# Cryptanalysis of a Secure and Efficient Authentication Scheme for Access Control in Mobile Pay-TV Systems

Chin-Yu Sun[1], and Ching-Chun Chang[2]
(Corresponding author: Chin-Yu Sun)

Department of Computer Science, National Tsing-Hua University[1]
Hsinchu, Taiwan 30013, R.O.C.
Department of Information Management, National Central University[2]
Taoyuan, Taiwan 32001, R.O.C.
(Email: sun.chin.yu@gmail.com)
(Received Mar. 15, 2014; revised and accepted June 5 & July 25, 2015)

## Abstract

In 2012, Yeh and Tsaur proposed an advanced scheme for access control in mobile pay-TV systems based on pairing and elliptic curve, which were inherent in the cryptography of Sun and Leu's scheme. In their paper, they pointed out two weaknesses in Sun and Leu's scheme and tried to overcome these weaknesses. However, we still found that Yeh and Tsaur's scheme was not secure. In this research, we will show that an attacker who obtains an obsolete, previous session key can easily break Yeh and Tsaur's scheme. The analysis shows that Yeh and Tsaur's scheme is not secure for practical applications.

*Keywords: Authentication, conditional access system, cryptanalysis, pay-TV services*

## 1 Introduction

With the tremendous breakthroughs in wireless network technologies and electronic commerce, television payment systems (i.e., pay-TV systems) have become one of the most significant modes of payment in multimedia services. Pay-TV systems allow viewers to selectively purchase their favorite programs and control the access of those authorized viewers to paid TV programs. For these reasons, the issue of authorization in pay-TV systems has become important and attracted a lot of attention.

In the early stages of designing pay-TV systems, researchers tried to utilize the properties of conditional access systems (CASs) to obtain more secure and convenient control of users' access. Several CASs based on symmetric cryptosystems have been proposed [2, 3, 8]. Unfortunately, researchers have found that schemes based on symmetric cryptosystems are insecure. For this reason, different types of pay-TV schemes have been proposed. In 2000, Lee [5] designed an authentication protocol based on the digital-signature technique. In Lee's scheme, pay-TV systems can deal effectively with the problems of privacy and non-repudiation. In 2003, Song and Korba [7] proposed an RSA-based authentication protocol for pay-TV systems. In 2009, Sun and Leu [9] proposed an authentication scheme for pay-TV systems using a bilinear pairing technique [1] and elliptic curve cryptography [4, 6]. However, Yeh and Tsaur [10] pointed out that there were two security flaws in Sun and Leu's scheme, i.e., 1) failure in subscriber authentication and 2) unauthorized access. Also, Yeh and Tsaur proposed an advanced scheme to improve these security flaws, but we found that Yeh and Tsaur's scheme still does not have adequate security. Specifically, their scheme cannot resist Type II adverse event (Section 3). This shortcoming will be demonstrated and analyzed in detail in the following section.

## 2 Yeh and Tsaur's Scheme

In this section, first, we review Yeh and Tsaur's scheme, and, then, we discuss its weakness. Yeh and Tsaur's scheme is divided into four phases: 1) initialization, 2) issue, 3) subscription, and 4) hand-off. Here, we omit descriptions of Phases 3 and 4 because the weakness has no immediate impact in those phases. A more-detailed description of Yeh and Tsaur's scheme are given in [10].

### 2.1 Initialization Phase

First, the server must choose an elliptic curve $E$ (with order $q$) and a base point $P$. Then, the server sets a cyclic additive group $G_1$ (with order $q$), multiplicative group $G_2$ (with order $q$), and a bilinear map $e$ ($G_1 \times G_1 \rightarrow G_2$). At the same time, the server chooses two secret numbers $x$ and $k_s \in Z_q^*$ to generate $A_S = x \cdot P$ and $Z_S = k_s \cdot A_S$. Then, the server encodes a service identity number $SIN$ to $GSIN = (x_{SIN}, y_{SIN}) \in G_1$ and encodes its identity $ID_S$ by a one-way hash function $H_1(\cdot)$, which maps $\{0,1\}^* \rightarrow G_1$. After that, the server publishes $Q_S = H_1(ID_S)$, $A_S$, and $GSIN$.

After self-setting, the server helps the $i^{th}$ user to compute $Q_i = H_1(ID_i)$ and choose one secret key $x_i$. Then, the server generates an authentication public key $A_i = x_i \cdot P$ and two private keys $P_i = x_i \cdot Q_i$ and $Z_i = x_i \cdot A_S$. Furthermore, the server encodes $ID_i$ to $GID_i = (x_{ID_i}, y_{ID_i}) \in G_1$. Finally, the server sends $Q_i$, $P_i$, $A_i$, $Z_i$, and $GID_i$ via a secure channel.

