Journal of Network and Computer Applications 34 (2011) 1131–1137

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

An efficient anonymous authentication protocol for mobile pay-TV

Tien-Ho Chen *, Yen-Chiu Chen, Wei-Kuan Shih, Hsin-Wen Wei

Department of Computer Science, National Tsing Hua University, No. 101, Kuang Fu Road, Section 2, 300 HsingChu, Taiwan, ROC

A R T I C L E I N F O

Article history:
Received 31 May 2010
Received in revised form
23 September 2010
Accepted 18 November 2010
Available online 26 November 2010

Keywords:
Mobile pay-TV
Authentication
ECC
Smart card
Dynamic ID
STB

A B S T R A C T

In terms of convenience requirements, mobility has been one of the most important services for pay-TV systems. In 2009, Yang and Chang proposed an authentication protocol for mobile devices using elliptic curves cryptography (ECC) and claimed that their mechanism is secure and efficient using in mobile pay-TV systems. In this paper, we demonstrate that their protocol still is insecure for authentication without password protection and performs inefficiently. Therefore, we offer an anonymous authentication protocol (AAP) to solve the performance issue and insecure risks. In addition, we present an analysis of our protocol to show that our protocol suits better for applications with higher security requirements and low power-consuming devices.

1. Introduction

With the integration of wireless communication and pay-TV, mobile broadcast TV technologies have advanced noticeably in recent years (Allamandri et al., 2007; ETSI, 2004, 2005; Fabio et al., 2007; Faria et al., 2006; Gallery and Tomlinson, 2005; Gardikis et al., 2008; Kornfeld and May, 2007; Lee et al., 2000; Ollikainen, 2006; Song and Korba, 2003; Sun and Leu, 2009). Especially, how to promise authorized subscribers a secure access and keep unauthorized subscribers from illegitimate accesses in mobile broadcast TV services has become an important issue. Typically, Conditional Access System (CAS) supports this mechanism. There are two main parts in CAS: (1) head end system (HES) and (2) numerous receivers. The structure of CAS is shown in Fig. 1 and the statements are described as follows:

- *Head end system (HES)*: HES is a system sending broadcast TV services to receivers.
- *Receiver*: A receiver is a subscriber device with a CAS module used for access control.
- *SAS/SMS*: Subscriber Authorization System and Subscriber Management System are subsystems responsible for subscriber authorization and management; its works include key management, user authentication, entitlement messages delivery, subscriber information management and rights management.
- *Encrypter/decrypter*: Encrypter is a component for enciphering Control Word (CW), keys, or sensitive information, and Decrypter employs the reverse engineering of encrypter.
- *Multiplexer (MUX)/Demultiplexer (DEMUX)*: MUX is a component for multiplexing A/V, data or IP into MPEG-2 transport stream, and DEMUX employs the reverse engineering of MUX.
- *Scrambler/Descrambler*: Scrambler is a component for signal scrambling, and descrambler employs the reverse engineering of Scrambler.
- *Transmitter (TX)/Receiving module (RX):* TX is a subsystem for signal transmission, and RX is a subsystem for signal receiving.
- *ECM/EMM*: ECM and EMM are defined by DVB (ETSI, 2004) as two conditional access messages, namely Entitlement Control Message (ECM) and Entitlement Management Message.

Pay-TV systems supply receivers with many different services. The CAS generally performs these services in two modes, namely broadcast and interactive mode. In the broadcast mode, A HES broadcasts the service messages via a SAS/SMS, Encrypter, MUX, Scrambler and Transmitter to subscriber devices periodically, and the receiver listens to the messages constantly. In the interactive mode, a subscriber's receiver must be authenticated first to obtain the entitlement service. While he/she wants to obtain a service, his/her device sends a subscription and authentication messages to a HES. After the authentication and subscription being validated, HES delivers the service messages which include rights codes and authentication messages via a SAS/SMS, Encrypter, MUX, Scrambler and Transmitter to this subscriber device. Then, the subscriber can use his/her private key, authentication key and entitlement data to obtain the service.

* Corresponding author. Tel.: +886 35715131x42808; fax: +886 35723694.
E-mail addresses: riverchen@rtlab.cs.nthu.edu.tw (T.-H. Chen), ycchen@rtlab.cs.nthu.edu.tw (Y.-C. Chen), wshih@rtlab.cs.nthu.edu.tw (W.-K. Shih), hwwei@iis.sincia.edu.tw (H.-W. Wei).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.11.005

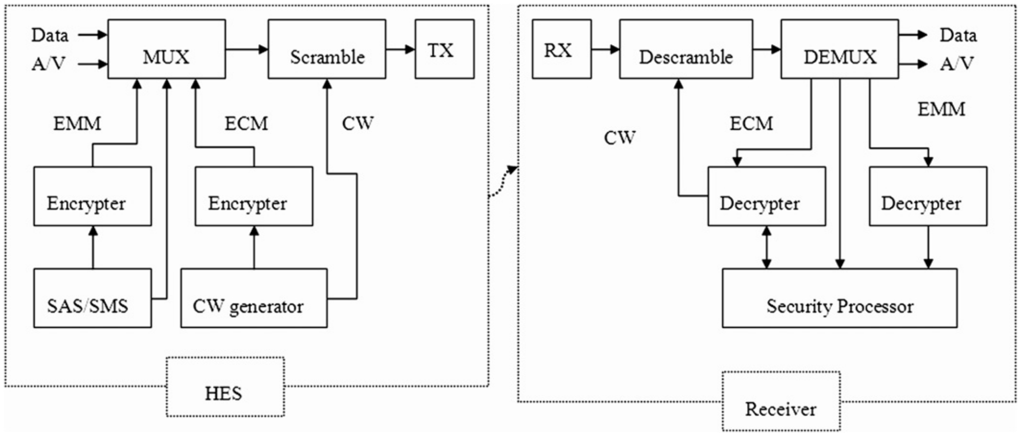

Figure 1. The structure of CAS in general mobile pay-TV system.

