Privacy Preservation for Versatile Pay-TV Services

Kazuto Ogawa[1](✉) and Koji Nuida[2]

[1] Japan Broadcasting Corporation, Tokyo, Japan
ogawa.k-cm@nhk.or.jp
[2] The University of Tokyo, Tokyo, Japan
nuida@mist.i.u-tokyo.ac.jp

Abstract. In pay-TV services, content is encrypted and transmitted to subscribers. Each subscriber has a security module that holds a decryption key(s) for the encrypted content. A set-top box or a smart card is often used as the security module. When a subscriber wants to obtain the same services outside the home, the subscriber has to bring the security module. However, even if the security module is a card, it is not easy to take it out because of the structure of TV sets and set-top boxes.

As a way of improving current pay-TV services, Ogawa, Tamura, and Hanaoka (OTH17) proposed a system using an attribute-based encryption scheme (ABE). ABE is used to restrict the time and location at which a subscriber can obtain the service.

However, OTH17 requires a third trusted party (TTP) for key and ciphertext generation; thus, the TTP knows the time and location of the subscriber. This means that the subscriber's private information is disclosed to the party.

Here, we propose a system that avoids disclosure of private data by adding a multi-party computation (MPC). In addition, MPC makes the TTP unnecessary.

Keywords: Pay-TV services · Attribute-based encryption · Multi-party computation · Privacy preserving · Non-trusted party

1 Introduction

1.1 Background

Broadcasting and cable TV services encrypt content for the purpose of copyright protection before distributing it to subscribers. Each subscriber needs a decoder with a decryption module for decrypting the content. In Japan, a smart card or a LSI (card what it follows) is used as a security module, and a decryption key is generated in the card [32,33]. Moreover, pay-TV services use the same card to control subscribers' access to their content. The card holds a subscriber's contract information, and the decryption keys are generated on the basis of the information in the card.

A. Moallem (Ed.): HCII 2019, LNCS 11594, pp. 417–428, 2019.
https://doi.org/10.1007/978-3-030-22351-9_28

If the card were be able to be taken out of the TV set or set-top box, subscribers would be able to get identical services outside the home, but it is not easy to take the card out of the receivers, because manufacturers produce receivers, considering breakage of cards.

If the decryption key(s) could be removed electronically and stored in such devices as a mobile phone or tablet PC, the subscriber would not need to take the card out; this would improve quality of service.

Nowadays, there are hybrid systems, such as youview [38], HbbTV [36], Hulu [37], and Hybridcast [35], that offer broadcasting services through the air and network services through the Internet. These systems consider cooperation of receivers and mobile terminals, meaning that it is easy to transmit data from the receiver to the mobile terminal. However, when a third party who can access and use the data transmitted to the mobile terminal illegally use the system in a way that the copyright would be infringed, for example. Hence, in cases in which data can be transmitted to the mobile terminal, countermeasures against possible illegal use of that data should be taken.

Ogawa, Hanaoka, and Imai (OHI07) [26] proposed a method in which a decryption key is updated periodically and a temporal decryption key can be taken out, as a way of improving the currently offered services. That is, the subscriber can obtain identical services outside the home only during a limited period. In this case, even if the decryption key is leaked, the damage caused by the leakage will not extend beyond the valid period of the key. Ogawa, Tamura, and Hanaoka (OTH17) proposed another countermeasure in which an attribute-based encryption scheme (ABE) is used and the location and time are used as attributes. That is, the subscriber can obtain services outside only during a limited period and in restricted area. Even if the decryption key is leaked, the damage would not extend beyond the valid period and the restricted area.

1.2 Contributions

The services considered in this paper are the same as those in OTH17. First, we consider a situation in which subscribers bring the decryption keys with them and obtain identical services outside their homes. The situation corresponds to one of traveling on business or sightseeing. In such a situation, the location where the subscriber stays during the period is usually decided before leaving the home. Moreover, it would likely be a hotel or similar establishment where the subscriber would most want to obtain the services. Furthermore, the time during which the subscriber would obtain the services at the hotel would be limited. Then, by generating a decryption key that can be used at the hotel during the time of stay and storing the key in the mobile terminal electronically would make it possible for a subscriber outside the home to obtain identical services to those received at home when he or she wants them.

