誌謝 (Acknowledgements)

在此論文完成之際，首先感謝我的指導教授李正吉博士，給予我許多寶貴的建議與指導，使能順利的完成此論文，讓我在這段學習過程中受益良多，僅此致最深的謝忱，提攜勉勵之情，將畢生難忘。

此外,還要感謝口試委員陳舜德博士、陳志銘博士及李俊達博士，感謝三位口試委員給予我最專業的指導,並給予我的論文最有用的建議，俾使論文得以更加完善。

當然，能夠完成這本論文，更要歸功於研究室的戰友們熱情地指導與包容。感謝伊婷學姐細心地分享細節，並互相給予鼓勵與打氣；感謝冠志同學耐心地和我討論研究的核心問題;感謝彥銘與哲維學弟，經常一同討論報告，思考問題，能夠做出珍貴的研究結果。

最後,感謝我的家人,謝謝你們在這段日子來給予我鼓勵與關懷，使得這一段求學生涯無後顧之憂，才得以順利完成學業。僅以本文獻給我敬愛的家人及所有關心我的人,感謝你們在我的求學旅途中給予我所有的幫助與關懷，深感謝意。

中文摘要

網路電視(Internet Protocol Television)為網路發展中非常重要的一個領域，有別於傳統電視，網路電視是一種以網路型態提供給用戶使用電視服務的一套架構，結合媒體、通訊與廣告等數位內容與互動服務成為新興的商業模式，由於網路電視包含許多優點，因此，世界各地對網路電視之發展都抱有高度的興趣。網路電視應用範圍相當廣泛，包括有線和無線，亦可結合電信業者提供手機服務，行動裝置服務等等，未來也將有可能影響傳統電視，將取而代之，若能將網路電視有效利用，將會是一個極大的市場。

由於在網路電視認證使用者身份時很容易暴露出用戶身份，因此，我們需要一個安全的加密方法。本研究將設計出具安全性之金鑰交換協定，達到安全的相互認證。同時更考量在智慧卡認證過程中，如何更有效率的透過加密進行認證也是我們研究的目標。我們更進一步研究如何防止攻擊者入侵的安全機制，因此，本研究將提出具有效率且安全的網路電視機制，這些新的機制增加了認證過程中之安全性，效率性和實用性，並且擁有新功能，透過此一研究預期將對網路電視有更完備的探討，並帶動網路電視的蓬勃發展。

關鍵字: 匿名性，認證，網路電視，無線射頻，智慧卡。

Abstract

IPTV (Internet Protocol Television) is a very important field in the network development. Compared to traditional television, IPTV combines the digital contents like media, communication and advertisements with interaction into the emerging business model to provide users with television service. Because the IPTV contains many merits, therefore, the whole world has a high interest in the development of the IPTV. The IPTV application scope is quite big, it includes not only wired and wireless, but also provides a unified way for the telecommunication entrepreneur to provide handset service, mobile device service and so on. In addition, in the future perhaps IPTV even will possibly affect and even displace traditional television. If we can use IPTV effectively, it could have an enormous market.

This study will design the internet authentication system which is both anonymous and secured. Simultaneously, how to authenticate more efficiently by encryption in the smart card authentication process is also our research objective. Further, we shall study how to build a security mechanism to prevent the attacks. Based on these researches, we anticipate having a more complete study of Internet Protocol Television. Therefore, this study plans to propose a new, efficient and new featured scheme Internet Protocol in IPTV broadcasting system; these new mechanisms will provide security, efficiency and usability in the authentication process.

Keywords: Anonymity, Authentication, IPTV, RFID, Smart Card.

