k_w, k_s)$ and $C_{ks_t} = Enc(k_{w_t}, k_s)$, and transmits C_{ks} and C_{ks_t} simultaneously to all subscribers through the air. After receiving the signal, receivers at home decrypt C_{ks} by using k_w and generate $k_s = Dec(k_w, C_{ks})$. On the other hand, the receivers at the hotels decrypt C_{ks_t} by using k_{w_t} and generate $k_s = Dec(k_{w_t}, C_{ks_t})$. Subsequently, receivers at both locations obtain the same services.

The roles of valid time of k_{w_t} and the time attribute of ABE are slightly different. The valid time of k_{w_t} is a countermeasure against work key leakage and meets the requirements of broadcasters. On the other hand, the time attribute of ABE is a restriction on the decryption time.

3.4 Proposed System

Figure 2 illustrates the system on which the above service is offered. The entities in the system are as follows:

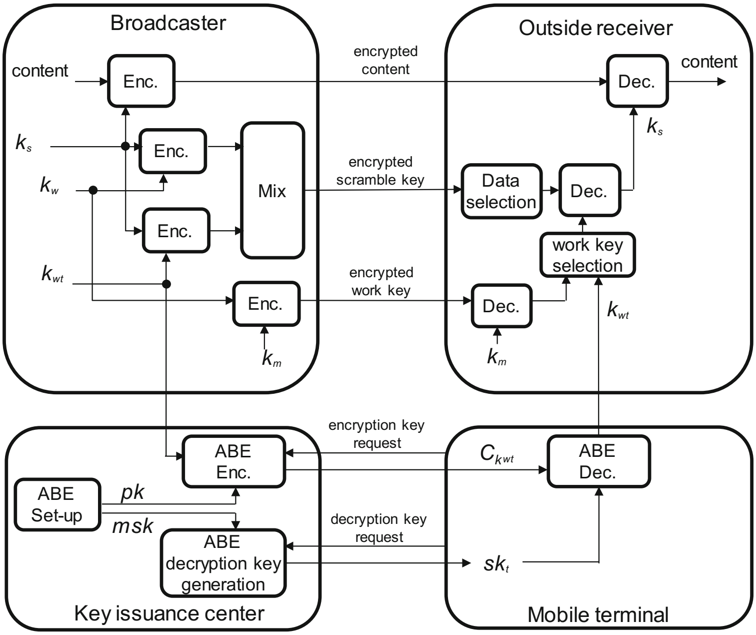

Fig. 2. Proposed system: Enc. and Dec. denote encryption and decryption blocks, respectively.

- Mobile terminal: A subscriber that has a contract with a broadcaster.
- Broadcaster: It encrypts content and transmits it to all subscribers.
- Key issuance center: It generates the keys regarding to ABE.
- Outside receiver: Receiver at a hotel.

New functions associated with k_{w_t} have to be added to each entity. In particular, the broadcaster has to have a new function to generate k_{w_t} and a function to encrypt k_s by using k_{w_t}. The similar function is standardized as an extension of the system (Part 3, Chap. 3 in [27]) and the impact on the broadcaster is light. The mobile terminal is a new entity, which is not used in conventional broadcasting services. It collaborates with receivers, which receive k_{w_t} from it, and decrypts k_s by using k_{w_t}. Here, we assume that the outside receivers do not have any contract with broadcasters, and hence, that the outside receivers cannot get any k_w. However, in reality, some outside receivers may actually have contracts, so a function to select one among k_w and k_{w_t} and a function to select one among C_{ks} and C_{ks_t} are necessary. The functions required by each entity are as follows.

The key issuance center is a new entity. It has, at least, the following four functions: (1) a function to obtain k_{w_t} from the broadcaster, (2) a function to set up an ABE scheme, (3) a function to generate a decryption key sk_t, and (4) a function to encrypt k_{w_t} and generate $C_{k_{w_t}} = \mathsf{ABE\_Enc}(pk, \beta, k_{w_t})$.

The mobile terminals need at least three functions: (1) a function to store sk_t securely, (2) a function to obtain $C_{k_{w_t}}$ from the key issuance center, and (3) a function to decrypt $k_{w_t} = \mathsf{ABE\_Dec}(sk_t, C_{k_{w_t}})$.