OTH17 uses ABE to control accesses to content, and the location and time are used as its attributes. In addition, a trusted third party (TTP) is needed to issue certain decryption keys, and private information, such as the place where the subscriber is and the period of the stay, is sent to the party in plaintext.

That the TTP gets such information is not preferable from the viewpoint of privacy preserving. Moreover, if the party is untrusted, there is a risk that the subscriber's private information will be disclosed. Such a system lacks versatility.

We propose a system that overcomes the above drawback. In order to reduce the risk, we add the multi-party computation protocol (MPC) [1,7,14,24,25,29,30] to OTH17. In MPC, it is impossible to recover original private data from the share provided to each party. Thus, MPC improves the OTH17 system into one that does not disclose any private information.

1.3 Related Works

The system we propose uses time and location data to control access to the content. As far as we know, there has not been any related proposal except for OHI07 and OTH17 regarding access control to pay-TV services. However, these systems do not consider privacy preservation. Although OHI07 cannot control the location at which the decryption key is used, OTH17 can do so, making it superior to OHI07 with regard to content copyright protection. However, OTH17 is still poor from the viewpoint of privacy preservation, because the user has to tell the place where he or she will use the decryption key.

A position based cryptography scheme (PBC) [6,8–10,16,20,28], which controls the decryption of a ciphertext according to the location the message sender specifies, and a time released encryption scheme (TRE) [3,13,15,18,19,21,22,27,31], which controls the decryption of a ciphertext according to the time the message sender specifies, can be used for the same purpose. However, the use of such schemes entails sending private data, such as the place and time of stay, in plaintext to certain parties; they too are not preferable from the viewpoint of privacy preservation. The use of PBC and TRE with homomorphic properties may make it possible to eliminate the above risk, but their use requires two encryptions or decryptions; moreover, homomorphic properties seem to raise computational costs.

2 Preliminary

2.1 Current Broadcasting System and OTH17

There are a lot of pay-TV services in North America, Europe, and Asia. The systems in North America and Europe vary from broadcaster to broadcaster, and their details are not disclosed. Although the Common Descrambling System of Digital Video Broadcasting (DVB-CSA) [34] is standardized in Europe, a non-disclosure agreement must be signed in order to see its details, and naturally, the details cannot be disclosed. On the other hand, the Japanese broadcasting system has been disclosed. Figure 1 shows the current broadcasting system used in Japan [32,33].

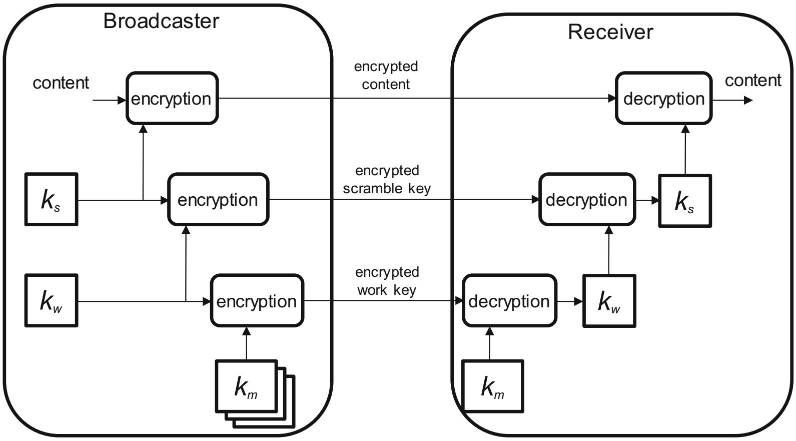

Fig. 1. Japanese Broadcasting System: k_s is the content (scramble) key, k_w is the work key, and k_m is the master key.