Table of Contents

List of Tables

List of figures

Chapter 1

Introduction

1.1 Research Motivation

With rapid technological advancements of networks, digital images have been adopted worldwide in traditional TV system architectures. Users must follow the programs provided by the networks, though because of time and space factors, this often leads to the specific needs of a large number of users being neglected because they do not coincide with the time periods when users watch TV. Therefore, the size of the TV market is limited. The maturing of Internet technology has resulted in excellent studies on Internet Protocol Television (IPTV), which not only overcame the shortcomings of traditional TV, but is a more convenient and efficient machine for viewing. Users may, at any time and place, watch TV via the Internet and the IP network that sends digital content. This approach requires a secure authentication mechanism for IPTV to protect the transmission content [2, 20, 24, 25]. At present, most IPTV authentication mechanisms are used on conditional access systems to provide content to paying customers [42, 49]. Regarding video signal transmission, IPTV and traditional TV networks are extremely different. The traditional manner involves transmitting televised images simultaneously and broadcasting all channels via either fiber wire or cable to clients. On the contrary, the IPTV is only transmitted when a user clicks on a specific channel.

IPTV delivery methods are advantageous as they save network bandwidth resources and watching the total number of channels without being limited by hardware, and can provide cross regional display or cross-transmission. The comparison between a traditional TV and IPTV is shown in Table 1.1.

Table 1.1 A comparison of traditional TV with IPTV

Project	Traditional TV	IPTV
Transport Platform	Provided by the television industry	Provided by private network traffic
Services	Watch in the fixed area	Fixed services, the industry owns and manage it
Equipment Requirement	TV	Personal computers, mobile devices, STB
Charging method	Half a year	Monthly fees or membership
Way of viewing	Watching the programs in fixed time	Watching the programs anytime

The development and application of IPTVs has become increasingly widespread. More users use IPTV through networks. IPTV services comprise toll-free channels, basic channels, and premium channels. Premium channels are free as long as users only purchase the set-top box (STB) to watch programs. Basic channels require fixed monthly payments. With paid channels that contain a specific channel for programs, users are required to pay additional fees. The IPTV comprises four parts: (1) head-end equipment; (2)

broadband receiver; (3) intermediary devices; (4) and client receiver. The head-end device is responsible for both video and audio coding and transmission. The broadband receiver is responsible for file transfer. The intermediary device is responsible for managing service providers, and the client receiver, which is installed in the client, is used for image conversion. The IPTV chart is shown in Figure 1.1.

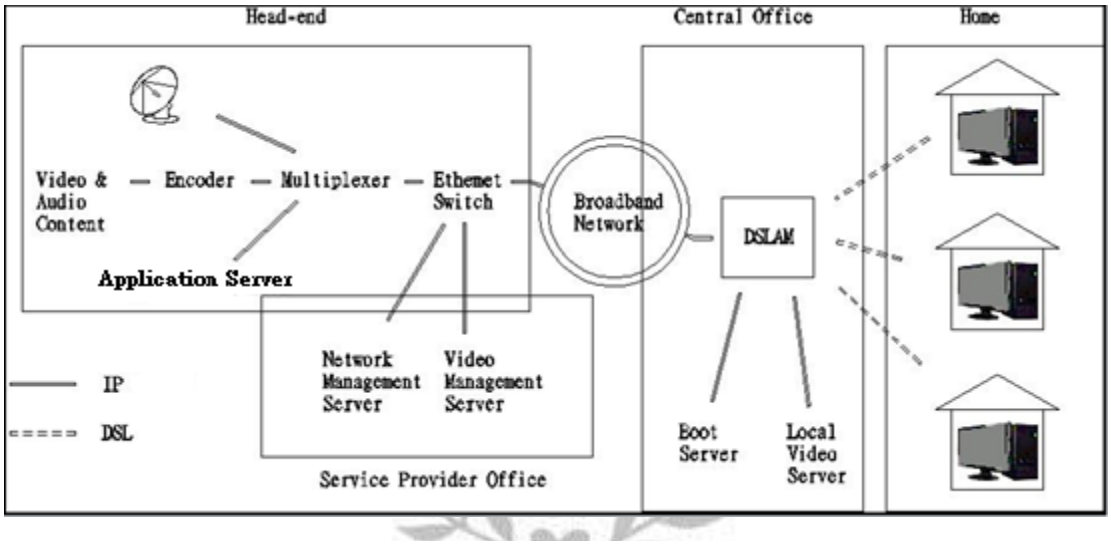

Figure 1.1 IPTV architecture [28]

