SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

May 2016, Vol. 59 052108:1–052108:15
doi: 10.1007/s11432-015-5469-5

One-to-many authentication for access control in mobile pay-TV systems

Debiao HE[1,2], Neeraj KUMAR[3], Han SHEN[4] & Jong-Hyouk LEE[5]*

[1]*State Key Laboratory of Software Engineering, Computer School, Wuhan University, Wuhan* 430072*, China;*
[2]*Fujian Provincial Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou* 350007*, China;*
[3]*Department of Computer Science and Engineering, Thapar University, Patiala* 147004*, India;*
[4]*State Key Laboratory of Software Engineering, Computer School, Wuhan University, Wuhan* 430072*, China;*
[5]*Department of Computer Science and Engineering, Sangmyung University, Cheonan* 330-720*, Republic of Korea*

Received May 31, 2015; accepted July 7, 2015; published online April 11, 2016

Abstract In traditional authentication schemes for access control in mobile pay-TV systems, one-to-one delivery is used, i.e., one authentication message per request is delivered from a head-end system (HES) to a subscriber. The performance of one-to-one delivery for authentication is not satisfactory as it requires frequent operations which results in high bandwidth consumption. To address this issue, one-to-many authentication for access control in mobile pay-TV systems was developed. It requires only one broadcasted authentication message from a HES to subscribers if there are many requests for the same service in a short period of time. However, later it was revealed that the one-to-many authentication scheme was vulnerable to an impersonation attack, i.e., an attacker without any secret key could not only impersonate the mobile set (MS) to the HES but also impersonate the HES to the MS. Then, a new scheme has been recently introduced for secure operations of one-to-many authentication. However, as shown in this paper, the recent work for one-to-many authentication is still vulnerable to the impersonation attack. To mitigate this attack, in this paper, a new scheme for one-to-many authentication using bilinear pairing is proposed that eliminates security weaknesses in the previous work. Results obtained depict that the new improved scheme in this paper provides better performance in terms of computation and communication overheads.

Keywords authentication, bilinear pairing, conditional access system, mobile pay-TV

Citation He D, Kumar N, Shen H, et al. One-to-many authentication for access control in mobile pay-TV systems. Sci China Inf Sci, 2016, 59(5): 052108, doi: 10.1007/s11432-015-5469-5

1 Introduction

With the development of wireless communication and television (TV) technologies, the mobile pay-TV becomes common in our life. These new technologies bring convenience to the end users as using these technologies, they enjoy pay-TV services using mobile [1] and home networks [2]. To protect interests of users and quality of services, illegitimate accesses must be blocked in this environment. As shown in Figure 1 [3], there are two parts in a typical CAS model, i.e., a Head-End System (HES) and a large number of receivers. Several important components of CAS are described as follows.

* Corresponding author (email: jonghyouk@smu.ac.kr)

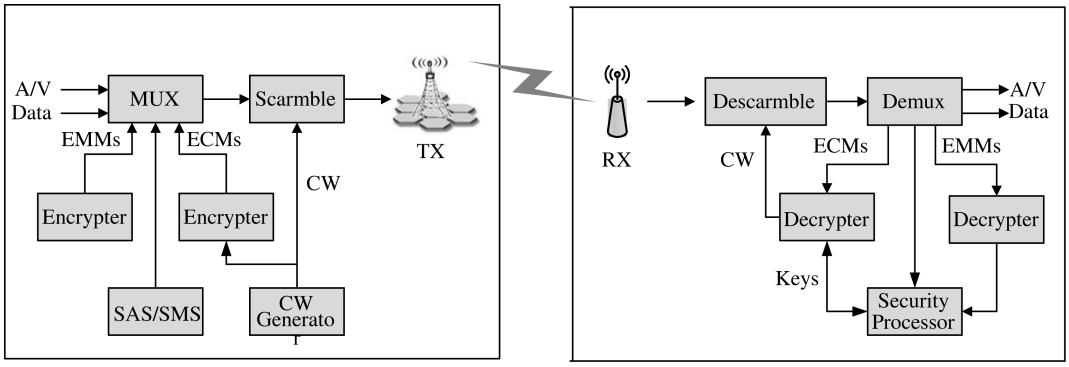

Figure 1 Typical model of CAS.

• **Head-End system (HES).** HES is a system responsible for sending TV services to receivers.

• **Receiver.** Receiver is a subscriber device with a module used for access control.

• **Subscriber authorization system (SAS).** SAS is a system responsible for subscriber authorization.

• **Subscriber management system (SMS).** SMS is a system responsible for subscriber management.

• **Encrypter.** Encrypter is a device responsible for enciphering data.

• **Decrypter.** Decrypter is a device responsible for deciphering data.

• **Multiplexer (MUX).** MUX is a device responsible for multiplexing Audio/Video (A/V) into MPEG-2 transport stream.

• **Demultiplexer (DEMUX).** DEMUX is a device responsible for demultiplexing MPEG-2 transport stream into A/V.

• **Scrambler.** Scrambler is a device responsible for scrambling the signal.

• **Descrambler.** Descrambler is a device responsible for descrambling the signal.

• **Transmitter (TX).** TX is a subsystem responsible for signal transmission.

• **Receiving module (RX).** RX is a subsystem responsible for signal receiving.

• **Entitlement control message (ECM).** ECM is a conditional access message defined by the digital video broadcast (DVB).

• **Entitlement management message (EMM).** EMM is a conditional access message defined by the DVB.

The ITU proposed the first CAS standard for pay-TV in 1992 [3]. However, it did not provide the service provider authentication. Since then, several CASs [4–7] using symmetric cryptosystems were proposed to enhance security. To enjoy the broadcast facility, the symmetric cryptosystems are used in most of those CASs. In these CASs, many users share the same group keys, which is used to encrypt and decrypt TV programs. Huang et al. [4] divided users into different groups according to their preference. However, Wang and Laih [5] found that Huang et al.'s scheme suffered from the key leakage problem and to solve the problem, they proposed a new key distribution scheme. At the same time, Sun et al. [6] proposed a model based on a four-level key hierarchy to support more flexible choices for the end users. Later, Zhu [7] proposed a one-to-many CAS based on the complete subtree method. However, the CAS is not suitable for large system since the number of keys a user should keep is related with the number of users. Furthermore, those CASs using symmetric cryptosystems suffer from a troublesome key distribution problem, and lack of non-repudiation. Also, it cannot withstand the collusion attack [8].

To solve such problems of the CASs using symmetric cryptosystems, Lee et al. [9] proposed an authentication scheme using a digital signature scheme. However, Lee et al.'s scheme cannot protect provider's privacy. To enhance security, Song and Korba [10] proposed an improved authentication scheme using RSA-based blind signatures. Later, Yeung et al. [11] used the RSA algorithm to construct a new CAS. In their scheme, the multimedia and proxy servers encrypt TV programs cooperatively. So, it could withstand the collusion attack. Later, Roh and Jung [12] adopted a RSA-based proxy signature scheme

to design a new authentication method. The above RSA-based CASs are one-to-one mechanism, i.e., the head end system (HES) has to generate a response message for every request message. Therefore, those CASs [9–12] cause poor performance when there are many requests for the same service in a short period of time.

To improve performance, Sun and Leu [13] proposed the first one-to-many authentication scheme for access control in mobile pay-TV systems using elliptic curve cryptography (ECC) [14]. However, Wang and Qin [15] found that Sun and Leu's scheme was vulnerable to the impersonation attack, i.e., an adversary could not only impersonate a mobile set (MS) to the HES but also could impersonate the HES to MS. Besides, Wang and Qin [15] also pointed out that Sun and Leu's scheme could not forbid unauthorized access to mobile TV programs. In order to enhance security, Wang and Qin [15] proposed an improved authentication and claimed that their scheme could withstand various attacks. Unfortunately, as presented in this paper, Wang and Qin's scheme [15] is still vulnerable to the impersonation attack while it does not provide anonymity. This paper proposes a new one-to-many authentication scheme for access control in mobile pay-TV systems, which is provably secure in the random oracle. Performed analysis results confirm that the proposed scheme not only overcomes weaknesses in the existing schemes but also shows better performance in terms of computation and communication overheads.

The rest of the paper is organized as follows. In Section 2, a brief review of Wang and Qin's scheme is provided. In Section 3, the security of Wang and Qin's scheme is analyzed. In Section 4, the proposed authentication scheme is presented. Security analysis and performance analysis are provided in Sections 5 and 6 respectively. Finally, Section 7 concludes this paper.