To provide secured access services of pay-TV systems, several studies have been proposed. For instance Lee et al. (2000) proposed a privacy and nonrepudiation authentication protocol for pay-TV systems by employing a digital signature in 2000. Song and Korba (2003) proposed an e-ticket authentication protocol for pay-TV systems in 2003. However, Lee et al.'s protocol has been found that their protocol protects only the subscriber's privacy, but not HES. Furthermore, Lee et al.'s protocol performed inefficient using digital signature techniques (Song and Korba, 2003). Later Scott et al. (2006), Sun et al. (2008) and Sun and Leu (2009) pointed out that Song and Korba's protocol which employs authentication using e-ticket which is based on RSA (Rivest et al., 1978) for public key cryptosystem is inefficient and is unsuitable for mobile pay-TV systems. Later, Yang and Chang (2009) proposed an authentication protocol using elliptic curves cryptography (ECC) for access control in 2009. They claimed that their mechanism is secure and efficient using in mobile pay-TV systems.

However, Yang and Chang's protocol is still insecure for authentication without password protection. Furthermore, ECC-based methods (Gupta et al., 2004b; Gura et al., 2004; Han et al., 2002; Liao and Wang, 2010; Scott et al., 2006) still needs a cubic polynomial elliptic curve cryptography computation cost for calculating private and public keys.

According to the above descriptions, we summarize the requirements of the authentication mechanism for MPTV, which a protocol should have the following.

1. *Efficiency*: In mobile pay-TV systems, low power consumption for a mobile device is one of the most important issues for mobile device designing. A viewer hopes that he/she can obtain his/her service anywhere for a long time. Thus, the power consumption management is significant for extending the executing time of the mobile device. Reduction of computation cost can reach the goal of low power consumption for a mobile device.
2. *Anonymity*: The anonymous authentication of mobile pay-TV is an important security issue because it can protect the privacy of a user's information and identification.
3. *Mutual authentication*: To protect the security of users and servers of the service provider, an authentication mechanism should promise the security of users and servers in an insecure environment. A protocol designed for mobile pay-TV should provide a mutual authentication for the user and server of the service provider to guarantee that all verified objects are secured.

In this paper, we offer an efficient mutual authentication mechanism to solve the heavy computation load and resist the insecure risks. In addition, our protocol provides the properties of dynamic ID based authentication for anonymity and hand-off authentication using smart cards.

The remainder of this paper is organized as follows. Section 2 reviews the related works. Section 3 presents a cryptanalysis of Yang and Chang'**s** authentication mechanism. Section 4 presents a novel anonymous authentication protocol for mobile pay-TV systems. The security and performance analysis are in Section 5. Finally, the conclusion is made in Section 6.

2. Related works

2.1. An overview of mobile pay-TV systems

Pay-TV systems provide a viewer demand for a range of services in the competitive prices and freedom of choice to switch to any program or service via wire or wireless environment. Convenience is one of the most important factors. For instance, a viewer hopes that he/she can obtain his/her request anytime and anywhere. Hence, mobility service is essential for pay-TV systems. Authentication is a mechanism which protects a consumer using system's service securely in an insecure environment, e.g., mobile pay-TV systems. Several studies have proposed methods for the mobile pay-TV system's authentication. In 2009, Yang and Chang proposed an authentication protocol for the mobile device and remote server authentication using ECC. We explain as follows.

2.2. ECC based authentication protocol

Yang and Chang proposed an ECC based authentication protocol for mobile devices. We state the elliptic curve cryptography based authentication protocol as follows.

2.2.1. ECC protocol

An elliptic curve is a cubic equation of the form

$$E:\ y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$$

where a_1,a_2,a_3,a_4 and a_6 are real number. ECC employs elliptic curve characteristic to complete key exchange. ECC defines a singular elliptic curve E over F_p to be an equation of form, where $E: y^2=(x^3+ax+b) \bmod p$ with $a,b \in F_P$ fulfilling $(4a^3+27b) \bmod p \neq 0$ and $E(F_P)=\{(x,y): x,y \in F_P, y^2=x^3+ax+b\} \cup \{\ \Theta\ \}$. We define $E(F_P)$ as the finite set of points in the elliptic group and Θ as the infinite one. The points of $E(F_P)$ must fulfill the elliptic curve addition algorithm. We sketch the summary (Girault, 1991; Koblitz, 1987;