The network television service provider must provide a method for authenticating user identification, which enables the user to carry on the identification authentication with the service end. Therefore, the authentication requires two types of chief equipment: the first is the smart card, and the other is a set-top box (STB). A smart card usually represents a user, though the STB serves as the medium for the authentication process between the user and service. However, in the mutual authentication communication involving both the smart card and STB

mutual authentication communication [43], a conditional access system is regarded as the main system, which is a comprehensive system that contains both encryption and decryption technology, which is capable of locking codes and is equipped with decoding technology, network technology, smart card technology, information bank technology, and so on. To integrate the aforementioned technologies, the system is suitable for IPTV encryption technology construction. The conditional access system must obtain a session key to decode the encrypted channel for reading the STB. This key for encrypting and decoding is called a control word [12]. In the conditional access system, a significant amount of program information is decoded by using the control word, which both prevents unauthorized users from entering, and also protects and allows paid users to log in normally. Digital images can be transmitted in the channel safely with this process, and authorized users can watch programs by successfully passing the authentication process of either the smart card or the STB. The conditional access system charges users by providing the aforementioned services.

The reason why most network television service providers use the conditional access system is that the structures of traditional televisions are both costly for calculation and inefficient in operations. Since most network television communication is one way, users cannot authenticate online. To solve this issue, the service provider must offer mutual authentication of both the smart card and STB in order to protect the user and ensure security. However, both a replay attack and smart card cloning

can occur during the mutual authentication process of either the STB or the smart card [19, 40].

The attack of smart card cloning [28] involves the attacker duplicating an authorized smart card and misleading STB to enable login. The replay attack entails the attacker intercepting information that the user sends using a smart card to execute the authentication process with STB, ensuring that STB mistakes the attacker for the user when logging into the system. Smart cards are critical for user authentication in IPTVs. Therefore, ensuring confidentiality of the information stored in the smart card is essential. A smart card is a tiny transmission device containing memory, which can store programs and keys to limit the access to stored information, to protect it from being revised or deleted. In addition, smart cards may use the key to verify user identify. The information related to the key is saved in the protected memory of the smart card.

1.2 Research Subjects

In this study, we focus on key agreement schemes for DTV environment. The first key agreement scheme is based on RSA. Any legal user can use the services in this scheme. The proposed scheme is secure against the man-in-the-middle attack, the replay attack, and achieves the property anonymous. Furthermore, it can provide mutual authentication. Therefore, a more secure scheme is presented in our first research subject.

The second DTV scheme provides billing service. The billing system can provide users a more convenient way for payment. For

charging in traditional television, many billings are half-yearly done. However, in the proposed protocol, users can watch TV in their free time and take single billing method. As a result, users can choose the most suitable billing methods according to their requirements.

The third DTV scheme is to use the RFID. As information technology continuously progresses, more applied technologies are developed, such as radio frequency identification (RFID). In this study, we propose a novel digital television (DTV) structure that uses RFID for encryption. RFID is widely used for various applications because of its advantages such as an extended lifetime and security, and it is less affected by environmental constraints.

1.3 Thesis Organization

The content of this thesis is organized as follows: Yoon et al.'s user authentication scheme and our improved scheme are introduced in Chapter 2. The proposed frequency billing service for digital television system is shown in Chapter 3. The proposed practical RFID authentication mechanism for digital television is shown in Chapter 4. Finally, our conclusion is given in Chapter 5.

Chapter 2

A Key Exchange Scheme with Anonymity between STB and Smart Card in IPTV Broadcasting

Internet Protocol Television (IPTV) is a critical field in network development. Compared to traditional television, the IPTV combines digital contents such as media. Interactive communication and advertisements serve the emerging business model to enable users to watch television services [29, 44]. Because the IPTV comprises a large number of advantages, the world are highly interested in its development. The IPTV application scope is relatively large, not only including wired and wireless, but also integrating telecommunication businesses to provide handset services, mobile device services and so on. This will affect traditional televisions in the future, and even displace them. If the IPTV becomes popularized with users, this could result in an enormous market.