2 Review of Wang and Qin's scheme

In this section, a brief overview of Wang and Qin's one-to-many authentication scheme [15] is presented. It consists of the following three phases — initialization, issue, and subscription. Notations used in the paper are as follows.

- q: a large prime number.
- E: an elliptic curve.
- G_1: a cyclic additive group generated by P with order q, where G_1 is a subgroup of group of points on elliptic curve E.
- G_2: a multiplicative group with order q.
- e: a bilinear linear map, where $e : G_1 \times G_1 \to G_2$.
- MS_i : the ith mobile set.
- ID_H: the identity string of HES.
- ID_i: the identity string of the ith user;
- Q_H: the public key of HES.
- Q_i: the public key of MS_i.
- P_i: the private key of MS_i.
- Ω_i: the secret key for MS_i.
- Z_H: the services control parameter.
- A_H: the authentication public key of HES.
- A_i: the authentication public key of MS_i.
- SK: the share secret between HES and MS_i.
- k_i: a secret key generated by MS_i.
- k_h: a secret key generated by HES.
- R_t: a service identity number.
- $H_1(\cdot)$: one way hash function mapping $\{0,1\}^* \to G_1$.
- $H_2(\cdot)$: one way hash function mapping $\{0,1\}^* \to G_2$.
- $H_3(\cdot)$: one way hash function mapping $\{0,1\}^* \to Z_q^*$.
- $E_k(\cdot)/D_k(\cdot)$: a symmetric encryption/decryption algorithm with key k.

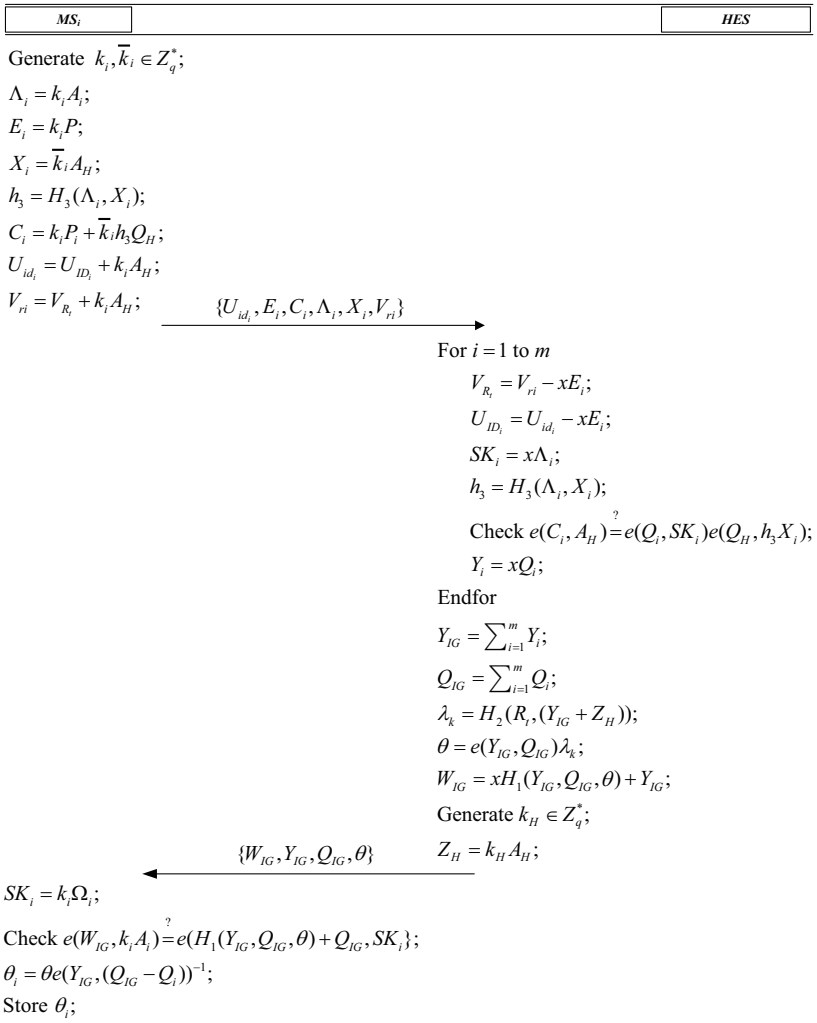

Figure 2 Issue phase of Wang and Qin's scheme.

2.1 Initialization phase

HES generates the system parameters and MS's secret key in this phase.

(1) HES chooses a secure elliptic curve E, a generator point P with order q. HES generates a subgroup G_1 with order q, a multiplicative group G_2 with order q and a bilinear linear map $e : G_1 \times G_1 \to G_2$. HES also chooses three secure hash functions $H_1 : \{0,1\}^* \to G_1$, $H_2 : \{0,1\}^* \to G_2$ and $H_3 : \{0,1\}^* \to Z_q^*$. The system parameters param $= \{E, P, q, G_1, G_2, e, H_1, H_2, H_3\}$ are published by HES.

(2) HES generates two secrets $x, k_h \in Z_q^*$. It also computes HES's public key $Q_H = H_1(ID_H)$, HES's authentication public key $A_H = xP$, and HES's secret services control parameter $Z_H = k_H A_H$.

(3) HES generates a secret s_i. Then, it encodes ID_i to $U_{ID_i} = (Uix, Uiy) \in G_1$ and R_t to $V_{R_t} = (V_x, V_y) \in G_1$. It also computes MS_i's public key $Q_i = H_1(ID_i)$, MS_i's authentication public key $A_i = s_i P$, MS_i's private key $P_i = s_i Q_i$, and MS_i's secret key $\Omega_i = s_i A_H$.

2.2 Issue phase

When a mobile user wants to access a service, his mobile set MS_i sends a service setup request to HES for mutual authentication as shown in Figure 2.

(1) MS_i generates two secrets $k_i, \overline{k}_i \in Z_q^*$ and computes $\Lambda_i = k_i A_i$, $E_i = k_i P$, $X_i = \overline{k}_i A_H$, $h_3 = H_3(\Lambda_i, X_i)$, $C_i = k_i P_i + \overline{k}_i h_3 Q_H$, $U_{id_i} = U_{ID_i} + k_i A_H$, and $V_{ri} = V_{R_t} + k_i A_H$. Then MS_i sends the message $\{U_{id_i}, E_i, C_i, \Lambda_i, X_i, V_{ri}\}$ to HES.

(2) Upon receiving the message $\{U_{id_i}, E_i, C_i, \Lambda_i, X_i, V_{ri}\}$, HES computes $V_{R_t} = V_{ri} - xE_i$ and maps V_{R_t} to V_{R_t}. HES computes $U_{ID_i} = U_{id_i} - xE_i$, maps U_{ID_i} to ID_i, and computes $SK_i = x\Lambda_i$, $h_3 = H_3(\Lambda_i, X_i)$. Then, it checks whether the equation $e(C_i, A_H) = e(Q_i, SK_i)e(Q_H, h_3X_i)$ holds. If the equation holds, HES accepts the MS_i as a legal unit and deducts the fee from the account of the ith user. Otherwise, it rejects the service setup request. For m requests of the same service in a short period of time, HES computes $Y_{IG} = \sum_{i=1}^{m} Y_i$, $Q_{IG} = \sum_{i=1}^{m} Q_i$, $\lambda_k = H_2(R_t, (Y_{IG} + Z_H))$, $\theta = e(Y_{IG}, Q_{IG})\lambda_k$ and $W_{IG} = xH_1(Y_{IG}, Q_{IG}, \theta) + Y_{IG}$, where $Y_i = xQ_i, , i = 1, \ldots, m$. Then, HES generates a new secret $k_H \in Z_q^*$, computes $Z_H = k_H A_H$ for next authentication process, and broadcasts the message $\{W_{IG}, Y_{IG}, Q_{IG}, \theta\}$ to all mobile sets including MS_i.

(3) Upon receiving the message $\{W_{IG}, Y_{IG}, Q_{IG}, \theta\}$, MS_i checks whether the equation $e(W_{IG}, k_iA_i) = e(H_1(Y_{IG}, Q_{IG}, \theta) + Q_{IG}, SK_i\}$ holds, where $SK_i = k_i\Omega_i$. If the equation holds, HES is authenticated. Otherwise, the message is rejected. At last, MS_i computes $\theta_i = \theta e(Y_{IG}, (Q_{IG} - Q_i))^{-1}$ and stores θ_i as the ith token.