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.

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

Each receiver needs a smart card or LSI as a security module to hold a k_m. Each security module has a distinct k_m, and broadcasters can transmit private contract information to each subscriber (receiver) by using 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 security module 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. In the Japanese broadcasting system, the descrambling scheme used for content decryption is different from the scheme of decrypting k_w and k_s, but this difference does not affect the proposed system. Hence, we will use the same notation $Dec(\cdot, \cdot)$.

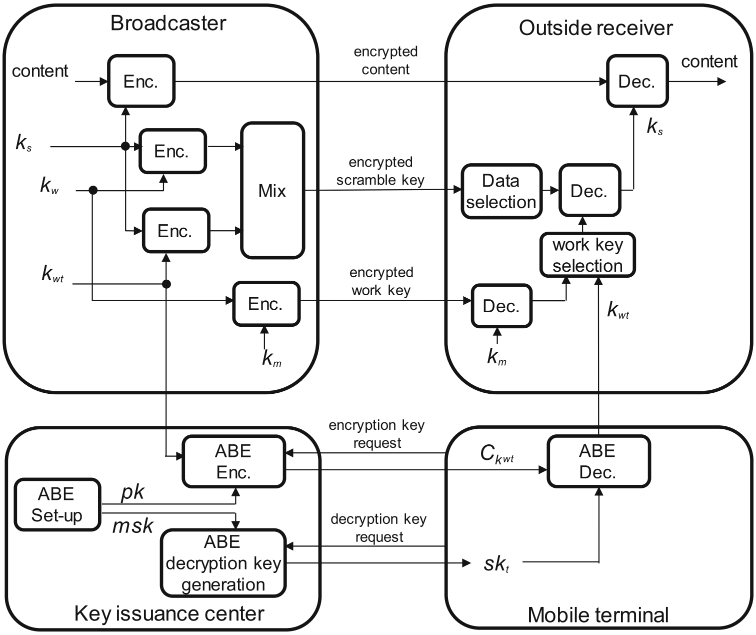

Fig. 2. OTH17 system

OTH17 is constructed on the basis of the above Japanese system. Figure 2 shows this system. It introduces a new work key k_{w_t}, and ABE is used to control accesses to broadcast content.

The broadcaster generates k_{w_t} and encrypts k_s by using k_{w_t}. Receivers receive k_{w_t} from the mobile terminals and decrypt k_s by using k_{w_t}. The key issuance center gets k_{w_t} from the broadcaster, sets up the ABE scheme, generates a decryption key sk_t, encrypts k_{w_t}, and generates $C_{k_{w_t}} = \mathsf{ABE\_Enc}(pk, \beta, k_{w_t})$. The mobile terminals need to store sk_t securely, obtain $C_{k_{w_t}}$ from the key issuance center, and decrypt $k_{w_t} = \mathsf{ABE\_Dec}(sk_t, C_{k_{w_t}})$.

2.2 Attribute-Based Encryption

ABE [2,5,12,17] 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 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 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, it employs the attribute-based encryption scheme proposed by Attrapadung et al. [2] that can assign an attribute with a range. Attrapadung et al.'s scheme can specify the range of an attribute by a direct expression $\{a, b\}$ and can calculate condition equations by using a tree-based attribute label. The range is included in β.

2.3 Multi-Party Computation

Multi-party computation (MPC) is a method in which multiple parties collaborate to calculate a function $f()$ without disclosure of the secret shares (information) that each party holds. By using MPC, it is possible to modify an arbitrary algorithm (function) into an information-theoretically secure one under certain conditions [4,11]. In MPC, a secret sharing algorithm makes secret shares from an input x to f, and multiple servers obtain distinct shares and execute some calculations. The user gets output shares from the servers and calculates the output $y = f(x)$. The original input x cannot be revealed from any of the secret shares or from any of the information communicated between the servers.