Menezes et al., 1997; Miller, 1986; Petersen et al., 1997) of ECC as follows:

i. Considering the elliptic curve addition algorithm, a value of n is a very large prime number such that $n \times P = \Theta$. We select a nonce n_E ($n_E \in Z_q^*$) where $n_E < n$ and compute Q as $Q = n_E \times P$. The elliptic curve discrete logarithm problem (ECDLP) is hard to determine n_E given P and Q.
ii. The user U_A selects a private key r_A ($r_A \in Z_q^*, r_A < n$) and computes the public key Q_A as $Q_A = r_A \times P$. U_A sends Q_A to the user U_B.
iii. U_B selects a private key r_B ($r_B \in Z_q^*$, $r_B < n$) and computes the public key Q_B as $Q_B = r_B \times P$.
U_B sends Q_B to U_A.
iv. U_A can compute key $K_A = r_A \times Q_B$ and U_B can compute key $K_B = r_B \times Q_A$ where $K_B = K_A$;
For example, consider the following elliptic curve:

$$y^2 = x^3 + ax + b (\mathrm{mod}\, p) \quad (1)$$

$$y^2 = x^3 - 4 \quad (2)$$

That is $a=0$, $b=-4$ and $p=211$. The elliptic curve group generated by above elliptic curve is then
$E_P(a,b) = E_{211}(0,-4)$. U_A can compute key $K_A = r_A \times Q_B$ and U_B can compute key $K_B = r_B \times Q_A$ as follows:

i. Let the generator point $E(F_P) = (2, 2)$ (for $1 \le P \le 211$).
ii. U_A selects a private key $r_A = 203$ and computes the public key Q_A as
$Q_A = r_A \times P = (203) \times (2,2) = (130,203)$
U_A sends Q_A to the user U_B.
iii. U_B selects a private key $r_B = 121$ and computes the public key Q_B as
$Q_B = r_B \times P = (121)(2,2) = (115,48)$
U_B sends Q_B to the user U_A.
iv. $K_A = r_A \times Q_B = (121) \times (130,203) = (161,169)$
$K_B = r_B \times Q_A = (203) \times (115,48) = (161,169)$
The elliptic curve key has been built up.

2.2.2. Yang and Chang's authentication protocol

Yang and Chang'**s** authentication mechanism consists of three phases namely: initialization, user registration and mutual authentication with key agreement phase. We describe as follows.

A. Initialization phase

The remote server S performs the following computations:
(1) Chooses an elliptic curve equation $E_P(a, b)$ with order n.
(2) Selects a base point P with the order n over $E_P(a, b)$, where n is a large number for the security considerations. And then, S computes its private/public key pair (q_s, Q_s) where $Q_s = q_s P$.
(3) Chooses three one-way hash functions $H_1(.)$, $H_2(.)$ and $H_3(.)$, where $H_1(.)$: $\{0, 1\} \rightarrow G_p$, $H_2(.)$:$\{0,1\} \rightarrow Z_P^*$ and $H_3(.)$:$\{0,1\} \rightarrow Z_P^*$ (G_p denotes a cyclic addition group of P).
(4) Stores q_s as a private key and publishes message[$E_P(a, b)$, P, $H_1(.)$, $H_2(.)$, $H_3(.)$,Q_s].

B. User registration phase

(1) The user U_A sends his identity ID_A to the server S.
(2) S computes $K_{IDA} = q_S H_1(ID_A) \in G_p$, where K_{IDA} is U_A's authentication key.
(3) S sends K_{IDA} to U_A over a secure channel.
(4) After receiving K_{IDA}, U_A checks whether $K_{IDA}P = Q_S H_1(ID_A)$. If it holds, U_A keeps K_{IDA} as a private key.

C. Mutual authentication with key agreement phase

(1) U_A chooses a random point $R_A = (x_A, y_A) \in E_P(a, b)$, where x_A and y_A are x and y coordinating point of R_A.
(2) U_A computes $t_1 = H_2(T_1)$, $M_A = R_A + t_1 K_{IDA}$ and $\bar{R_A} = x_A P$ at the timestamp T_1.
(3) U_A sends message $m_1 = [T_1, ID_A, M_A, \bar{R_A}]$ to S.
(4) After receiving m_1, S performs the following computations to obtain $Q_{IDA} = (x_Q, y_Q)$ and $R'_A = (x'_A, y'_A)$ of U_A.
- $Q_{IDA} = \mathrm{H1(IDA)}$
- $t_1 = H_2(T_1)$
- $R'_A = M_A - q_s t_1 Q_{IDA}$

(5) S verifies whether $\overline{R_A} = x'_A P$. If it holds, U_A is authenticated by S.
(6) S chooses a random point $R_S = (x_S, y_S) \in E_P(a\ b)$.
(7) S computes $t_2 = H_2(T_2)$, $M_S = R_S + t_2 q_S Q_{IDA}$, session key $k = H_3(x_Q, x_A, x_S)$ and $M_k = (k + x_S)$ at the timestamp T_2.
(8) S sends message $m_2 = [T_2, M_S, M_k]$to U_A.
(9) After receiving m_2, U_A performs the following computations to obtain $Q_{IDA} = (x_Q, y_Q)$ and $R'_S = (x'_S, y'_S)$ of S.
- $Q_{IDA} = \mathrm{H_1(ID_A)}$
- $t_2 = H_2(T_2)$
- $R'_S = M_S - t_2 K_{IDA}$

(10) U_A computes $k' = H_3(x_Q, x_A, x'_S)$ and $M'_k = (k' + x'_S) \cdot P$ to verify whether $M'_k = M_k$. If it holds, S is authenticated by U_A.
(11) U_A and S employ k as a session key for communication.