2.3 Subscription phase

After getting the ith token θ_i from HES, MS_i could use it to subscribe the services R_t as shown in Figure 3.

(1) MS_i generates two secrets $k_i, \overline{k}_i \in Z_q^*$, computes $\Lambda_i = k_iA_i$, $E_i = k_iP$, $X_i = \overline{k}_iA_H$, $h_3 = H_3(\Lambda_i, X_i, \theta_i)$, $C_i = k_iP_i + \overline{k}_ih_3Q_H$, $U_{id_i} = U_{ID_i} + k_iA_H$ and $V_{ri} = V_{R_t} + k_iA_H$. Then, MS_i sends the message $\{U_{id_i}, E_i, C_i, \Lambda_i, X_i, V_{ri}, \theta_i\}$ to HES.

(2) Upon receiving the message $\{U_{id_i}, E_i, C_i, \Lambda_i, X_i, V_{ri}, \theta_i\}$, HES computes $V_{R_t} = V_{ri} - xE_i$, $U_{ID_i} = U_{id_i} - xE_i$ and maps them to V_{R_t}, ID_i respectively. HES restores Y_{IG} and λ_i, which are built in the issue phase. HES computes $SK_i = x\Lambda_i$ and $h_3 = H_3(\Lambda_i, X_i, \theta_i)$. It then checks whether both of the equations $e(C_i, A_H) = e(Q_i, SK_i)e(Q_H, h_3X_i)$ and $\theta_i = e(Y_{ID}, Q_i)\lambda_i$ hold. HES rejects the request if either of the two equations does not hold. For l requests of the same service in a short period of time, HES computes the authentication parameters $Y_{SG} = \sum_{i=1}^{l} Y_i$, $Q_{SG} = \sum_{i=1}^{l} Q_i$ and $\lambda_{SG} = \prod_{i=1}^{l} \lambda_i$, where $Y_i = xQ_i, i = 1, \ldots, l$. HES then computes a group authentication key $\gamma_{SG} = e(Y_{IG}, Q_{SG})\lambda_{SG}$ for l request. Afterwards, HES computes $W_{SG} = xH_1(Y_{SG}, Q_{SG}, \gamma_{SG}) + Y_{IG}$. Finally, HES broadcasts the message $\{W_{SG}, Y_{SG}, Q_{SG}, \gamma_{SG}\}$ to all mobile sets including MS_i.

(3) Upon receiving the message $\{W_{SG}, Y_{SG}, Q_{SG}, \gamma_{SG}\}$, MS_i checks whether the equation $e(W_{SG}, k_iA_i) = e(H_1(Y_{SG}, Q_{SG}, \gamma_{SG}) + Q_{SG}, SK_i\}$ holds, where $SK_i = k_i\Omega_i$. If the equation holds, HES is authenticated; otherwise, the message is rejected. MS_i computes the ith authentication key $\gamma_i = \gamma_{SG}e(Y_{IG}, Q_{SG} - Q_i)^{-1}$; MS_i then uses the authentication key γ_i and its private key to get the service.

3 Cryptanalysis of Wang and Qin's scheme

3.1 Impersonation attack

A possible impersonation attack to Wang and Qin's scheme is presented, i.e., an adversary $\mathcal{A}$ without MS_i's secret could impersonate MS_i to HES through the following steps.

(1) $\mathcal{A}$ generates two secrets $k_i, \overline{k}_i \in Z_q^*$, computes $\Lambda_i = k_iP$, $E_i = k_iP$, $X_i = \overline{k}_iA_H$, $h_3 = H_3(\Lambda_i, X_i)$, $C_i = k_iQ_i + \overline{k}_ih_3Q_H$, $U_{id_i} = U_{ID_i} + k_iA_H$ and $V_{ri} = V_{R_t} + k_iA_H$. Then $\mathcal{A}$ sends the message $\{U_{id_i}, E_i, C_i, \Lambda_i, X_i, V_{ri}\}$ to HES. Note that since $\Lambda_i = k_iP$, $C_i = k_iQ_i + \overline{k}_ih_3Q_H$, $A_H = xP$, $X_i = \overline{k}_iA_H$,

$$SK_i = x\Lambda_i = x(k_iP) = k_ixP = k_iA_H \tag{1}$$

and

$$\begin{aligned} e(C_i, A_H) &= e(k_iQ_i + \overline{k}_ih_3Q_H, A_H) \\ &= e(k_iQ_i, A_H)e(\overline{k}_ih_3Q_H, A_H) \\ &= e(Q_i, k_iA_H)e(Q_H, \overline{k}_ih_3A_H) \end{aligned}$$

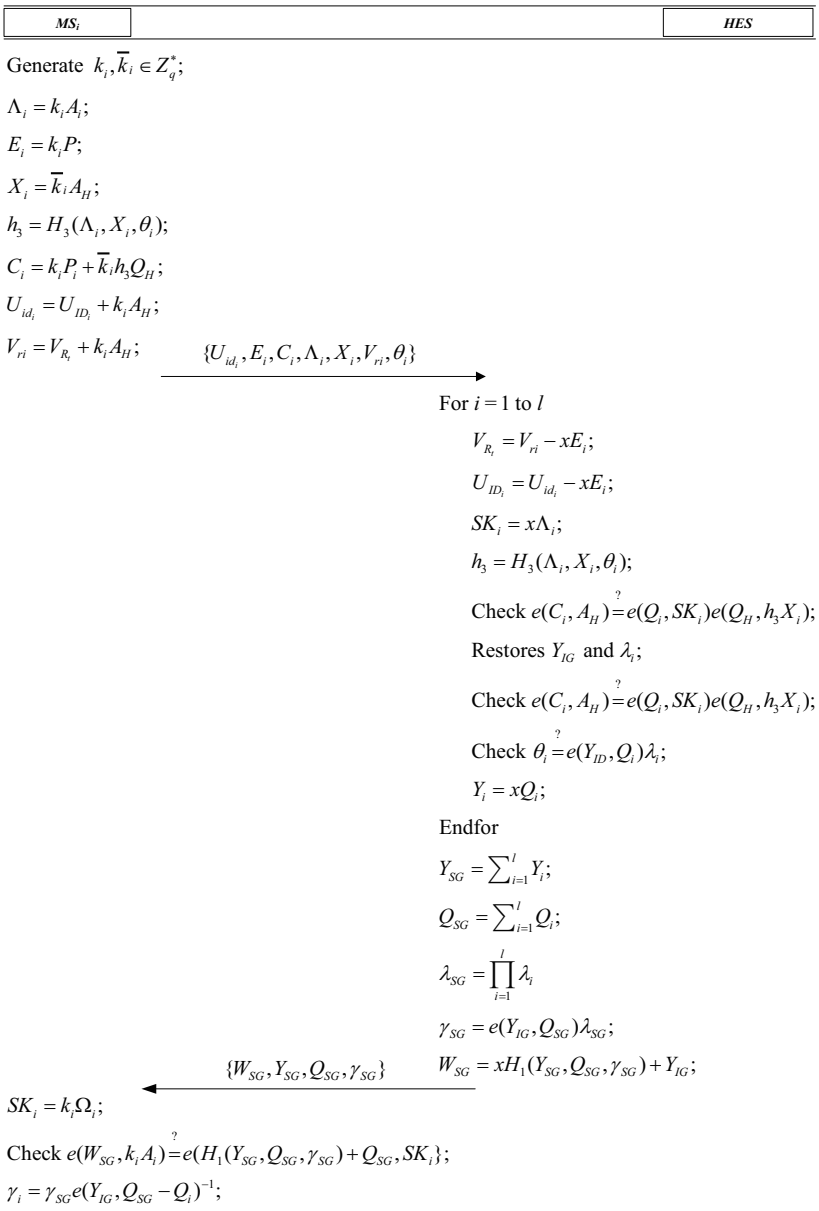

Figure 3 Subscription phase of Wang and Qin's scheme.

$$= e(Q_i, SK_i)e(Q_H, h_3 X_i). \tag{2}$$

Therefore, the message $\{U_{id_i}, E_i, C_i, \Lambda_i, X_i, V_{ri}\}$ generated by $\mathcal{A}$ could pass HES's verification.