Here, we will assume a semi-honest model. That is, all entities execute their roles without any error. The secret sharing scheme and client-aided client-server model [23,24] used in this paper are described below.

Secret Sharing. A secret sharing scheme consists of two algorithms: Share and Reveal. Share takes as input x and outputs shares $([\![x]\!]_1, \cdots, [\![x]\!]_N)$, $([\![x]\!]_1, \cdots, [\![x]\!]_N) \leftarrow \mathsf{Share}(x)$, where N is the number of parties and $[\![x]\!]_i$ denotes a share for the i-th ($i \in [1, N]$) party. Reveal takes as input $([\![x]\!]_1, \cdots, [\![x]\!]_N)$ and outputs $[\![x]\!]$, $[\![x]\!] \leftarrow \mathsf{Reveal}([\![x]\!]_1, \cdots, [\![x]\!]_N)$. In this paper, we set $N = 2$. That is, we will use the $\binom{2}{2}$-secret sharing scheme, where Share generates two shares and REVEAL takes input two shares.

Client-Aided Client-Server Model. We employ Morita and et al.'s secret-sharing based MPC in the client-aided client-server model [24]. Its procedure is as follows:

Suppose there are N servers and t clients.

1. Client-j($j \in [1, t]$) takes input $a_j \in \mathbb{A}$ and generates shares $[\![a_j]\!] = ([\![a_j]\!]_1, \cdots, [\![a_j]\!]_N) \leftarrow \mathsf{Share}(a_j)$ for N servers. Client-1 generates a set of aiding information (Beaver triple) $BT_1, \cdots, BT_N$ that helps each server's calculation.

2. Client-j sends $[\![a_j]\!]_i$ to Server-i and Client-1 sends BT_i to Server-i.
3. Server-i calculates its output $[\![b_i]\!]$ from t inputs $([\![a_1]\!]_i, \cdots, [\![a_t]\!]_i)$, communicating with the other servers.
4. Server-i sends $[\![b_i]\!]$ to all clients.
5. Each client takes n inputs $([\![b_1]\!], \cdots, [\![b_N]\!])$ and obtains $b = f(a_1, \cdots, a_t)$ by performing $b \leftarrow \mathsf{Reveal}([\![b_1]\!], \cdots, [\![b_N]\!])$.

3 Proposal

OTH17 employs a trusted third party (TTP) and subscribers' private information; e.g., the subscriber's travel destination is disclosed to the TTP. In contrast, we construct a system that preserves subscribers' private information while maintaining the other properties of OTH17.

Let us suppose that a subscriber carries keys and obtains services outside his or her home (at a hotel). Furthermore, the period of stay at the hotel is limited. Accordingly, a decryption key that can only be used during the stay at the hotel and that can be stored in the subscriber's mobile terminal would make it possible to obtain the expected services.

From the viewpoint of privacy preservation, the data supplied by the subscriber should be kept secret from every other party. To ensure this, we employ the multi-party computation protocol (MPC). In particular, the calculation of TTP in OTH17 is divided up into multiple parts and each part is performed by a separate distinct party. The output of each party is sent to the subscriber. MPC is secure if the original data cannot be recovered from the share of any party. Hence, due to the MPC, no party can obtain original data from its share and the subscriber's privacy is preserved.

3.1 System

Figure 3 shows the proposed system using MPC. There are four entities.

- Mobile terminal: It belongs to a subscriber who has a contract with a broadcaster.
- Broadcaster: It encrypts content and transmits it to all subscribers.
- Server-1, 2: It plays the role of a key issuance center. It generates pk and msk of ABE and issues sk_t and C_{kw_t}.
- Outside receiver: It is a receiver at a hotel, for example.

The broadcaster encrypts k_s by using k_{w_t} and broadcasts the encrypted $C_{k_s} = Enc(k_{w_t}, k_s)$ through the air. k_{w_t} is also encrypted and sent to the outside receiver through communication channels. MPC is used for k_{w_t}'s encryption.