Two new functions are added to the receivers: (1) a function to select k_{w_t} not k_w and (2) a function to select C_{kst} not C_{ks}.

The broadcasters have a new function: (1) a function that encrypts k_s by using k_{w_t}.

These additional functions make it possible for subscribers to obtain the same services that they receive at home outside their homes.

3.5 Key Management Procedure

Figure 3 shows the key management procedure in the system.

To prepare the services, the key issuance center performs $\mathsf{ABE\_Setup}(1^\lambda)$ and generates master and public keys of ABE (msk, pk).

As Fig. 2 shows, two versions of an encrypted scramble key $C_{ks} = Enc(k_w, k_s)$ and $C_{ks_t} = Enc(k_{w_t}, k_s)$ are transmitted by the broadcaster, and the outside receiver selects one version. Precisely, the security module in the receiver selects one version. Generally, the hotel does not have a contract for pay-TV services, and it does not have any k_w of the pay-TV services. When the subscriber brings

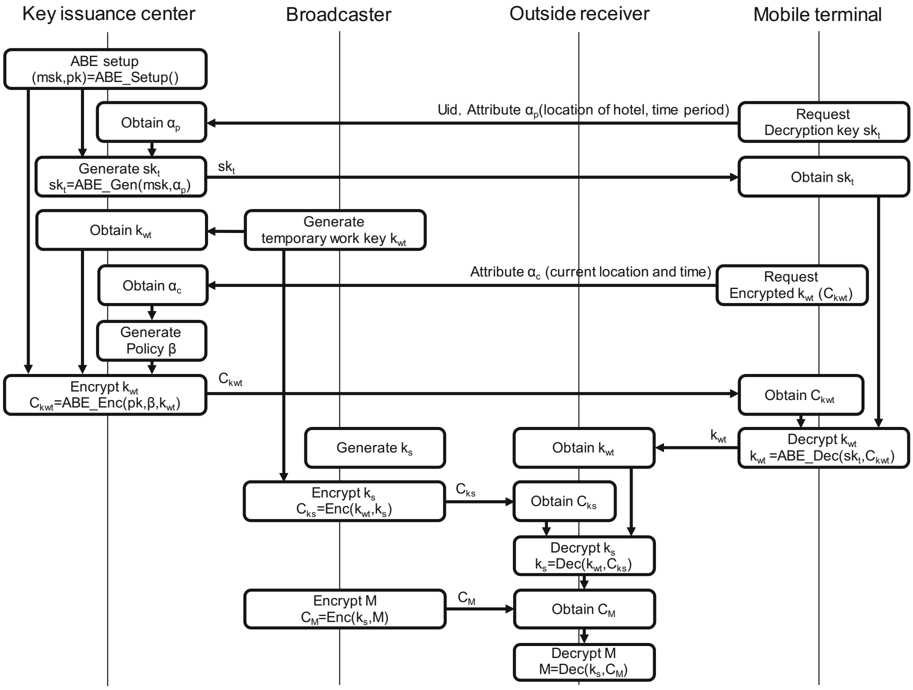
Key issuance center
Broadcaster
Outside receiver
Mobile terminal
ABE setup (msk,pk)=ABE_Setup()
Obtain α_p
Uid, Attribute α_p(location of hotel, time period)
Request Decryption key sk_t
Generate sk_t sk_t=ABE_Gen(msk,α_p)
sk_t
Obtain sk_t
Obtain k_{wt}
Generate temporary work key k_{wt}
Obtain α_c
Attribute α_c (current location and time)
Request Encrypted k_{wt} (C_{kwt})
Generate Policy β
Encrypt k_{wt} C_{kwt}=ABE_Enc(pk,β,k_{wt})
C_{kwt}
Obtain C_{kwt}
Generate k_s
Obtain k_{wt}
k_{wt}
Decrypt k_{wt} k_{wt} =ABE_Dec(sk_t,C_{kwt})
Encrypt k_s C_{ks}=Enc(k_{wt},k_s)
C_{ks}
Obtain C_{ks}
Decrypt k_s k_s=Dec(k_{wt},C_{ks})
Encrypt M C_M=Enc(k_s,M)
C_M
Obtain C_M
Decrypt M M=Dec(k_s,C_M)

Fig. 3. Key management procedure of the system

the key k_{w_t} in its mobile terminal, k_{w_t} is transmitted to the outside receiver. The receiver selects C_{ks_t} and decrypts it by using k_{w_t}. If the subscriber does not bring the key k_{w_t}, he or she cannot obtain the services.