(2) Upon receiving the message $\{U_{id_i}, E_i, C_i, \Lambda_i, X_i, V_{ri}\}$, HES computes $V_{R_t} = V_{ri} - xE_i$ and maps V_{R_t} to R_t. HES computes $U_{ID_i} = U_{id_i} - xE_i$, maps U_{ID_i} to ID_i, computes $SK_i = x\Lambda_i$, $h_3 = H_3(\Lambda_i, X_i)$ and checks whether the equation $e(C_i, A_H) = e(Q_i, SK_i)e(Q_H, h_3 X_i)$ holds (From Eqs. (1) and (2), we know the equation holds). For m request of the same service in a short period of time, HES computes $Y_{IG} = \sum_{i=1}^{m} Y_i$, $Q_{IG} = \sum_{i=1}^{m} Q_i$, $\lambda_k = H_2(R_t, (Y_{IG} + Z_H))$, $\theta = e(Y_{IG}, Q_{IG})\lambda_k$ and $W_{IG} = xH_1(Y_{IG}, Q_{IG}, \theta) + Y_{IG}$, where $Y_i = xQ_i, , i = 1, \ldots, m$. Then, HES generates a new secret $k_H \in Z_q^*$, computes $Z_H = k_H A_H$ for the next authentication process and broadcasts the message $\{W_{IG}, Y_{IG}, Q_{IG}, \theta\}$ to all mobile sets including MS_i.

(3) Upon intercepting the message $\{W_{IG}, Y_{IG}, Q_{IG}, \theta\}$, $\mathcal{A}$ checks whether the equation $e(W_{IG}, k_i A_i) = e(H_1(Y_{IG}, Q_{IG}, \theta) + Q_{IG}, SK_i\}$ holds, where $SK_i = k_i \Omega_i$. If the equation holds, HES is authenticated. Otherwise, the message is rejected. At last, $\mathcal{A}$ computes $\theta_i = \theta e(Y_{IG}, (Q_{IG} - Q_i))^{-1}$ and stores θ_i as the ith token.

From the above description, it is confirmed that $\mathcal{A}$ could generate a legal message and get the correct token. Therefore, $\mathcal{A}$ could impersonate MS_i to HES successfully. Similarly, it is possible that $\mathcal{A}$ could impersonate MS_i to HES successfully in the subscription phase.

3.2 Anonymity problem

Another attack is that $\mathcal{A}$ could get the user's identity through the off-line guessing. The details are described as follows.

(1) $\mathcal{A}$ intercepts the message $\{U_{id_i}, E_i, C_i, \Lambda_i, X_i, V_{ri}\}$ sent by MS_i, where $\Lambda_i = k_i A_i$, $E_i = k_i P$, $X_i = \overline{k}_i A_H$, $h_3 = H_3(\Lambda_i, X_i)$, $C_i = k_i P_i + \overline{k}_i h_3 Q_H$, $U_{id_i} = U_{ID_i} + k_i A_H$ and $V_{ri} = V_{R_t} + k_i A_H$.

(2) $\mathcal{A}$ guesses an identity ID_i^* and a service identity number R_t^* and maps them to $U_{ID_i}^*$ and $V_{R_t}^*$ separately.

(3) $\mathcal{A}$ computes $T_1 = U_{id_i} - U_{ID_i}^*$ and $T_2 = V_{ri} - V_{R_t}^*$, then $\mathcal{A}$ checks whether T_1 and T_2 are equal. If these are equal, $\mathcal{A}$ confirms that ID_i^* is the user's identity. Otherwise, $\mathcal{A}$ repeats steps (2) and (3) until the correct identity is found.

In the proposed attack, $\mathcal{A}$ tries all possible offline combinations of service identity numbers and identities in a given set of values. The proposed attack is valid since both of service identity numbers and identities are human-memorable short strings. Therefore, Wang and Qin's scheme cannot provide user anonymity. Besides, the proposed method is also valid for Sun and Leu's scheme.

4 The proposed scheme

The proposed one-to-many authentication scheme that is robust against the above attacks is illustrated in the following phases- initialization, issue, and subscription.

4.1 Initialization phase

(1) HES chooses a secure elliptic curve E, a generator point P with order q. HES generates a subgroup G_1 with order q, a multiplicative group G_2 with order q, and a bilinear linear map $e : G_1 \times G_1 \to G_2$. HES also chooses three secure hash functions $H_1 : \{0,1\}^* \to G_1$, $H_2 : \{0,1\}^* \to G_2$ and $H_3 : \{0,1\}^* \to Z_q^*$. Then, HES publishes param $= \{E, P, q, G_1, G_2, e, H_1, H_2, H_3\}$.

(2) HES generates two secrets $x, k_h \in Z_q^*$. Then, it computes HES's public key $Q_H = H_1(ID_H)$, HES's authentication public key $A_H = xP$, and HES's secret services control parameter $Z_H = k_H A_H$.

(3) HES generates a secret s_i, encodes ID_i to $U_{ID_i} = (Ui_x, Ui_y) \in G_1$ and R_t to $V_{R_t} = (V_x, V_y) \in G_1$. It then computes MS_i's public key $Q_i = H_1(ID_i)$, MS_i's authentication public key $A_i = s_i P$, MS_i's private key $P_i = s_i Q_i$, and MS_i's secret key $\Omega_i = s_i A_H$.

4.2 Issue phase

When a mobile user wants to access a service, his mobile set MS_i sends a service setup request to HES for mutual authentication as shown in Figure 4.

(1) MS_i generates a secret $k_i \in Z_q^*$, computes $E_i = k_i P$, $X_i = k_i A_H$, $h_3 = H_3(A_i, E_i, X_i, ID_i, R_t, T_i)$, $C_i = h_3 P_i + k_i Q_H$ and $\Lambda_i = E_{X_i}(ID_i, R_t, C_i, T_i)$, where T_i is the current timestamp. Then, MS_i sends the message $\{E_i, \Lambda_i\}$ to HES.

(2) Upon receiving the message $\{E_i, \Lambda_i\}$, HES computes $X_i = xE_i$ and $(ID_i, R_t, C_i, T_i) = D_{X_i}(\Lambda_i)$. HES checks the freshness of T_i. If it is not fresh, HES rejects the request. Otherwise, HES computes $h_3 = H_3(A_i, E_i, X_i, ID_i, R_t, T_i)$ and checks whether the equation $e(C_i, P) = e(Q_i, h_3 A_i) e(Q_H, E_i)$ holds. If the equation holds, HES accepts the MS_i as a legal unit and deducts the fee from the account of the ith user. Otherwise, it rejects the service setup request. For m requests of the same service in a short period of time, HES computes $Y_{IG} = \sum_{i=1}^{m} Y_i$, $Q_{IG} = \sum_{i=1}^{m} Q_i$, $\lambda_k = H_2(R_t, (Y_{IG} + Z_H))$, $\theta = e(Y_{IG}, Q_{IG})\lambda_k$ and $W_{IG} = xH_1(Y_{IG}, Q_{IG}, \theta, T_H) + Y_{IG}$, where $Y_i = xQ_i, i = 1, \ldots, m$ and T_H is the current timestamp.