Before the subscriber gets k_{w_t}, the decryption key sk_t of ABE is generated from the location and date attributes of where and when the subscriber plans to obtain the service. This key is generated by using MPC. That is, the subscriber generates multiple shares from his or her attributes (Gen. Shares for MPC-ABE Enc.) and sends each share to a distinct party. Each party generates an output

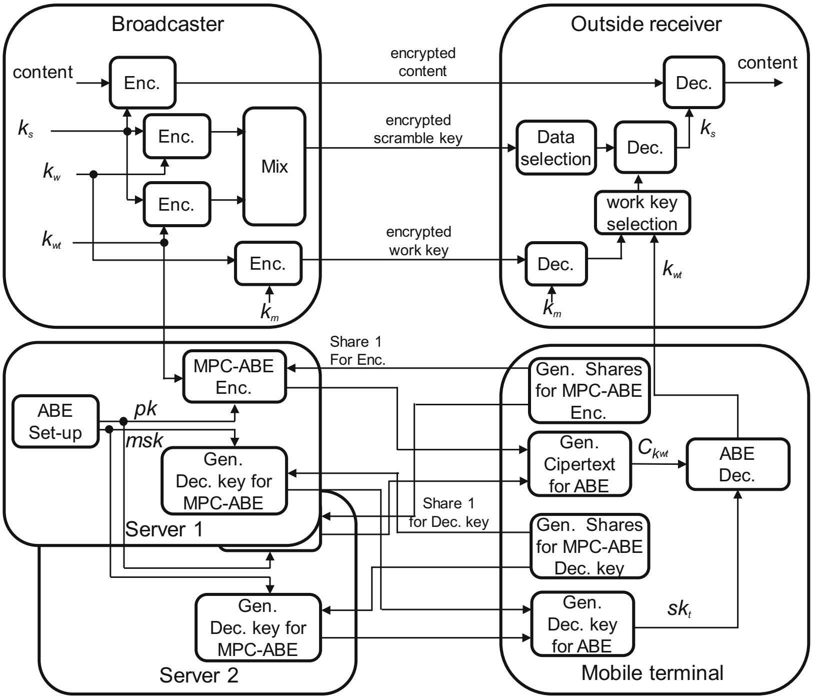

Fig. 3. Proposed System: *pk* and *msk* are public and master keys for ABE. MPC-ABE Enc. and Gen Dec. key for MPC-ABE are encryption and decryption-key generation functions of ABE using a multi-party computation. Gen. Shares for MPC-ABE Enc. is a share-generation function for MPC-ABE Enc. and Gen. Shares for MPC-ABE Dec. key is a share-generation function for Gen. Dec. key for MPC-ABE. Gen. Ciphertext for ABE and Gen. Dec. key for ABE are ciphertext-generation and decryption-key-generation functions for ABE.

share from its input and returns it to the subscriber. This algorithm (Gen. Dec. Key for MPC-ABE) is for generating sk_t. The subscriber generates sk_t from the outputs of all parties. The subscriber stores sk_t in the mobile terminal and brings it to the travel destination.

A ciphertext of k_{w_t} is necessary at the hotel. The subscriber generates multiple shares from his or her attributes (Gen. Shares for MPC-ABE Enc.) and sends each share to a distinct party. Each party generates its output share from its input and transmits it through communication networks to the mobile terminal. The algorithm (MPC-ABE Enc.) is for generating the ciphertext. The terminal generates a ciphertext of k_{w_t} from the outputs of all parties. Finally, the subscriber gets the service at the hotel by using sk_t and the ciphertext of k_{w_t}.

This system enables subscribers to enjoy enriched services without having to disclose any of their private information.