In addition, when and where the subscriber uses the services must be specified before travel. If the actual time or location is different from the specified time or location, he or she cannot obtain the service. These two controls are enabled by the following procedure.

When the key issuance center generates a decryption key sk_t, the attributes of the subscriber are sent to the key issuance center and the sk_t associated with the attributes is generated. When the key issuance center generates an encrypted k_{w_t}, a ciphertext $C_{k_{w_t}}$ associated with the policy regarding the attributes and their error range is generated. When the mobile terminal decrypts k_{w_t}, k_{w_t} can be decrypted if the set of attributes of sk_t matches the policy of $C_{k_{w_t}}$.

k_{w_t} is decrypted in the mobile terminal and is transmitted to the security module in the outside receiver after communication between the mobile terminal and the outside receiver is established. k_{w_t} is then used to decrypt $k_s = Dec(k_{w_t}, C_{ks})$ by using $C_{ks} = Enc(k_{w_t}, k_s)$, and finally, content M is decrypted $M = Dec(k_s, C_M)$ by using k_s and $C_M = Enc(k_s, M)$. The details of the procedure are as follows:

(1) The key issuance center performs $\mathsf{ABE\_Setup}(\mathsf{a}^{\lambda})$ to prepare the services and generates (msk, pk).
(2) A subscriber sends its identifier (Uid) and its attributes (time when staying at the hotel and location of the hotel $\alpha_p := ((p_{px}, p_{py}), t_p))$ to the key issuance center by using his/her mobile terminal.
(3) The key issuance center checks the Uid and the subscriber's contract, generates a decryption key $sk_t = \mathsf{ABE\_Gen}(msk, \alpha_p)$ and returns sk_t to the subscriber.
(4) The subscriber stores sk_t in the mobile terminal.
(5) A broadcaster generates a temporary work key k_{w_t} and sends it to the key issuance center.
(6) The subscriber obtains his/her current location (p_{cx}, p_{cy}) by using the GPS function of the mobile terminal.
(7) The subscriber sends a decryption key request including the subscriber's attributes $\alpha_c := ((p_{cx}, p_{cy}), t_c)$ to the key issuance center.
(8) The key issuance center extracts $p_c = (p_{cx}, p_{cy})$ from α_c, and calculates the range of attributes $p_{cxl} \sim p_{cxu}$ $p_{cyl} \sim p_{cyu}$, where (ϵ_x, ϵ_y) are errors of latitude and longitude and they are decided previously, and where $p_{cxl} = p_{cx} - \epsilon_x$, $p_{cxu} = p_{cx} + \epsilon_x$, $p_{cyl} = p_{cy} - \epsilon_y$, $p_{cyu} = p_{cy} + \epsilon_y$ are upper and lower bounds of latitude and longitude.
(9) The key issuance center generates an encrypted temporary work key $C_{kwt} = \mathsf{ABE\_Enc}(pk, \beta, k_{w_t})$ by using a public key pk and a policy $\beta = (p_{px} \in \{p_{cxl}, p_{cxu}\}) \wedge (p_{py} \in \{p_{cyl}, p_{cyu}\}) \wedge (t_p = t_c)$ and transmits C_{kwt} to the mobile terminal through communication networks.
(10) The mobile terminal decrypts the temporary work key $k_{w_t} = \mathsf{ABE\_Dec}(sk_t, C_{kwt})$ from an encrypted temporary work key C_{kwt} transmitted through communication networks.

(11) The subscriber establishes a link between his/her mobile terminal and the receiver at the outside receiver (at the hotel) and sends k_{w_t} from the mobile terminal to the outside receiver.

(12) The outside receiver decrypts the scramble key $k_s = Dec(k_{w_t}, C_{k_s})$ by using k_{w_t}.

(13) Finally, the outside receiver decrypts content $M = Dec(k_s, C_M)$ by using k_s.

The acceptable error range (ϵ_x, ϵ_y) between location data $p_p = (p_{px}, p_{py})$ obtained from the hotel's address and the location data $p_c = (p_{cx}, p_{cy})$ obtained by using the GPS function of mobile terminal should be adequately determined according to the services to be provided.