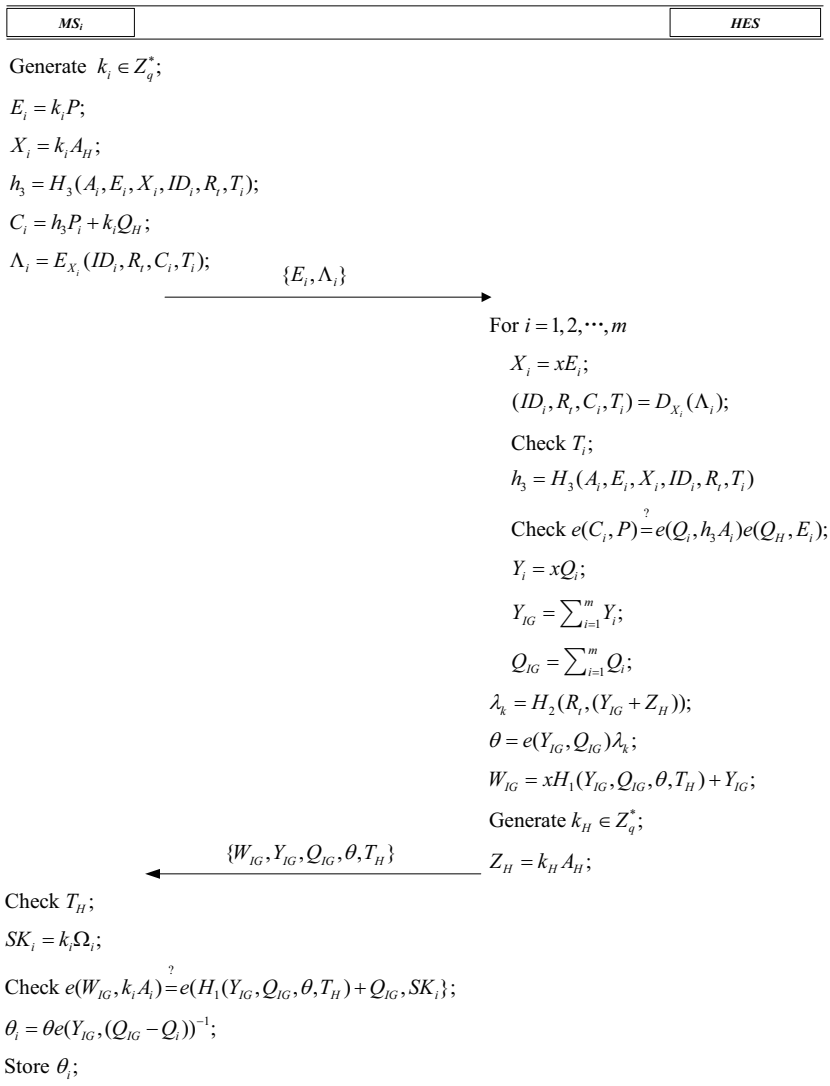

Figure 4 Issue phase of the proposed scheme.

Then, HES generates a new secret $k_H \in Z_q^*$, computes $Z_H = k_H A_H$ for the next authentication process, and broadcasts the message $\{W_{IG}, Y_{IG}, Q_{IG}, \theta, T_H\}$ to all mobile sets including MS_i.

(3) Upon receiving the message $\{W_{IG}, Y_{IG}, Q_{IG}, \theta, T_H\}$, MS_i checks the freshness of T_H. If T_H is not fresh, MS_i stops the session. Otherwise, MS_i checks whether the equation $e(W_{IG}, k_i A_i) = e(H_1(Y_{IG}, Q_{IG}, \theta, T_H) + Q_{IG}, SK_i)$ holds, where $SK_i = k_i \Omega_i$. If the equation holds, HES is authenticated. Otherwise, the message is rejected. At last, MS_i computes $\theta_i = \theta e(Y_{IG}, (Q_{IG} - Q_i))^{-1}$ and stores θ_i as the ith token.

4.3 Subscription phase

After getting the ith token θ_i from HES, MS_i could use it to subscribe the services R_t as shown in Figure 5.

(1) MS_i generates a secret $k_i \in Z_q^*$, computes $E_i = k_i P$, $X_i = k_i A_H$, $h_3 = H_3(A_i, E_i, X_i, ID_i, R_t, T_i, \theta_i)$, $C_i = h_3 P_i + k_i Q_H$ and $\Lambda_i = E_{X_i}(ID_i, R_t, C_i, T_i, \theta_i)$, where T_i is the current timestamp. Then, MS_i sends the message $\{E_i, \Lambda_i\}$ to HES.

(2) Upon receiving the message $\{E_i, \Lambda_i\}$, HES computes $X_i = xE_i$ and $(ID_i, R_t, C_i, T_i, \theta_i) = D_{X_i}(\Lambda_i)$. HES checks the freshness of T_i. If it is not fresh, HES rejects the request. Otherwise, HES restores Y_{IG} and λ_i, which are built in the issue phase. HES computes $h_3 = H_3(A_i, E_i, X_i, ID_i, R_t, T_i, \theta_i)$ and checks

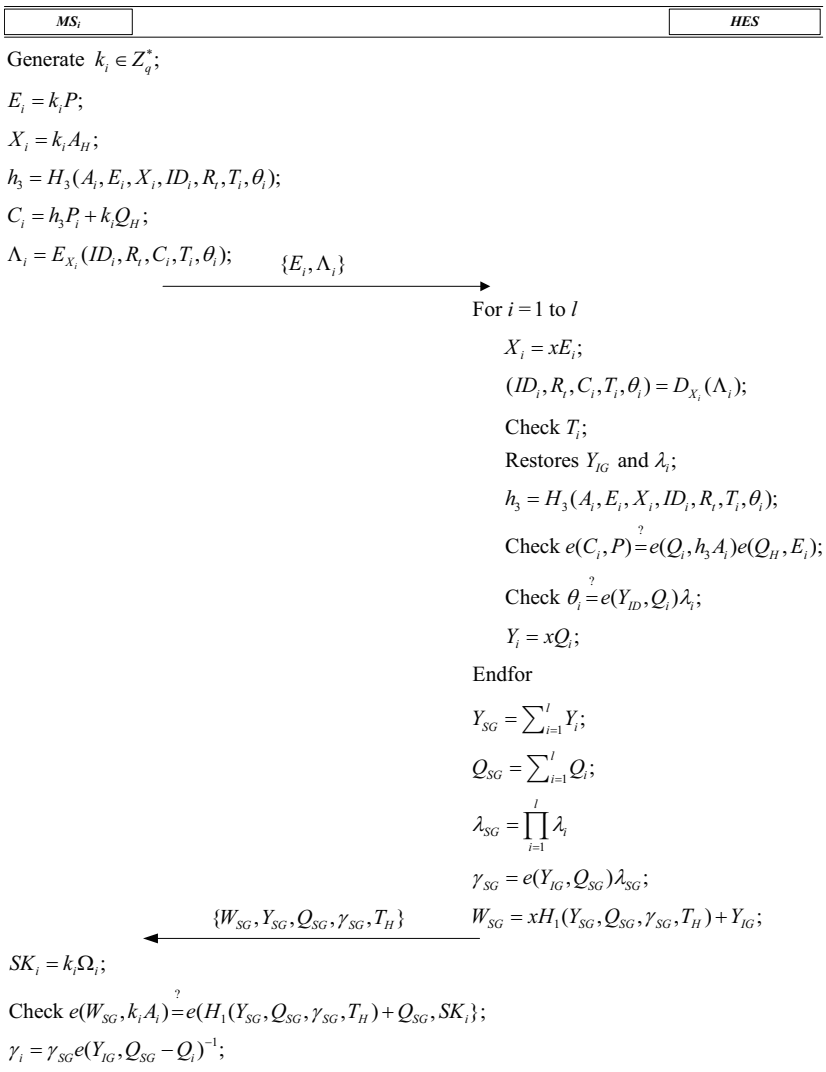

Figure 5 Subscription phase of the proposed scheme.

whether both of the equations $e(C_i, P) = e(Q_i, h_3 A_i)e(Q_H, E_i)$ and $\theta_i = e(Y_{ID}, Q_i)\lambda_i$ hold. HES rejects the request if any of the two equations does not hold. For l requests of the same service in a short period of time, HES computes the authentication parameters $Y_{SG} = \sum_{i=1}^{l} Y_i$, $Q_{SG} = \sum_{i=1}^{l} Q_i$ and $\lambda_{SG} = \prod_{i=1}^{l} \lambda_i$, where $Y_i = xQ_i, i = 1, \ldots, l$. HES then computes a group authentication key $\gamma_{SG} = e(Y_{IG}, Q_{SG})\lambda_{SG}$ for l request. Afterwards, HES computes $W_{SG} = xH_1(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H) + Y_{IG}$, where T_H is the current timestamp. Finally, HES broadcasts the message $\{W_{SG}, Y_{SG}, Q_{SG}, \gamma_{SG}, T_H\}$ to all mobile sets including MS_i.

(3) Upon receiving the message $\{W_{SG}, Y_{SG}, Q_{SG}, \gamma_{SG}, T_H\}$, MS_i checks the freshness of T_H. If it is not fresh, MS_i rejects the session. Otherwise, MS_i checks whether the equation $e(W_{SG}, k_i A_i) = e(H_1(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H) + Q_{SG}, SK_i)$ holds, where $SK_i = k_i \Omega_i$. If the equation holds, HES is authenticated. Otherwise, the message is rejected. MS_i computes the ith authentication key $\gamma_i = \gamma_{SG} e(Y_{IG}, Q_{SG} - Q_i)^{-1}$, MS_i then uses the authentication key γ_i and its private key to get the service.

5 Security analysis

In this section, the random oracle model based security analysis for the proposed scheme is presented. This analysis only focuses on the issue phase as the subscription phase is similarly analyzed.