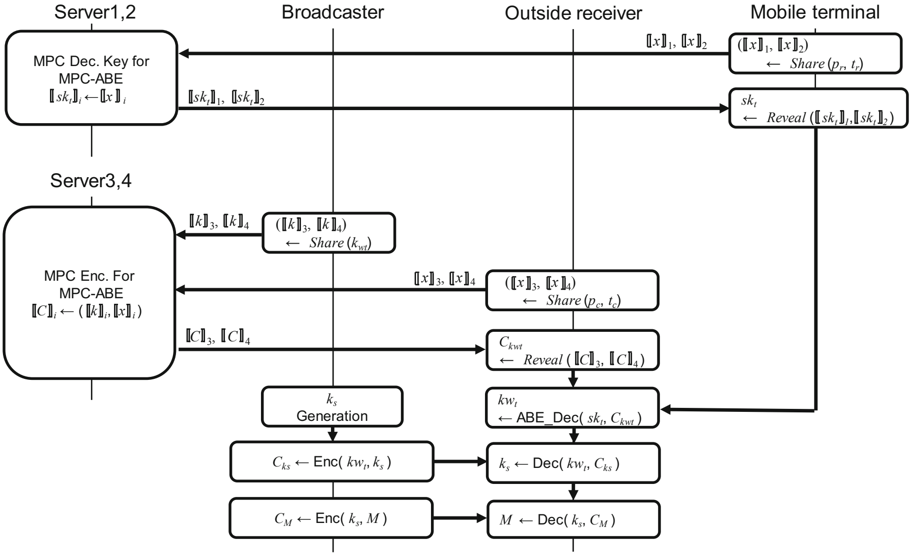
Server1,2
Broadcaster
Outside receiver
Mobile terminal
$[\![x]\!]_1$, $[\![x]\!]_2$
$([\![x]\!]_1, [\![x]\!]_2) \leftarrow Share(p_r, t_r)$
MPC Dec. Key for MPC-ABE
$[\![sk_t]\!]_i \leftarrow [\![x]\!]_i$
$[\![sk_t]\!]_1$, $[\![sk_t]\!]_2$
$sk_t \leftarrow Reveal([\![sk_t]\!]_1, [\![sk_t]\!]_2)$
Server3,4
$[\![k]\!]_3$, $[\![k]\!]_4$
$([\![k]\!]_3, [\![k]\!]_4) \leftarrow Share(k_{wt})$
MPC Enc. For MPC-ABE
$[\![C]\!]_i \leftarrow ([\![k]\!]_i, [\![x]\!]_i)$
$[\![x]\!]_3$, $[\![x]\!]_4$
$([\![x]\!]_3, [\![x]\!]_4) \leftarrow Share(p_c, t_c)$
$[\![C]\!]_3$, $[\![C]\!]_4$
$C_{kwt} \leftarrow Reveal([\![C]\!]_3, [\![C]\!]_4)$
k_s Generation
$kw_t \leftarrow$ ABE_Dec(sk_t, C_{kwt})
$C_{ks} \leftarrow$ Enc(kw_t, k_s)
$k_s \leftarrow$ Dec(kw_t, C_{ks})
$C_M \leftarrow$ Enc(k_s, M)
$M \leftarrow$ Dec(k_s, C_M)

Fig. 4. Service procedure

3.2 Service Procedure

Figure 4 shows the service procedure in the system.

(1) The subscriber obtains a token β from the broadcaster after its authentication and saves it in the mobile terminal.

(2) The subscriber inputs its private information, the place (p_x, p_y) and time t_p at which the subscriber will obtain the service, to its mobile terminal.

(3) The mobile terminal performs $\binom{2}{2}$-secret sharing protocol with (p_x, p_y) and t_p, generates shares $([\![p_1]\!], [\![p_2]\!]) \leftarrow \mathsf{Share}(p_x||p_y||t_p||\beta)$, and sends $[\![p_i]\!]$ to the server-$i (i \in \{1,2\})$. In addition, aiding shares BT_1 and BT_2 are generated and BT_i is sent to server-i.

(4) After receiving $[\![p_i]\!]$ from the mobile terminal, server-i generates a share $[\![sk_{t_i}]\!]$ to calculate a function $f_{kg}(p_x||p_y||t_p||\beta||\alpha)$ and returns it to the mobile terminal, where α is secret data that all servers share.