3. Cryptanalysis of Yang and Chang's authentication protocol

Yang and Chang's authentication method provides a session key agreement for the users and server but there is no password protection in their protocol. Password-based authentication protocols are widely adopted for logging into the remote servers. They can provide authentication between the client and the server to ensure the legality of the user over an open network. Many schemes in this area have been proposed such as Chen et al. (2010), Hsiang et al. (2009), Hsiang and Shih (2009b), Khan et al. (in press), Wang et al. (2009), Yoon et al. (2004) for the client–servers architecture and Hsiang and Shih (2009a), Lin et al. (2003) for multi-servers architecture. Without password protection, Yang and Chang's protocol exposes the user and system to the risk of insider attack, impersonation attack, etc. We explain as follows:

3.1. Insider attack

If the privileged insider of the authentication server has the knowledge of the user U_A's authentication key K_{IDA}, he/she may try to impersonate the user U_A to access the authentication server. Assuming an attacker obtains U_A's authentication key K_{IDA} and ID_A, he/she can impersonate U_A to access the authentication server just selecting a random point $R_{A'} = (x_{A'}, y_{A'}) \in E_P(a, b)$ and performing the following steps of Yang and Chang's protocol in the mutual authentication with key agreement phase. The whole procedure will succeed without any obstruction because the attacker employs the authentication process using U_A's authentication key K_{IDA} and ID_A without the protection of password.

3.2. Impersonation attack:

If an attacker has a legitimate user U_A's ID_A, he/she just re-register ID_A to the server to obtain U_A's authentication key K_{IDA}. Then, he/she can impersonate U_A to access the authentication server without any obstruction.

Furthermore, Yang and Chang's ECC-based authentication method usually requires ECC metric computation cost to encrypt/decrypt the cipher-text, which includes elliptic curve point mapping with cubic polynomial equation $E: y^2 = (x^3 + ax + b)$, point addition and point multiplication in ECC. It is not suitable for the restricted resource of mobile pay-TV systems. According to Gupta et al. (2004a), Gura et al. (2004), Han et al. (2002) and Scott et al. (2006) studies, the polynomial computation cost for private key and public key with elliptic curve cryptography is considerably higher than the hash function.

In this paper, we propose a novel more efficient secret authentication mechanism with hash for mobile devices, for instance, the mobile TV using in pay-TV systems.

4. A novel anonymous authentication protocol (AAP) for MPTV

There are four phases in our authentication method which includes initialization, issue, subscription and hand-off phase. A user U_i can register to an MPTV service provider's subscriber database server (*DBS*) of HES via *SAS/SMS*. *DBS* saves U_i's identity ID_i for service at initialization phase. An MPTV service provider can authenticate a legitimate user by broadcasting a service code R_t and authenticate a legitimate user's rights by mutual authenticating a verifying code θ and service rights code γ at the issue and subscription phase.

When a mobile device (MS) moves to a new coverage area, HES of the previous area cannot provide services anymore to that device. As a consequence, a hand-off occurs, and the mobile device (MS) needs to perform re-authentication. The proposed protocol is described as follows.

4.1. Initialization phase

This phase is invoked whenever user U_i registers to the subscribers' database server (*DBS*) of HES via *SAS/SMS* and the *DBS* saves U_i's identity ID_i. Many pay-TV systems can provide the services via wire, for instance, set-top-box (STB) with wire (Shirazi et al., 2010) or wireless communication, this paper propose the initialization phase using STB as a secure channel which usually is provided or assigned a STB ID by the pay-TV system providers for registration and payment. The following steps are performed to complete this phase:

(1) U_i chooses his/her ID_i and pw_i and generates a random number b for calculating $PWB=h(pw_i \oplus b)$. Then, U_i submits ID_i and PWB to the pay-TV system server S.
(2) S checks the database whether his/her ID_i is already in the database or not. If ID_i is already in the database, S checks whether U_i performs a re-registration or not. If U_i performs a re-registration then S sets ID_i's registration number $N=N+1$ and updates ID_i and N in the database otherwise S suggests U_i to choose another ID_i. If ID_i is not in the database then S sets $N=0$ and stores values of ID_i and N in the database.
(3) S calculates $K=h(ID_i \oplus PWB)$, $Q=h(UD||x) \oplus PWB$ and $R=h(PWB||ID_i) \oplus h(y)$. (Here $UD=h(ID_i||N)$, y is the secret key of the remote server stored in the hash function and x is the secret key of S.)
(4) S issues a smart card containing $[K,R,Q]$to U_i over a secure channel.
(5) U_i stores the random number b on the smart card. Such that the smart card contains $[K,R,Q,b]$.

4.2. Issue phase

Assume that U_i's MS_i (MS_i denotes a mobile subscriber device of U_i) asks a service R_t and the kth *HES* performs this authentication process of issue phase for U_i to obtain a right code θ_i. The statements are described as follows:

(1) U_i entries his/her ID_i and PW_i in order to login for obtaining the service, MS_i performs the following computations:
  - Calculates $PWB=h(pw_i \oplus b)$ and $h(ID_i \oplus PWB)$ to verify whether $K=h(ID_i \oplus PWB)$. If it does not hold, MS_i terminates the request.
  - Calculates $P=Q \oplus PWB$ and $h(y)=h(PWB||ID_i) \oplus R$.
  - Generates a random number n_i and calculates $R_i=R_t \oplus h(y||n_i)$, $CID_i=ID_i \oplus h(y||T_1||n_i)$ and $C_i=h(P||CID_i||T_1||n_i)$. Here T_1 is the current timestamp.
  - Sends the message $m=[R_i,C_i,CID_i,T_1,n_i]$ to *HES*.
(2) *HES* receives the message at the timestamp T_2 and performs the following computations:
  - Checks the validity of $(T_2-T_1) \leq \Delta T$ (here ΔT denotes the expected valid time interval for transmission delay). If it does not hold, *HES* terminates the request.
  - Calculates $ID_i=CID_i \oplus h(y||T_1||n_i)$ and verifies if ID_i is a valid user's identity. If it does not hold, *HES* terminates the login request, otherwise *HES* checks the value of N in the database and calculates $P'=h(UD||x)=h(h(ID_i||N)||x)$.
  - Calculates $C_i'=h(P'||CID_i||T_1||n_i)$ and checks whether $C_i'=C_i$. If they are equal, *HES* accepts U_i 's request of authentication.
  - Calculates $R_t=R_i \oplus h(y||n_i)$.
  - Then, *HES* chooses a token θ_i for U_i and stores into *DBS*, calculates $D_i=h(P'||CID_i||T_2||n_i)$ and $E_i=\theta_i \oplus h(P'||T_2||n_i)$.
  - Broadcasts the mutual authentication message $m_2=[D_i, E_i, T_2]$.
(3) After receiving message m_2 at the time T_3, U_i checks the validity of $(T_3-T_2) \leq \Delta T$. If it does not hold, U_i terminates the request. Otherwise, U_i executes the following operations to authenticate *HES*.
  - Calculates $D_i'=h(P||CID_i||T_2||n_i)$ and checks whether $D_i'=D_i$. If they are equal, U_i accepts *HES*'s request of mutual authentication.
  - U_i calculates the certified token $\theta_i=E_i \oplus h(P||T_2||n_i)$ as the authentication session key to get service of the pay-TV system.

4.3. Subscription phase

After U_i obtaining a right code θ_i, U_i's MS_i asks a service R_t using θ_i and the kth *HES* performs this authentication process. The statements are described as follows:

(4) U_i entries his/her ID_i and PW_i in order to login for obtain the service, MS_i performs the following computations:
  - Calculates $PWB=h(pw_i \oplus b)$ and $h(ID_i \oplus PWB)$ to verify whether $K=h(ID_i \oplus PWB)$. If it does not hold, MS_i terminates the request.
  - Calculates $P=Q \oplus PWB$ and $h(y)=h(PWB||ID_i) \oplus R$.
  - Generates a random number n_i and calculates $R_i=\theta_i \oplus h(y||n_i)$, $CID_i=ID_i \oplus h(y||T_1||n_i)$ and $C_i=h(P||CID_i||T_1||n_i)$. Here T_1 is the current timestamp.
  - Sends the message $m=[R_i,C_i,CID_i,T_1,n_i]$to *HES*.
(5) *HES* receives the message at the timestamp T_2 and performs the following computations:
  - Checks the validity of $(T_2-T_1) \leq \Delta T$ (here ΔT denotes the expected valid time interval for transmission delay). If it does not hold, *HES* terminates the request.
  - Calculates $ID_i=CID_i \oplus h(y||T_1||n_i)$ and verifies if ID_i is a valid user's identity. If it does not hold, *HES* terminates the login request, otherwise *HES* checks the value of N in the database and calculates $P'=h(UD||x)=h(h(ID_i||N)||x)$.
  - Calculates $C_i'=h(P'||CID_i||T_1||n_i)$ and checks whether $C_i'=C_i$. If they are equal, *HES* accepts U_i 's request of authentication.
  - Calculates $\theta_i=R_i \oplus h(y||n_i)$
  - Then, *HES* chooses a token γi for U_i, and calculates $D_i=h(P'||CID_i||T_2||n_i)$ and $E_i=\gamma_i \oplus h(P'||T_2||n_i)$.
  - Broadcasts the mutual authentication message $m_2=[D_i, E_i, T_2]$.
(6) After receiving message m_2 at the time T_3, U_i checks the validity of $(T_3-T_2) \leq \Delta T$. If it does not hold, U_i terminates the

request. Otherwise, U_i executes the following operations to authenticate *HES*.

- Calculates $D_i' = h(P||CID_i||T_2||n_i)$ and checks whether $D_i' = D_i$. If they are equal, U_i accepts *HES*'s request of mutual authentication.
- U_i calculates the certified token $\gamma_i = E_i \oplus h(P||T_2||n_i)$ as the authentication session key to get service of the pay-TV system.

4.4. Hand-off phase

When MS_i moves to a new coverage area that older HES cannot support such that a hand-off occurs, the MS_i needs to perform re-authentication without re-login. The statements are described as follows:

(1) MS_i performs the following computations:
- Generates a new random number n_i and calculates $Z_i = \theta_i \oplus h(y||n_i)$, $CID_i = ID_i \oplus h(y||T_1||n_i)$ and $C_i = h(P||CID_i||n_i)$. Here T_1 is the current timestamp.
- Sends the message $m = [Z_i, C_i, CID_i, T_1, n_i]$ to *HES*.

(2) *HES* receives the messages at the timestamp T_2 and performs the following computations:
- Checks the validity of $(T_2 - T_1) \le \Delta T$. If it does not hold, *HES* terminates the request.
- Calculates $ID_i = CID_i \oplus h(y||T_1||n_i)$ and verifies if ID_i is a valid user's identity. If it does not hold, *HES* terminates the login request, otherwise *HES* checks the value of N in the database and calculates $P' = h(UD||x) = h(h(ID_i||N)||x)$.
- Calculates $C_i' = h(P'||CID_i||T_1||n_i)$ and checks whether $C_i' = C_i$. If they are equal, *HES* accepts U_i's request of authentication.
- Calculates $\theta_i = Z_i \oplus h(y||n_i)$ for verifying U_i's request of service.
- Then, *HES* chooses an authentication session key γ_i, calculates $D_i = h(P'||CID_i||T_2||n_i)$ and $F_i = \gamma_i \oplus h(P'||T_2||n_i)$.
- Broadcasts the mutual authentication message $m_2 = [D_i, F_i, T_2]$.