### 2.2 Issue Phase

When the user $i$ wants to access the service, he or she can execute the issue phase. In this phase, first, the user selects one secret key $k_i \in Z_q^*$ to generate the authentication parameters as $a_i = k_i \cdot A_i$, $E_i = k_i \cdot P$, $X_i = k_i \cdot A_S$, $C_i = k_i \cdot P_i + k_i \cdot x_{sk} \cdot Q_S$, $UID_i = GID_i + k_i \cdot y_{sk} \cdot Z_S$, and $USIN_i = GSIN + k_i \cdot (x_{sk} + y_{sk}) \cdot A_S$. After all of the authentication parameters have been generated, the user sends the message $Auth_i = \{a_i, E_i, X_i, C_i, UID_i, USIN_i\}$ to the server to request service.

After the server receives the message $Auth_i$ from the user, the server generates the session key $SK_i = a_i \cdot x = (x_{sk}, y_{sk}) \in G_1$. Then, the server can decrypt $UID_i$ and $USIN_i$ to extract $GID_i$ and $GSIN$. After that, the server can decode $GID_i$ and $GSIN$ to $ID_i$ and $SIN$, respectively. Finally, the server computes and verifies the equation $e(C_i, A_S)? = e(Q_i, SK_i) \cdot e(Q_S, x_{sk} \cdot X_i)$ to verify the identity of the user, where $e(\cdot)$ is a bilinear paring map. After passing the verification, the server can use received parameters to compute $Y_i = Q_i \cdot x$, $Y_G = \sum_{i=1}^{m} Y_i$, $Q_G = \sum_{i=1}^{m} Q_i$, $\lambda_K = H_2(SIN, (Y_G + Z_S))$, and a certification token $CT = e(Y_G, Q_G) \cdot \lambda_K$. Then, the server sends the message $Auth_S = \{Y_G, Q_G, CT\}$ to the user.

Then, after the user receives the message $Auth_S$, he or she can compute and verify the equation $e(Y_G, a_i)? = e(Q_G, SK_i)$ to verify the validity of the server. If the equation holds, the user can generate her or his own individual certification token $CT_i = CT \cdot e(Y_G, (Q_G - Q_i))^{-1}$; otherwise, the user terminates the procedure.

### 2.3 Security Analysis

Two types of adverse events were pointed out by Yeh and Tsaur in [9], i.e., 1) an attacker can modify the authentication parameters and pass the subscriber authentication and 2) an attacker can use one previous session key to gain access to services. Yeh and Tsaur claimed that their scheme could withstand both of these adverse events. Upon careful assessment of their security analysis, we were able to demonstrate that Yeh and Tsaur's scheme can be defeated by a Type II adverse event. In order to obtain more clear security analyses, we developed a scenario to analyze Yeh and Tsaur's scheme. Here, we assume that there is an attacker, Justin, who obtains the previous round's session key $SK_i$ from his target user $i$. Then, we can proceed to accomplish the scenario as described below.

First, Justin intercepts the message $Auth_i = \{a_i, E_i, X_i, C_i, UID_i, USIN_i\}$, which was transmitted between the user $i$ and the server. Also, he can use the session key $SK_i$ and the parameters $UID_i$ and $USIN_i$ to extract $GID_i$ and $GSIN$ by computing $GID_i = UID_i - (y_{sk} \cdot SK_i)$ and $GSIN = USIN_i - ((x_{sk} + y_{sk}) \cdot SK_i)$. Second, Justin chooses a random number $J$ to generate one fake session key $SK_i' = a_i x \cdot J = (x_{sk}', y_{sk}')$ and computes the fake parameters as $a_i' = a_i \cdot J$, $E_i' = E_i / cdot J$, $X_i' = X_i \cdot J \cdot (x_{sk}')^{(-1) \cdot x_{sk}}$, $C_i' = C_i \cdot J$, $UID_i' = GID_i + y_{sk}' \cdot SK_i'$, and $USIN_i' = GSIN + ((x_{sk}' + y_{sk}') \cdot SK_i')$. After that, he sends the fake message $Auth_i' = \{a_i', E_i', X_i', C_i', UID_i', USIN_i'\}$ to the server.