(5) After receiving $[\![sk_{t_1}]\!]$ and $[\![sk_{t_2}]\!]$ from the servers, the mobile terminal calculates a secret key $sk_t \leftarrow \mathsf{Reveal}([\![sk_{t_1}]\!], [\![sk_{t_2}]\!])$.

(6) The broadcaster generates k_{w_t}, and sends it to server-1 and 2.

(7) At the destination, the mobile terminal generates shares of the current place (p_{cx}, p_{cy}) and time t_{cp} by performing $\binom{2}{2}$-secret sharing protocol ($[\![p_{c1}]\!]$, $[\![p_{c2}]\!]) \leftarrow \mathsf{Share}(p_{cx}||p_{cy}||t_{cp}||\beta)$, and sends $[\![p_{ci}]\!] (i \in \{1,2\})$ to server-i. In addition, the terminal generates shares BT_{c1} and BT_{c2}, and sends $BT_{ci} (i \in \{1,2\})$ to server-i.

(8) After receiving k_{w_t} from the broadcaster, $[\![p_{ci}]\!]$ and $[\![BT_{ci}]\!]$ from the mobile terminal, server-i generates a share $[\![c_i]\!]$ to calculate a function $C_{k_{w_t}} = f_{cg}(p_{cx}||p_{cy}||t_{cp}||\beta||\alpha, k_{w_t})$ and returns it to the mobile terminal.

(9) After receiving $[\![c_1]\!]$ and $[\![c_2]\!]$ from the servers, the mobile terminal reconstructs the encrypted temporal work key $C_{k_{w_t}} \leftarrow \mathsf{Reveal}([\![c_1]\!], [\![c_2]\!])$.

(10) The mobile terminal decrypts the temporal work key $k_{w_t} = Dec(sk_t, C_{k_{w_t}})$ and sends it to the outside receiver.

(11) The outside receiver decrypts the scramble key $k_s = Dec(k_{w_t}, C_{k_s})$ and finally decrypts the content $M = Dec(k_s, C_M)$.

As can be seen, the set (p_{px}, p_{py}) at the subscriber's home should be the same with (p_{cx}, p_{cy}) obtained at the travel destination. If this is not the case, the subscriber cannot get the service.

Steps (8) to (11) of the mobile terminal are performed only once at the start of the service at the travel destination.

4 Conclusion

We proposed a method that enables the subscriber to obtain services at a travel destination. In the system, a secret key is generated on the basis of location and time information. That is, the place and time are used to control the subscriber's access to the content. In addition, this system does not require a TTP and it preserves the subscriber's private information; thus, the system can use an untrusted server. Moreover, there are some information-theoretically secure MPCs, and when the system uses such an information-theoretically secure MPC, it becomes secure against attacks from quantum computers.

References

1. Araki, T., Furukawa, J., Lindell, Y., Nof, A., Ohara, K.: High-throughput semi-honest secure three-party computation with an honest majority. In: Proceedings of ACM SIGSAC CCS 2016, pp. 805–817 (2016)
2. 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). https://doi.org/10.1007/978-3-319-44618-9_3
3. 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). https://doi.org/10.1007/978-3-540-31979-5_33
4. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: Proceedings of STOC 1988, pp. 1–10 (1988)
5. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: Proceedings of IEEE S&P 2007, pp. 321–334 (2007)
6. Brands, S., Chaum, D.: Distance-bounding protocols. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 344–359. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48285-7_30