5.1 Security model

Similar to Bellare et al.'s security model [16], in the authentication phase of authentication scheme, every participant is either a mobile set $MS \in$ MobileSet or a head end system HES $\in$ HeadEndSystem and MS gets a secret key from HES. Let $\mathcal{A}$ and P^k denote a probabilistic polynomial-time adversary and kth instance of a participant P separately, where P is the MS or HES. The security of the authentication scheme is represented as a game between a challenger $\mathcal{A}$ and a simulator $\mathcal{S}$. $\mathcal{A}$ could make the following queries:

• $H_i(m)$: Upon receiving query, $\mathcal{S}$ first checks whether there is a tuple (m, Q_i) in the list L_{H_i}. If so, $\mathcal{S}$ returns Q_i to $\mathcal{A}$. Otherwise, $\mathcal{S}$ generates a random point $Q_i \in G_i$, records (m, Q_i) into L_{H_i} and returns Q_1 to $\mathcal{A}$, where L_{H_i} is initialized to empty and $i = 1, 2$.

• $H_3(m)$: Upon receiving query, $\mathcal{S}$ first checks whether there is a tuple (m, r) in the list L_{H_3}. If so, $\mathcal{S}$ returns r to $\mathcal{A}$. Otherwise, $\mathcal{S}$ generates a random point $r \in Z_q^*$, records (m, r) into L_{H_3} and returns r to $\mathbf{A}$, where L_{H_3} is initialized to empty.

• SymEnc$([E, D], k, [M, C])$: Upon receiving an encryption query SymEnc(E, k, M) with the plaintex M, $\mathcal{S}$ first checks if there is a tuple (k, M, C) in the list L_{Sym}. If so, $\mathcal{S}$ returns the ciphertext C to $\mathcal{A}$. Otherwise, $\mathcal{S}$ generates a random number C, records (k, M, C) into L_{Sym} and returns C to $\mathcal{A}$. Similarly, upon receiving a decryption query SymEnc(D, k, C), $\mathcal{S}$ first checks if a tuple (k, M, C) exists in the list L_{Sym}. If so, $\mathcal{S}$ returns M to $\mathcal{A}$. Otherwise, $\mathcal{S}$ generates a random number M, records (k, M, C) into L_{Sym} and returns M to $\mathcal{A}$.

• Create(MS) : Upon receiving the query, $\mathcal{S}$ generates private key, secret key and authentication public key for MS, and returns the authentication public key to $\mathcal{A}$.

• Create(HES) : Upon receiving the query, $\mathcal{S}$ generates private key, secret key, authentication public key and secret services control parameter for HES and returns the authentication public key to $\mathcal{A}$.

• Send(P^k, m) : Upon receiving the query, $\mathcal{S}$ outputs the message that P^k generates upon receipt of m.

• Reveal(P^k) : Upon receiving the query, $\mathcal{S}$ returns the session key of the participant instance P^k to the adversary $\mathcal{A}$.

• Corrupt(P^k) : Upon receiving the query, $\mathcal{S}$ outputs the private key of P to $\mathcal{A}$.

It is true: (1) $\mathcal{A}$ could violate MS-to-HES authentication of an authentication scheme Π if he could generate a login request message; and (2) $\mathcal{A}$ could violate HES-to-MS authentication of an authentication scheme Π if he could generate a response message. Let $\text{Adv}_{\Pi}^{\text{HES-to-MS}}(A)$ and $\text{Adv}_{\Pi}^{\text{MS-to-HES}}(A)$ denote the probability that $\mathcal{A}$ could violate MS-to-HES authentication and HES-to-MS authentication respectively.

Definition 1. An authentication scheme Π for access control in mobile pay-TV systems is mutual authentication (MA)-secure if the sum of $\text{Adv}_{\Pi}^{\text{HES-to-MS}}(A)$ and $\text{Adv}_{\Pi}^{\text{MS-to-HES}}(A)$ is negligible.

5.2 Security analysis

The security analysis confirms the proposed scheme is MA-secure in the random oracle and is described in details as follows.

Lemma 1. If there is an adversary $\mathcal{A}$ could violate MS-to-HES authentication of our authentication scheme with a non-negligible advantage ε and within time t, there is an algorithm $\mathcal{S}$, which could solve the computational Diffie-Hellman problem.

Proof. First of all, the identity attack is focused. Assume that there is an adversary $\mathcal{A}$ could run an adaptive chosen message attack and an identity attack with a non-negligible advantage ε within time t. In view of Lemma 1 of [17], there is an algorithm A_0, which could run an adaptive chosen message attack for a fixed identity with a non-negligible advantage $\varepsilon_0 \geqslant \varepsilon(1 - 1/q_{H_1})/q_{H_1}$ within time $t_0 \leqslant t$, where q_{H_1} is the number of H_1-query made by $\mathcal{A}$. Without losing generality, it is confirmed that the fixed identity is the identity of the ith user.

Assume that A_0 could generate a legal login request message $\{E_i, \Lambda_i\}$ that could be accepted by HES with a non-negligible advantage ε_0 within time t_0, where $E_i = k_i P$, $X_i = k_i A_H$, $h_3 = H_3(A_i, E_i, X_i, ID_i,$

$R_t, T_i)$, $C_i = h_3 P_i + k_i Q_H$, $\Lambda_i = E_{X_i}(ID_i, R_t, C_i, T_i)$ and T_i is the current timestamp. Through the forking lemma [18], it is confirmed that A_0 outputs another message $\{E_i, \Lambda_i'\}$ if we replay T_i with the same random tape but different choice of H_3, where $E_i = k_i P$, $X_i = k_i A_H$, $h_3' = H_3(A_i, E_i, X_i, ID_i, R_t, T_i)$, $C_i' = h_3' P_i + k_i Q_H$ and $\Lambda_i' = E_{X_i}(ID_i, R_t, C_i', T_i)$.

Since $\{E_i, \Lambda_i\}$ and $\{E_i, \Lambda_i'\}$ could pass HES's verification, the following two equations are given

$$e(C_i, P) = e(Q_i, h_3 A_i) e(Q_H, E_i) \tag{3}$$

and

$$e(C_i', P) = e(Q_i, h_3' A_i) e(Q_H, E_i). \tag{4}$$

Let $A_i = aP$ and $Q_i = bP$. Then, the followings are given

$$\begin{aligned} e(C_i - C_i', P) &= \frac{e(C_i, P)}{e(C_i', P)} = \frac{e(Q_i, h_3 A_i) e(Q_H, E_i)}{e(Q_i, h_3' A_i) e(Q_H, E_i)} \\ &= \frac{e(Q_i, h_3 A_i)}{e(Q_i, h_3' A_i)} = \frac{e(bP, h_3 aP)}{e(bP, h_3' aP)} \\ &= \frac{e(h_3 abP, P)}{e(h_3' abP, P)} = e((h_3 - h_3')abP, P) \end{aligned} \tag{5}$$

and

$$abP = (h_3 - h_3')^{-1}(C_i - C_i'). \tag{6}$$

Therefore, for a given instance $(P, A_i, Q_i) = (P, aP, bP)$ of the computational Diffie-Hellman problem, $\mathcal{S}$ could use the adversary $\mathcal{A}$ to solve the computational Diffie-Hellman problem with a non-negligible advantage$\varepsilon_0 \geqslant \varepsilon(1 - 1/q_{H_1})/q_{H_1}$ within time $t_0 \leqslant t$.

Lemma 2. If there is an adversary, $\mathcal{A}$ could violate HES-to-MS authentication of our authentication scheme with a non-negligible advantage ε and within time t, there is an algorithm $\mathcal{S}$, which could solve the computational Diffie-Hellman problem.