After receiving the message $Auth_i'$, the server begins to use its secret number $x$ to generate the session key $SK_i' = a_i' \cdot x = (x_{sk}', y_{sk}')$. Then, the server computes $GID_i = UID_i' - (y_{sk}' \cdot SK_i')$ and $GSIN = USIN_i' - ((x_{sk}' + y_{sk}') \cdot SK_i')$. Furthermore, the server can use extracted parameters $GID_i$ and $GSIN$ to map $ID_i$ and $SIN$. Finally, the server computes and verifies the equation $e(C_i', A_S)? = e(Q_i, SK_i') \cdot e(Q_S, x_{sk}' X_i')$ to verify the validity of the user. However, the fake parameters that were generated by Justin can still pass the verification. The details of the equation are shown as follows:

$$\begin{aligned}
& e(C_i', A_S) \\
= \; & e(J \cdot k_i \cdot P_i + J \cdot k_i \cdot x_{sk} \cdot Q_S, A_S) \\
= \; & e(J \cdot k_i \cdot x_i \cdot Q_i, A_S) \cdot e(J \cdot k_i \cdot x_{sk} \cdot Q_S, A_S) \\
= \; & e(Q_i, A_S)^{J \cdot k_i \cdot x_i} \cdot e(Q_S, A_S)^{J \cdot k_i \cdot x_{sk}} \\
= \; & e(Q_i, x \cdot P)^{J \cdot k_i \cdot x_i} \cdot e(Q_S, J \cdot k_i \cdot x_{sk} \cdot A_S) \\
= \; & e(Q_i, J \cdot k_i \cdot x_i \cdot x \cdot P) \cdot e(Q_S, J \cdot k_i \cdot x_{sk} \cdot A_S) \\
= \; & e(Q_i, SK_i') \cdot e(Q_S, x_{sk}' X_i').
\end{aligned}$$

According to the above derivation, we see that Justin can use the fake parameters to cheat the server successfully. Most importantly, the original session key $SK_i$ that protects the services in the pay-TV system was replaced by the fake session key $SK_i'$. However, Justin can compute and generate $SK_i' = SK_i \cdot J$, thereby obtaining unauthorized access to the pay-TV system.

## 3 Conclusions

Although Yeh and Tsaur proposed an advanced scheme for pay-TV systems to overcome the weaknesses in Sun and Leu's scheme, their advanced scheme still has a serious security flaw. In this research, we pointed out Yeh and Tsaur's advanced scheme is insecure. Using a simple and clear attack scenario, we showed that an unauthorized attacker can modify the transmitted message and cheat the server by gaining access easily.

# References


[1] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", in *Proceedings of 21st Annual International Cryptology Conference*, vol. 2139, pp. 213-229, California, USA, 2001.

[2] ETSI, *Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Service Purchase and Protection*, Technical Specification ETSI-TS-102-474-V1.2.1, 2009. (http://www.etsi.org/deliver/etsi_ts/102400_102499/102474/01.02.01_60/ts_102474v010201p.pdf)

[3] Y. L. Huang, S. P. Shieh, F. S. Ho, and J. C. Wang, "Efficient key distribution schemes for secure media delivery in pay-TV systems", *IEEE Transactions on Multimedia*, vol. 6, no. 5, pp. 760–769, 2004.

[4] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[5] N. Y. Lee, C. C. Chang, C. L. Lin and T. L. Hwang, "Privacy and non-repudiation on pay-TV systems", *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 20–27, 2000.

[6] V. S. Miller, "Use of elliptic curves in cryptography", in *Proceedings of Advances in Cryptology (CRYPTO'85)*, vol. 218, pp. 417–426, California, U.S.A., 1985.

[7] R. Song and L. Korba, "Pay-TV system with strong privacy and non-repudiation protection", *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 408–413, 2003.

[8] H. M. Sun, C. M. Chen and C. Z. Shieh, "Flexible-Pay-Per-Channel: A new model for content access control in pay-TV broadcasting systems", *IEEE Transactions on Multimedia*, vol. 10, no. 6, pp. 1109–1120, 2008.

[9] H. M. Sun and M. C. Leu, "An efficient authentication scheme for access control in mobile pay-TV systems", *IEEE Transactions on Multimedia*, vol. 11, no. 5, pp. 947–959, 2009.

[10] L. Y. Yeh and W. J. Tsaur, "A secure and efficient authentication scheme for access control in mobile pay-TV systems", *IEEE Transactions on Multimedia*, vol. 14, no. 6, pp. 1690–1694, 2009.


**Chin-Yu Sun** received the MS degree in Department of Information Engineering and Computer Science from Feng Chia University, Taichung, Taiwan in 2013. He is currently pursuing his Ph.D. degree in computer science from National Tsing Hua University, Hsinchu, Taiwan. He current research interests include information security, cryptography, wireless communications, mobile communications, and cloud computing.

**Ching-Chun Chang** was born in Taiwan. He is presently an undergraduate student of the Department of Information Management, National Central University, Taoyuan, Taiwan. His current research interests include Information Security, Data Communication as well as E-Commerce Applications

.