7. Catrina, O., de Hoogh, S.: Improved primitives for secure multiparty integer computation. In: Garay, J.A., De Prisco, R. (eds.) SCN 2010. LNCS, vol. 6280, pp. 182–199. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-15317-4_13
8. Capkun, S., Hubaux, J.: Secure positioning of wireless devices with application to sensor networks. In: Proceedings of IEEE Infocom 2005, pp. 1917–1928 (2005)
9. 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). https://doi.org/10.1007/978-3-642-03356-8_23
10. Chandran, N., Goyal, V., Moriarty, R., Ostrovsky, R.: Position-based cryptography. SIAM J. Comput. **43**(4), 1291–1341 (2014)
11. Chaum, D., Crépeau, C., Damgård, I.: Multiparty unconditionally secure protocols. In: Proceedings of STOC 1988, pp. 11–19 (1988)
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). https://doi.org/10.1007/978-3-319-10879-7_16
13. Cheon, J.H., Hopper, N., Kim, Y., Osipkov, I.: Provably secure timed-release public key encryption. ACM Trans. Inf. Syst. Secur. **11**, 4:1–4:44 (2008)
14. Damgård, I., Fitzi, M., Kiltz, E., Nielsen, J.B., Toft, T.: Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 285–304. Springer, Heidelberg (2006). https://doi.org/10.1007/11681878_15
15. 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). https://doi.org/10.1007/978-3-540-75496-1_11
16. 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). https://doi.org/10.1007/978-3-319-06734-6_19
17. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceeding of ACM CCS 2006, pp. 89–98 (2006)
18. 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). https://doi.org/10.1007/11556992_25
19. 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), 549–571 (2016)
20. Kuno, S., Attrapadung, N., Kitagawa, T., Imai, H.: Position-based encryption. In: Proceedings of SCIS 2012, 1A1-4 (2012). (in Japanese)
21. Matsuda, T., Nakai, Y., Matsuura, K.: Efficient generic constructions of timed-release encryption with pre-open capability. In: Joye, M., Miyaji, A., Otsuka, A. (eds.) Pairing 2010. LNCS, vol. 6487, pp. 225–245. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-17455-1_15
22. May, T.: Time-release crypto (1993). http://www.cyphernet.org/cyphernomicon/chapter14/14.5.html

23. Mohassel, P., Zhang, Y.: SecureML: a system for scalable privacy-preserving machine learning. In: Proceedings of IEEE Symposium on Security and Privacy 2017, pp. 19–38 (2017)
24. Morita, H., Attrapadung, N., Teruya, T., Ohata, S., Nuida, K., Hanaoka, G.: Constant-round client-aided secure comparison protocol. In: Lopez, J., Zhou, J., Soriano, M. (eds.) ESORICS 2018. LNCS, vol. 11099, pp. 395–415. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-98989-1_20
25. Nishide, T., Ohta, K.: Multiparty computation for interval, equality, and comparison without bit-decomposition protocol. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 343–360. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-71677-8_23
26. Ogawa, K., Hanaoka, G., Imai, H.: Traitor tracing scheme secure against key exposure and its application to anywhere TV service. IEICE Trans. Fundam. **E90–A**(5), 1000–1011 (2007)
27. 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). https://doi.org/10.1007/978-3-642-15317-4_1
28. Sastry, N., Shankar, U., Wagner, D.: Secure verification of location claims. In: Proceedings of ACM Wireless Security 2003, pp. 1–10 (2003)
29. Schneider, T., Zohner, M.: GMW vs. Yao? Efficient secure two-party computation with low depth circuits. In: Sadeghi, A.-R. (ed.) FC 2013. LNCS, vol. 7859, pp. 275–292. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39884-1_23
30. Schoenmakers, B., Tuyls, P.: Practical two-party computation based on the conditional gate. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 119–136. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-30539-2_10
31. 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). https://doi.org/10.1007/11734727_3
32. ARIB: Conditional Access System Specifications for Digital Broadcasting, ARIB STD-B25 (2007)
33. ARIB: Conditional Access System (Second Generation) and CAS Program Download System Specifications for Digital Broadcasting, ARIB STD-B61 (2017)
34. ETSI: DVB common scrambling algorithm-distribution agreements. Technical report (2013)
35. http://www.nhk.or.jp/hybridcast/online/
36. http://www.hbbtv.org/
37. http://www.hulu.com/
38. http://www.youview.com/