Proof. Let Event$^{\text{MS-to-HES}}$ and Event$^{\text{HES-to-MS}}$ denote the event violating MS-to-HES authentication and HES-to-MS authentication separately. From Lemma 1, it is known that Event$^{\text{MS-to-HES}}$ does not occur. Assume that $\mathcal{A}$ could violate HES-to-MS authentication, i.e., $\mathcal{A}$ could generate a legal response message $\{W_{IG}, Y_{IG}, Q_{IG}, \theta, T_H\}$ with a non-negligible advantage ε after receiving the message $\{E_i, \Lambda_i\}$ sent by MS, where $Y_i = xQ_i, i = 1, \ldots, m$, $Y_{IG} = \sum_{i=1}^m Y_i$, $Q_{IG} = \sum_{i=1}^m Q_i$, $\lambda_k = H_2(R_t, (Y_{IG} + Z_H))$, $\theta = e(Y_{IG}, Q_{IG})\lambda_k$ and $W_{IG} = xH_1(Y_{IG}, Q_{IG}, \theta, T_H) + Y_{IG}$. Through the forking lemma [18], it is confirmed that A_0 outputs another message $\{W_{IG}', Y_{IG}, Q_{IG}, \theta, T_H\}$ if we replay T_i with the same random tape but different choice of H_1, where $Y_i = xQ_i, i = 1, \ldots, m$, $Y_{IG} = \sum_{i=1}^m Y_i$, $Q_{IG} = \sum_{i=1}^m Q_i$, $\lambda_k = H_2(R_t, (Y_{IG} + Z_H))$, $\theta = e(Y_{IG}, Q_{IG})\lambda_k$ and $W_{IG}' = xH_1'(Y_{IG}, Q_{IG}, \theta, T_H) + Y_{IG}$.

Since $\{W_{IG}, Y_{IG}, Q_{IG}, \theta, T_H\}$ and $\{W_{IG}', Y_{IG}, Q_{IG}, \theta, T_H\}$ are legal response messages, the followings are given

$$e(W_{SG}, k_i A_i) = e(H_1(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H) + Q_{SG}, SK_i) \tag{7}$$

and

$$e(W_{SG}', k_i A_i) = e(H_1'(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H) + Q_{SG}, SK_i). \tag{8}$$

Since $SK_i = k_i \Omega_i$, $\Omega_i = s_i A_H$, $A_i = s_i P$ and $A_H = xP$, followings are given

$$\begin{aligned} e(W_{SG} - W_{SG}', k_i A_i) &= \frac{e(W_{SG}, k_i A_i)}{e(W_{SG}', k_i A_i)} = \frac{e(H_1(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H) + Q_{SG}, SK_i)}{e(H_1'(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H) + Q_{SG}, SK_i)} \\ &= e(H_1(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H) - H_1'(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H), SK_i) \\ &= e(H_1(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H) - H_1'(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H), k_i \Omega_i) \\ &= e(H_1(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H) - H_1'(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H), k_i s_i A_H) \\ &= e(H_1(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H) - H_1'(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H), k_i s_i xP) \end{aligned}$$

$$= e(H_1(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H) - H_1'(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H), xk_i s_i P)$$
$$= e(H_1(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H) - H_1'(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H), xk_i A_i)$$
$$= e(xH_1(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H) - H_1'(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H), k_i A_i) \quad (9)$$

and

$$x(H_1(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H) - H_1'(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H)) = W_{SG} - W_{SG}'. \quad (10)$$

Therefore, for the instance $(P, A_H, Q) = (P, aP, bP)$ of the computational Diffie-Hellman problem, $\mathcal{S}$ could use the adversary $\mathcal{A}$ to solve the computational Diffie-Hellman problem with a non-negligible advantage ε within time t, where

$$Q = H_1(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H) - H_1'(Y_{SG}, Q_{SG}, \gamma_{SG}, T_H).$$

Theorem 1. The proposed authentication scheme for access control in mobile pay-TV systems is MA-secure.

Proof. It is well known that there is no polynomial-time algorithm that could solve the computational Diffie-Hellman problem. From Lemma 1 and Lemma 2, there is no adversary that could violate MS-to-HES authentication or HES-to-MS authentication of the proposed authentication scheme. Therefore, it is concluded that the proposed scheme is MA-secure.

5.3 Other discussions

In this subsection, we prove that the proposed scheme provides mutual authentication and anonymity [19–21], while withstanding the replay attack, impersonation attack, man-in-the-middle attack, and modification attack [22–24].

Mutual authentication. From Lemma 1 and Lemma 2, it is known that any adversary cannot generate a legal message $\{E_i, \Lambda_i\}$ or $\{W_{IG}, Y_{IG}, Q_{IG}, \theta, T_H\}$, where $E_i = k_i P$, $X_i = k_i A_H$, $h_3 = H_3(A_i, E_i, X_i, ID_i, R_t, T_i)$, $C_i = h_3 P_i + k_i Q_H$, $\Lambda_i = E_{X_i}(ID_i, R_t, C_i, T_i)$, $Y_i = xQ_i, i = 1, \ldots, m$, $Y_{IG} = \sum_{i=1}^{m} Y_i$, $Q_{IG} = \sum_{i=1}^{m} Q_i$, $\lambda_k = H_2(R_t, (Y_{IG} + Z_H))$, $\theta = e(Y_{IG}, Q_{IG})\lambda_k$ and $W_{IG} = xH_1(Y_{IG}, Q_{IG}, \theta, T_H) + Y_{IG}$. Then, MS_i and HES could authenticate each other by checking the validity of the two messages separately. Therefore, the proposed scheme provides mutual authentication.

Anonymity. From the description of the proposed scheme, we know that the user's identity ID_i and the service identity number R_t are hidden in the message $\{E_i, \Lambda_i\}$, where $E_i = k_i P$, $X_i = k_i A_H$, $h_3 = H_3(A_i, E_i, X_i, ID_i, R_t, T_i)$, $C_i = h_3 P_i + k_i Q_H$ and $\Lambda_i = E_{X_i}(ID_i, R_t, C_i, T_i)$. The adversary has to compute $X_i = k_i xP$ from $E_i = k_i P$ and $A_H = xP$ if he wants to get the user's identity ID_i and the service identity number R_t. Then, he has to solve the computational Diffie-Hellman problem. Therefore, the proposed scheme provides anonymity.

Replay attack. An adversary may intercept the message $\{E_i, \Lambda_i\}$ and try to impersonate MS_i by replaying it to HES, where, $E_i = k_i P$, $X_i = k_i A_H$, $h_3 = H_3(A_i, E_i, X_i, ID_i, R_t, T_i)$, $C_i = h_3 P_i + k_i Q_H$ and $\Lambda_i = E_{X_i}(ID_i, R_t, C_i, T_i)$. HES could find the attack by checking whether the timestamp T_i is fresh. It is demonstrated that MS_i finds the replay of the message $\{W_{IG}, Y_{IG}, Q_{IG}, \theta, T_H\}$. Therefore, the proposed scheme withstands replay attack.

Impersonation attack. From the above discussion, it is confirmed that any adversary cannot impersonate MS_i/HES to HES/MS_i by replaying legal message. To impersonate MS_i/HES to HES/MS_i, he has to generate a legal message $\{E_i, \Lambda_i\}/\{W_{IG}, Y_{IG}, Q_{IG}, \theta, T_H\}$ by himself. However, Lemma 1 and Lemma 2 show that there is no adversary which could generate the message $\{E_i, \Lambda_i\}$ or $\{W_{IG}, Y_{IG}, Q_{IG}, \theta, T_H\}$. Therefore, the proposed scheme withstands the replay attack.

Man-in-the-middle attack. The above discussion shows that the proposed scheme provides mutual authentication between MS_i and HES. Therefore, the proposed scheme withstands man-in-the middle attack.

Modification attack. Suppose that there is an adversary which modifies the message $\{E_i, \Lambda_i\}/\{W_{IG}, Y_{IG}, Q_{IG}, \theta, T_H\}$ and sends it to HES/MS_i. HES/MS_i could find the modification by checking whether

Table 1 Computation cost comparison

	Issue phase		Subscription phase	
	MS_i	HES	MS_i	HES
Sun and Leu's scheme	$3T_e$+$9T_s \approx 18T_s$	$(4m+1)T_e$+$4mT_s$ $\approx(16m+1)T_s$	$3T_e$+$6T_s \approx 15T_s$	$4mT_e$+$2mT_s$ $\approx(14m)T_s$
Wang and Qin's scheme	$3T_e$+$8T_s \approx 17T_s$	$(3m+1)T_e$+$(4m+1)$ T_s $\approx(13m+4)T_s$	$3T_e$+$8T_s \approx 17T_s$	$(4m+1)T_e$+$(4m+1)$ T_s $\approx(16m+4)T_s$
The proposed scheme	$3T_e$+$5T_s \approx 14T_s$	$(3m+1)T_e$+$(3m+1)$ T_s $\approx(12m+4)T_s$	$3T_e$+$5T_s \approx 14T_s$	$(3m+1)T_e$+$(3m+1)$ T_s $\approx(12m+4)T_s$

Table 2 Communication cost comparison

	Issue phase	Subscription phase
Sun and Leu's scheme	(1920m+800)bits	(1120m+800)bits
Wang and Qin's scheme	(1920m+1152)bits	(2080m+1152)bits
The proposed scheme	(736m+1152)bits	(896m+1152)bits

$e(C_i, P) = e(Q_i, h_3A_i)e(Q_H, E_i)/\ e(W_{IG}, k_iA_i) = e(H_1(Y_{IG}, Q_{IG}, \theta, T_H) + Q_{IG}, SK_i)$ since $\{E_i, C_i\}/\{W_{IG}\}$ is a digital signature generated by MS_i/HES. Therefore, the proposed scheme withstands the modification attack.