(3) After receiving message m_2 at the time T_3, U_i checks the validity of $(T_3 - T_2) \le \Delta T$. If it does not hold, U_i terminates the request. Otherwise, U_i executes the following operations to authenticate *HES*.
- Calculates $D_i' = h(P||CID_i||T_2||n_i)$ and checks whether $D_i' = D_i$. If they are equal, U_i accepts *HES*'s request of mutual authentication.
- U_i calculates the authentication session key $\gamma_i = F_i \oplus h(P||T_2||n_i)$ to obtain new *HES*'s service.

5. Security and performance analysis

In this section, we discuss the security of our proposed protocol.

5.1. Security analysis

Several studies have discussed the security issues of remote user authentication. We make a summary of the security requests from the standards and studies (Camenisch and Lysyanskaya, 2003; Chen et al., in press; ETSI, 2004, 2005; Gardikis et al., 2008; Yang et al., 2010; Hsiang and Shih, 2009a, b; Khan et al., in press; Kornfeld and May, 2007; Lee et al., 2000; Pequeno et al., 2010; Rocha et al., 2010; Tamura and Miyaji, 2003; Chen and Shih, 2010; Yoon et al., 2004) and provide a theorem for our protocol to certificate the security requests.

Lemma 1. *Our protocol, shown in Section 4, provides a resistance to replay attack.*

Proof. If an attacker wants to reply the messages which have been eavesdropped from middle way to attack the pay-TV system, the result is clear that he/she cannot succeed because there is the random nonce numbers n_i in each long-term secret cipher and n_i is different in each authentication session. Furthermore, if the attacker replays the message to impersonate the user U_i, the server *HES* will check the expected valid time interval for transmission delay ΔT. Thus, the replay attack cannot succeed. □

Lemma 2. *Our protocol, shown in Section 4, provides a resistance to offline password guessing attack.*

Proof. There are two variables pw_i and b in password protection. A legitimate user U_i uses $PWB = h(pw_i \oplus b)$ to register the authentication server *HES* in the registration phase, and calculates *PWB* for the authentication and password change phase. Our protocol can resist offline guessing attack. □

Lemma 3. *Our protocol, shown in Section 4, provides a resistance to impersonation attack.*

Proof. For successfully complete the impersonation attack, an attacker must know U_i's password to pass the verification in login phase and interpret verification message correctly for mutual authentication. The attacker cannot masquerade as a legitimate user U_i even if he/she is a legitimate user, he/she cannot masquerade as U_i without U_i's password or forgery the same messages sending to the authentication server in the issue, subscription and hand-off phase. □

Lemma 4. *Our protocol, shown in Section 4, provides a resistance to forgery attack.*

Proof. When an attacker try to forge the valid message codes, for instance, C_i, CID_i, D_i, E_i, etc., he/she must know the secret key y within the hash function and the secret key x, θ_i and γ_i which are selected by *HES* to construct all the transaction messages. It is impossible for any attacker to complete the mission. Thus, our protocol resists forgery attack. □

Lemma 5. *Our protocol, shown in Section 4, provides a resistance to man-in-the middle attack.*

Proof. Our proposed protocol provides the cipher message codes, for instance, C_i, CID_i, D_i, E_i, etc., which includes the timestamp, random number, the secret code x and y, which makes our protocol achieving mutual authentication and securing against the attacker to cheat the user or the server by eavesdropping the messages in the middle to forge or replay the messages. □

Lemma 6. *Our protocol, shown in Section 4, provides a resistance to insider attack.*

Proof. It is common practice that many users apply same passwords to access different applications for their convenience. If the privileged insider of HES has the knowledge of a legitimate user's (U_i) password, he/she may try to impersonate the user U_i to access other applications. □

Our proposed protocol can resist an insider attack. The details are described as follows:

1. Assume that a privileged insider Λ of HES has the knowledge of a legitimate user's (U_i) password pw_i and ID_i, and tries to login for obtaining a service.
2. Λ employs a login procedure using pw_i and a random number b'.
3. Λ calculates $PWB' = h(pw_i \oplus b')$ and $h(ID_i \oplus PWB')$ to verify whether $K = h(ID_i \oplus PWB')$ (where U_i's parameter $K = h(ID_i \oplus PWB)$ has been stored in his/her smart card).
4. Λ's login procedure cannot pass the verification of $K = h(ID_i \oplus PWB')$ because he/she does not has the knowledge of U_i's

Table 1
The communication cost of the related protocols.

Communication cost of authentication	Ours	Yang–Chang	Song–Korba	Lee et al.
Issue and subscription phases	$16t_h$	$8t_h$+$2\hat{e}$+6 PM+2 PA	$8\hat{E}$	$9\hat{E}$

random number b which U_i stores b in the smart card after he/she has received and verified his/her smart card.
5. There are two parameters to protect our protocol security.

Further, Our proposed protocol provides U_i registers the authority using cipher code $PWB=h(pw_i \oplus b)$ over a secret channel, which avoids an inherent risk of password stolen. Furthermore, in our protocol, U_i's authentication key K_{IDA} is not stored in HES, the privileged insider of HES cannot try to impersonate the user U_i to access the authentication server. Thus, our protocol resists insider attack.