4 Conclusion

We proposed a key management system that allows subscribers enjoy versatile broadcasting services. The subscribers can obtain services identical to those they normally receive at home outside their homes. The system uses a temporary key that has compatibility with the conventional key, an ABE scheme that can assign a range of attributes [4], and a mobile terminal. Although the system needs a key issuance center, it does not impact the conventional broadcasting system in a big way and has backward compatibility.

The current location data comes from the GPS function of a mobile terminal. The terminal is the subscriber's and there are a lot of reports on modifying GPS data. If the mobile terminal has a secure memory and can store a signing key in the memory, and if the mobile terminal has a high-performance CPU, the terminal can sign its GPS data electronically and the signature would be an effective countermeasure against modification attacks on GPS data. If the terminal does not have a high-performance CPU, the nearest mobile station or edge router should be used as a TTP, and the TTP should issue the current location and time instead of the mobile terminal. However, mobile stations and edge routers are not densely allocated, and in many cases, the nearest station or router would be far away from, say, the hotel where the subscriber is staying, and the distance between the mobile terminal and the nearest station or router depends on the station or router allocation plan of the communications provider. Subsequently, such stations and routers are impractical. Recently, a lot of researches has gone into mobile edge computing (MEC) [2,24,25,33] and edge computers on the mobile networks handling loads instead of mobile terminals. An edge computer could be used as a TTP, but it has yet to be decided where and how many computers are to be assigned.

An actual system must be trustworthy. A digital signature scheme or TTP should be considered for this purpose. Efficiency is also important in practice. The ABE schemes used in our system have a heavier load than that of conventional encryption schemes, such as RSA, but the number of processes involving them in the mobile terminal during travel is only one and the load only lasts a number of seconds. Therefore, a subscriber would not likely find the load of the ABE process to be unacceptable. On the other hand, the load of the key issuance center would be much heavier, especially if the number of subscribers is large. That means we have to construct a system with a lighter load.

Acknowledgment. A part of this work is supported by JST CREST grant number JPMJCR1688.

References

1. Agrawal, S., Freeman, D.M., Vaikuntanathan, V.: Functional encryption for inner product predicates from learning with errors. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 21–40. Springer, Heidelberg (2011). doi:10.1007/978-3-642-25385-0_2
2. Ahmed, A., Ahmed, E.: A survey on mobile edge computing. In: Proceedings of IEEE ISCO 2016. IEEE (2016)
3. Attrapadung, N., Libert, B.: Functional encryption for public-attribute inner products: achieving constant-size ciphertexts with adaptive security or support for negation. J. Math. Cryptol. **5**(2), 115–158 (2012)
4. Attrapadung, N., Hanaoka, G., Ogawa, K., Ohtake, G., Watanabe, H., Yamada, S.: Attribute-based encryption for range attributes. In: Zikas, V., De Prisco, R. (eds.) SCN 2016. LNCS, vol. 9841, pp. 42–61. Springer, Cham (2016). doi:10.1007/978-3-319-44618-9_3
5. Baek, J., Safavi-Naini, R., Susilo, W.: Token-controlled public key encryption. In: Deng, R.H., Bao, F., Pang, H.H., Zhou, J. (eds.) ISPEC 2005. LNCS, vol. 3439, pp. 386–397. Springer, Heidelberg (2005). doi:10.1007/978-3-540-31979-5_33
6. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: Proceedings of IEEE S&P 2007, pp. 321–334. IEEE (2007)
7. Boneh, D., Sahai, A., Waters, B.: Functional encryption: definitions and challenges. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 253–273. Springer, Heidelberg (2011). doi:10.1007/978-3-642-19571-6_16
8. Brands, S., Chaum, D.: Distance-bounding protocols. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 344–359. Springer, Heidelberg (1994). doi:10.1007/3-540-48285-7_30
9. Capkun, S., Hubaux, J.: Secure positioning of wireless devices with application to sensor networks. In: Proceedings of IEEE Infocom 2005, pp. 1917–1928. IEEE (2005)
10. Chandran, N., Goyal, V., Moriarty, R., Ostrovsky, R.: Position based cryptography. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 391–407. Springer, Heidelberg (2009). doi:10.1007/978-3-642-03356-8_23
11. Chandran, N., Goyal, V., Moriarty, R., Ostrovsky, R.: Position-based cryptography. SIAM J. Comput. **43**(4), 1291–1341 (2014). SIAM
12. Chen, J., Wee, H.: Semi-adaptive attribute-based encryption and improved delegation for Boolean formula. In: Abdalla, M., De Prisco, R. (eds.) SCN 2014. LNCS, vol. 8642, pp. 277–297. Springer, Cham (2014). doi:10.1007/978-3-319-10879-7_16
13. Dent, A.W., Tang, Q.: Revisiting the security model for timed-release encryption with pre-open capability. In: Garay, J.A., Lenstra, A.K., Mambo, M., Peralta, R. (eds.) ISC 2007. LNCS, vol. 4779, pp. 158–174. Springer, Heidelberg (2007). doi:10.1007/978-3-540-75496-1_11