6 Performance analysis

In this section, the performance of the proposed scheme is analyzed and compared with the two recent authentication schemes [13, 15] for access control mobile pay-TV systems.

Compared with the computation cost of elliptic curve scale multiplication operation and bilinear pairing operation, the computation cost of symmetric encryption/decryption algorithm operation, hash function operation and modular multiplication operation could be ignored. Therefore, we just consider point multiplication operation and bilinear pairing operation in the comparison. Let m, T_e and T_s denote the number of request, the running time of a bilinear pairing operation and the running time of an elliptic curve scale multiplication operation separately. Many implementations about operations related to the bilinear pairing were reported in the last several years [25]. According to those results, the running time of a bilinear pairing operation is about three times more than that of an elliptic curve scale multiplication operation. The computation cost comparison is listed in Table 1.

In order to get the same security level of 1024-bit RSA algorithm, we use 160-bit elliptic curve cryptography. Then, the length of an elliptic curve point in G_1 is 320 bits. Let the length of the user's identity, the service identity number, the output of hash function and the length of an element in G_2 be 32 bits, 32 bits, 160 bits and 160 bits. The login request message in the issue phase of the proposed scheme is $\{E_i, \Lambda_i\}$, where $E_i = k_iP$, $X_i = k_iA_H$, $C_i = h_3P_i + k_iQ_H$ and $h_3 = H_3(A_i, E_i, X_i, ID_i, R_t, T_i)$, $\Lambda_i = E_{X_i}(ID_i, R_t, C_i, T_i)$. Then, the length of the message is 320+32+32+320+32=736 bits. The response message in the issue phase of the proposed scheme is $\{W_{IG}, Y_{IG}, Q_{IG}, \theta, T_H\}$, where $Y_{IG} = \sum_{i=1}^{m} Y_i$, $Q_{IG} = \sum_{i=1}^{m} Q_i$, $\lambda_k = H_2(R_t, (Y_{IG} + Z_H))$, $\theta = e(Y_{IG}, Q_{IG})\lambda_k$ and $W_{IG} = xH_1(Y_{IG}, Q_{IG}, \theta, T_H) + Y_{IG}$ and $Y_i = xQ_i, i = 1, \ldots, m$. Then, the length of the message is 320+320+320+160+32=1152 bits. Therefore, the communication cost in the issue phase of the proposed scheme is (736m+1152) bits. The communication cost comparison is listed in Table 2.

From Tables 1 and 2, we know that the proposed scheme has better performance than the two latest authentication schemes [13, 15]. Moreover, both of the two schemes are vulnerable to the impersonation attack and cannot provide user anonymity. The proposed scheme not only overcomes those weaknesses but also has better performance. Therefore, the proposed authentication scheme is more suitable for access control in mobile pay-TV systems.

7 Conclusion

In this paper, we analyzed the security of Wang and Qin's authentication scheme for access control in mobile pay-TV systems. We have shown that their scheme is vulnerable to the impersonation attack and cannot provide user anonymity. To address the weaknesses in the existing scheme, We proposed the new one-to-many authentication scheme for access control in mobile pay-TV systems and demonstrated that it is provable secure in the random oracle. Performance analysis results show that the proposed scheme performs better than the existing schemes in terms of computation cost and communication cost.

Acknowledgements The work of D. He was supported in part by the National Natural Science Foundation of China (Grant Nos. 61373169, 61572379, 61501333), National High Technology Research and Development Program of China (863 Program) (Grant No. 2015AA016004), Fujian Provincial Key Laboratory of Network Security and Cryptology Research Fund through Fujian Normal University (Grant No. 15011), and Natural Science Foundation of Hubei Province of China (Grant No. 2015CFB257). The work of J.-H. Lee was supported by Basic Science Research Program and Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning (Grant Nos. NRF-2014R1A1A1006770, NRF-2014M3C4A7030648).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Shirazi H, Cosmas J, Cutts D. A cooperative cellular and broadcast conditional access system for pay-TV systems. IEEE Trans Broadcast, 2011, 56: 44–56
2 Diaz-Sanchez D, Marin A, Almenarez F, et al. Sharing conditional access modules through the home networks for pay TV access. IEEE Trans Consum Electron, 2009, 55: 88–96
3 ITU-R. Conditional-Access Broadcasting System. BT.810. https://www.itu.int/rec/R-REC-BT.810/en. 1992
4 Huang Y, Shish S, Ho F, et al. Efficient key distribution schemes for secure media delivery in pay-TV systems. IEEE Trans Multimedia, 2004, 6: 760–769
5 Wang S, Laih C. Efficient key distribution for access control in pay-TV systems. IEEE Trans Multimedia, 2008, 10: 480–492
6 Sun H, Chen C, Shieh C. Flexible-pay-per-channel: a new model for content access control in pay-TV broadcasting systems. IEEE Trans Multimedia, 2008, 10: 1109–1120
7 Zhu W. A cost-efficient secure multimedia proxy system. IEEE Trans Multimedia, 2008, 10: 1214–1220
8 Digital Video Broadcasting (DVB). IP Datacast over DVB-H: Service Purchase and Protection. ETSI TS 102 474 v1.1.1 Std. https://www.etsi.org/deliver/etsi_ts/102400_102499/102474/01.02.01_60/ts_102474v010201p.pdf. 2007
9 Lee N, Chang C, Lin C, et al. Privacy and non-repudiation on pay-TV systems. IEEE Trans Consum Electron, 2000, 46: 20–27
10 Song R, Korba L. Pay-TV system with strong privacy and nonrepudiation protection. IEEE Trans Consum Electron, 2003, 49: 408–413
11 Yeung S, Lui J, Yau D. A multikey secure multimedia proxy using asymmetric reversible parametric sequences: theory, design, and implementation. IEEE Trans Multimedia, 2005, 7: 330–338
12 Roh D, Jung S. An authentication scheme for consumer electronic devices accessing mobile IPTV service from home networks. In: Proceedings of the 29th International Conference on Consumer Electronics, Las Vegas, 2011. 717–718
13 Sun S, Leu M. An efficient authentication scheme for access control in mobile pay-TV systems. IEEE Trans Multimedia, 2009, 11: 947–959
14 Koblitz N. Elliptic curve cryptosystems. Math Comput, 1987, 48: 203–209
15 Wang H, Qin B. Improved one-to-many authentication scheme for access control in pay-TV systems. IET Inform Secur, 2012, 6: 281–290
16 Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attacks. In: Advances in Cryptology-EUROCRYPT. Berlin: Springer, 2000. 139–155
17 Cha J, Cheon J. An identity-based signature from gap diffie-Hellman groups. In: Proceedings of International Conference on Practice and Theory in Public-Key Cryptography, Miami, 2003. 18–30

18 Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures. J Cryptol, 2000, 13: 361–396
19 Ren Y, Shen J, Wang J, et al. Mutual verifiable provable data auditing in public cloud storage. J Internet Techno, 2015, 16: 317–323
20 He D, Kumar N, Chilamkurti N. A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. Inf Sci, 2015, 321: 263–277
21 He D, Zeadally S. Authentication protocol for ambient assisted living system. IEEE Commun Mag, 2015, 35: 71–77
22 Guo P, Wang J, Li B, et al. A variable threshold-value authentication architecture for wireless mesh networks. J Internet Techno, 2014, 15: 929–936
23 Shen J, Tan H, Wang J, et al. A novel routing protocol providing good transmission reliability in underwater sensor networks. J Internet Techno, 2015, 16: 171–178
24 He D, Zhang Y, Chen J. Cryptanalysis and improvement of an anonymous authentication protocol for wireless access networks. Wirel Pers Commun, 2014, 74: 229–243
25 Scott M, Costigan N, Abdulwaha W. Implementing cryptographic pairings on smartcards. In: Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Yokohama, 2006. 134–147