Lemma 7. *Our protocol, shown in Section 4, provides a mutual authentication.*

Proof. Mutual authentication is an important feature for a verification service resisting to server spoofing attack. Our protocol provides a mutual authentication for the user U_i and server *HES*. U_i can authenticate *HES* by means of the cipher message code D_i to check whether $D_i=h(P||CID_i||T_2||n_i)$. Further, HES can authenticate U_i by means of the cipher message code C_i to check whether $C_i=h(P'||CID_i||T_1||n_i)$. Thus, our protocol provides mutual authentication service and resists server spoofing attack. □

Lemma 8. *Our protocol, shown in Section 4, provides an anonymous authentication.*

Proof. An anonymity feature of users is authenticating servers cannot find out anything about a user from a credentials which is encrypted and transferred with or without the identity, except authenticating servers can decrypt a credentials with a secret key or private key which is only generated by verifying organizations. Accordance with Yang et al.'s, Li et al.'s and Tamura et al.'s research (Li et al., 2009; Guomin et al., 2010; Tamura and Miyaji, 2003), the proposed protocol provides a user's anonymous request. A user U_i can send an anonymous identity $CID_i=ID_i \oplus h(y||n_i||T_1)$ to a remote server S for each login request and ID_i is encrypted by the timestamp T_1, random number n_i and secret key y. Therefore, S can only obtain ID_i by means of T_1, n_i and secret key y during the remote server *S's* decryption procedure but an intruder cannot obtain ID_i without secret key y. Furthermore, CID_i varies at each login request because it is encrypted by T_1 and n_i which vary at each login attempt. □

Theorem 1. *Our protocol, shown in Section 4, provides resistance to six kinds of attacking behaviors and two authentication characteristics.*

Proof. The proofs for the six kinds of attacking behaviors are shown in Lemmas 1–6. In addition, the proofs for authentication characteristic are shown in Lemmas 7 and 8. □

5.2. Performance analysis

For comparing performance of communication cost with Yang and Chang's protocol, we define the notation t_h as the hash computation time, $\hat{E}$ as a modular exponentiation, $\hat{e}$ as an elliptic curve (*EC*) computation operation, *PM* as point multiplication and *PA* as point multiplication in ECC for private key and public key computation. According to Yang and Chang's research and Gupta et al. (2004a), Gura et al. (2004), Han et al. (2002), Liao and Wang (2010) and Scott et al. (2006), $\hat{E}$, $\hat{e}$, *PM* and *PA* are considerably higher than t_h.

In this paper, we compare the cost of mutual authentication with key agreement phase which is the major computation of authentication process. In the mutual authentication phase which includes issue and subscription phases, our protocol requires $16t_h$. However, Yang and Chang's protocol needs eight hash functions, two elliptic curve computation operations, six multiplications and four point additions. Song's scheme needs 8 modular exponentiation operations and Lee's scheme needs 9 modular exponentiation operations. The comparison of related protocols is shown in Table 1. Furthermore, in the hand-off phase which is a mutual authentication method, the cost of computation only requires $12t_h$ without re-login operations.

6. Conclusion

In this paper, we have analyzed elliptic curve cryptography based authentication protocol (Yang and Chang's protocol) for mobile pay-TV. Since MPTV needs more efficient methods to perform mutual authentication in an insecure network environment, we use a hash-based mechanism to accomplish the request. The proposed protocol is highly efficient and provides secured mutual authentication. Lastly, it not only inherits the merits of hash-based mechanism but also provides dynamic ID based authentication and hand-off authentication for MPTV with higher security.

References

Allamandri F, Campion S, Centonza A, Chernilov A, Cosmas JP, Duffy A, et al. Service platform for converged interactive broadband broadcast and cellular wireless. IEEE Trans Broadcast 2007;53:200–11.

Camenisch J, Lysyanskaya AA. Signature scheme with efficient protocols. In: Cimato S, Persiano G, Galdi C, editors. Security in communication networks. Berlin, Heidelberg: Springer; 2003. p. 268–89.

Chen T-H, Shih W-K. Robust mutual authentication protocol for wireless sensor networks. ETRI J 2010;32:704–12.

Chen T-H, Hsiang H-C, Shih W-K. Security enhancement on an improvement on two remote user authentication schemes using smart cards. Future Gener Comput Syst, in press. doi:10.1016/j.future.2010.08.007.

Chen T-H, Hsiang H-C, Shih W-K. Security improvement on a remote user authentication scheme using smart cards. In: Proceedings of the information security and assurance (ISA). vol. CCIS 76, 2010. p. 9–16.

ETSI. Digital Video Broadcasting (DVB): transmission system for handheld terminals (DVB-H). ETSI EN 302 304 V111, 2004.

ETSI. Digital Video Broadcasting (DVB): IP datacast over DVB-H: service purchase and protection. ETSI TS 102 474 v111, 2005.

Fabio A, Sebastien C, Angelo C, Alex C, John PC, Annette D, et al. Service platform for converged interactive broadband broadcast and cellular wireless. broadcasting. IEEE Trans 2007;53:200–11.

Faria G, Henriksson JA, Stare E, Talmola P. DVB-H: digital broadcast services to handheld devices. Proc IEEE 2006;94:194–209.

Gallery E, Tomlinson A. Conditional access in mobile systems: securing the application. In: First international conference on distributed frameworks for multimedia applications (DFMA05), 2005.