14. Dziembowski, S., Zdanowicz, M.: Position-based cryptography from noisy channels. In: Pointcheval, D., Vergnaud, D. (eds.) AFRICACRYPT 2014. LNCS, vol. 8469, pp. 300–317. Springer, Cham (2014). doi:10.1007/978-3-319-06734-6_19
15. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of ACM CCS 2006, pp. 89–98. ACM (2006)
16. Hwang, Y.H., Yum, D.H., Lee, P.J.: Timed-release encryption with pre-open capability and its application to certified e-mail system. In: Zhou, J., Lopez, J., Deng, R.H., Bao, F. (eds.) ISC 2005. LNCS, vol. 3650, pp. 344–358. Springer, Heidelberg (2005). doi:10.1007/11556992_25
17. Kasamatsu, K., Matsuda, T., Emura, K., Attrapadung, N., Hanaoka, G., Imai, H.: Time-specific encryption from forward-secure encryption: generic and direct constructions. Int. J. Inf. Secur. **15**(5), 549–57 (2016)
18. Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 62–91. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13190-5_4
19. May, T.: Time-release crypto (1993). http://www.cyphernet.org/cyphernomicon/chapter14/14.5.html
20. Ogawa, K., Hanaoka, G., Imai, H.: Traitor tracing scheme secure against key exposure and its application to anywhere TV service. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **E90–A**(5), 1000–1011 (2007). IEICE
21. Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 191–208. Springer, Heidelberg (2010). doi:10.1007/978-3-642-14623-7_11
22. Paterson, K.G., Quaglia, E.A.: Time-specific encryption. In: Garay, J.A., De Prisco, R. (eds.) SCN 2010. LNCS, vol. 6280, pp. 1–16. Springer, Heidelberg (2010). doi:10.1007/978-3-642-15317-4_1
23. Sastry, N., Shankar, U., Wagner, D.: Secure vefirication of location claims. In: Proceedings of ACM Wireless Security 2003, pp. 1–10. ACM (2003)
24. Takahashi, N., Tanaka, H., Kawamura, R.: Analysis of process assignment in multi-tier mobile cloud computing and application to edge accelerated web browsing. In: Proceedings of IEEE Mobile Cloud 2015, pp. 233–234. IEEE (2015)
25. Tran, T.X., Pnadey, P., Hajisami, A., Pompili, D.: Collaborative multi-bitrate video caching and processing in mobile-edge computing networks. In: Proceedings of IEEE WONS 2017, pp. 165–172. IEEE (2017)
26. Yoshida, M., Mitsunari, S., Fujiwara, T.: A timed-release key management scheme for backward recovery. In: Won, D.H., Kim, S. (eds.) ICISC 2005. LNCS, vol. 3935, pp. 3–14. Springer, Heidelberg (2006). doi:10.1007/11734727_3
27. ARIB: Conditional Access System Specifications for Digital Broadcasting. ARIB STD-B25 (2007)
28. ETSI: DVB Common Scrambling Algorithm-Distribution Agreements. Technical report (2013)
29. http://www.nhk.or.jp/hybridcast/online/
30. http://www.hbbtv.org/
31. http://www.hulu.com/
32. http://www.youview.com/
33. ETSI: Mobile Edge Computing (MEC); Framework and Reference Architecture. http://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/01.01.01_60/gs_MEC003v010101p.pdf