Gardikis G, Xilouris G, Skianis C, Kourtis A. Broadband multimedia on the move with DVB-H. Multimedia Tools Appl 2008;36:133–44.

Girault M. Self-certified public keys. Lect Notes Comput Sci 1991;547:490–7.

Gupta V, Stebila D, Fung S. Speeding up secure web transactions using elliptic curve cryptography. In: 11th network and distributed systems security symposium, 2004a. p. 231–9.

Gupta V, Stebila D, Fung S, Shantz SC, Gura N, Eberle H. Speeding up secure web transactions using elliptic curve cryptography. In: Proceedings of the 11th network and distributed systems security symposium, 2004b. p. 231–9.

Gura N, Patel A, Wander A, Eberle H, Shantz SC. Comparing elliptic curve cryptography and RSA on 8-bit CPUs. Cryptographic hardware and embedded systems—Ches 2004, proceedings, vol. 3156, 2004. p. 119–32.

Han JH, Kim YJ, Jun SI, Chung KI, Seo CH. S. Implementation of ECC/ECDSA cryptography algorithms based on Java card. In: 22nd international conference on distributed computing systems workshops, 2002. p. 272–6.

Hsiang HC, Chen TH, Shih WK. Security enhancement on an improvement on two remote user authentication scheme using smart cards. Advances in communication and networking lecture notes in computer science. Berlin, Heidelberg: Springer; 2009. p. 65–73.

Hsiang HC, Shih WK. Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. Comput Stand Interfaces 2009a;31:1118–23.

Hsiang HC, Shih WK. Weaknesses and improvements of the Yoon–Ryu–Yoo remote user authentication scheme using smart cards. Comput Commun 2009b;32: 649–52.

Khan MK, Kim S-K, Alghathbar K. Cryptanalysis and security enhancement of a "more efficient and secure dynamic ID-based remote user authentication scheme". Comput Commun, in press, doi:10.1016/j.comcom.2010.02.011.

Koblitz N. Elliptic curve cryptosystems. Math Comput 1987;48:203–9.

Kornfeld M, May G. DVB-H and IP datacast—broadcast to handheld devices. IEEE Trans Broadcast 2007;53:161–70.

Lee N-Y, Chang C-C, Lin C-L, Hwang T. Privacy and non-repudiation on pay-TV systems. IEEE Trans Consumer Electron 2000;46:20–7.

Li J, Li N, Winsborough WH. Automated trust negotiation using cryptographic credentials. ACM Trans Inf Syst Secur 2009;13:1–35.

Liao Y-P, Wang S-S. A new secure password authenticated key agreement scheme for SIP using self-certified public keys on elliptic curves. Comput Commun 2010;33: 372–80.

Lin IC, Hwang MS, Li LH. A new remote user authentication scheme for multi-server architecture. Future Gener Comput Syst 2003;19:13–22.

Menezes A, Oorschot PV, Vanstone S. Handbook of applied cryptography. CRC Press Inc.; 1997.

Miller VS. Use of elliptic curves in cryptography. LNCS, advances in cryptology—CRYPTO '85: proceedings. Berlin, Heidelberg: Springer; 1986. p. 417.

Ollikainen VA. Handover approach to DVB-H services. In: Chengyuan P, editor. 2006 IEEE international conference on multimedia and expo(icme). Toronto, Canada, 2006. p. 629–32.

Pequeno HSL, Gomes GAM, Andrade RMC, de Souza JN, de Castro MF. FrameIDTV: a framework for developing interactive applications on digital television environments. J Network Comput Appl 2010;33:503–11.

Petersen H, Horster P, Horster DP. Self-certified keys—concepts and applications. Chapman & Hall; 1997.

Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 1978;21:120–6.

Rocha BPS, Costa DNO, Moreira RA, Rezende CG, Loureiro AAF, Boukerche A. Adaptive security protocol selection for mobile computing. J Network Comput Appl 2010;33:569–87.

Scott M, Costigan N, Abdulwahab W. Implementing cryptographic pairings on smartcards. Cryptographic hardware and embedded systems—(CHES 2006), Proceedings2006. p. 134–47.

Shirazi H, Cosmas J, Cutts DA. Cooperative Cellular and broadcast conditional access system for pay-TV systems. IEEE Trans Broadcast 2010;56:44–57.

Song R, Korba L. Pay-TV system with strong privacy and non-repudiation protection. IEEE Trans Consumer Electron 2003;49:408–13.

Sun H-M, Chen C-M, Shieh C-Z. Flexible-pay-per-channel: a new model for content access control in pay-TV broadcasting systems. IEEE Trans Multimedia 2008;10: 1109–20.

Sun H-M, Leu M-C. An efficient authentication scheme for access control in mobile pay-TV systems. IEEE Trans Multimedia 2009;11:947–59.

Tamura Y, Miyaji A. Anonymity-enhanced pseudonym system. Applied cryptography and network security. Berlin/Heidelberg: Springer; 2003. p. 33–47.

Wang YY, Liu JY, Xiao FX, Dan J. A more efficient and secure dynamic ID-based remote user authentication scheme. Comput Commun 2009;32:583–5.

Yang J-H, Chang C-C. An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Comput Secur 2009;28:138–43.

Yang GM, Huang Q, Wong D, Deng XT. Universal authentication protocols for anonymous wireless communications. IEEE Trans Wireless Commun 2010;9: 168–74.

Yoon EJ, Ryu EK, Yoo KY. Further improvement of an efficient password based remote user authentication scheme using smart cards. IEEE Trans Consum Electr 2004;50:612–4.