Because the identities of users are generally exposed with ease when IPTVs authenticate them, the optimal method for securing information security is to hide the identities of users. This study designed an Internet authentication system that is anonymous and secure, which can be applied to solve the smart card duplication and data resending attack problems. The session key and timestamp of cryptography are used in the

technique to achieve security and anonymity in the authentication process. An approach to more efficient authentication via encryption in the smart card authentication process is also an objective of this study. Furthermore, this thesis contributes to the methodology to build a security mechanism preventing attacks. Based on relevant research, this study proposes a new, efficient, and safe IPTV. This new mechanism enhances the security, efficiency, and usability of the authentication process. More complete studies on IPTV will be required.

2.1 Preliminary

This section introduces the conditional access system [1, 16, 18, 30, 31, 32, 38] and a discussion of the current literature relevant to smart cards and STBs for key agreements of mutual authentication. The structure of the conditional access system is shown in Figure 2.1.

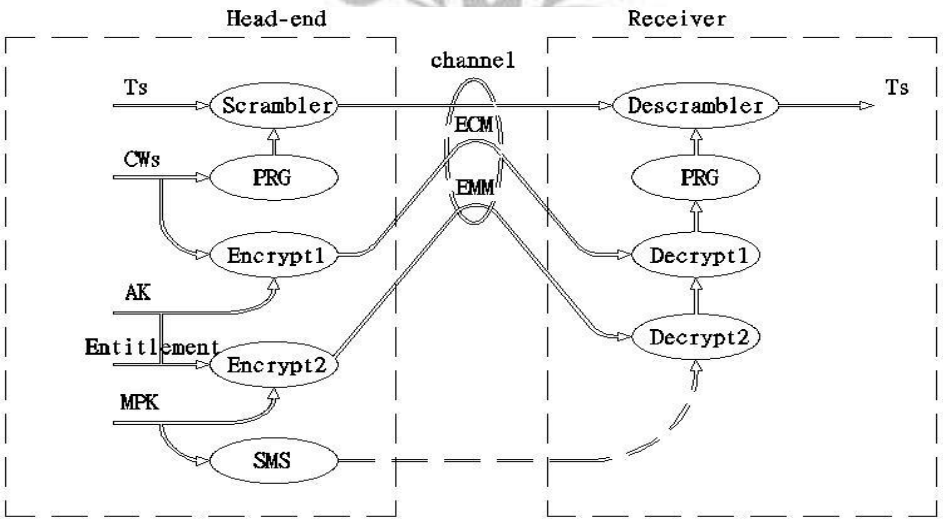

Figure 2.1 Conditional access system

The head-end, which mainly includes terrestrial broadcasting, transnational satellites and content providers offer video and audio content, formatting, encoding, and multiplexing transmissions. The control word (CW) for each user initiates a set of randomly generated virtual strings, which is produced by the pseudo-random number generator. The virtual strings are used to lock and decode digital video. The control word is encrypted with an authorization key (AK). The encrypted control word is transferred to the corresponding channel via entitlement control message (ECM). The AK also is encrypted with a master private key (MPK) via entitlement management message (EMM). The ECM, EMM, and scrambled program are multiplexed in a new transport stream (TS). The IPTV is responsible for the data management unit of users, known as the subscriber management system (SMS). The SMS manages issuing or updating the smart card for the subscriber and memorizes the private key and account information of users, which contain MPK and other information. When the user receives a transmission from the SMS over the data, it can scan the smart cards and STB for mutual authentication. When users want to watch subscription channels, the requirements will be sent to the STB. When STB receives the demand from the channel signal, modems signal the demanded reduction and restore the signal transferred to the smart card for decryption. This mutual authentication key agreement requires using both the smart card and STB. A set of control words is encrypted using symmetric keys in the smart card before being sent back to the STB. The user can then use the control word decoder to

decode this set of symmetric keys.

In other words, the control words must be encrypted before the STB returns the transmission. Otherwise, the attacker can change the control word with any decoder to decrypt the program, thus rendering the system extremely unsafe. If no mutual authentication is produced between the STB and smart card, an attacker could use the smart card cloning and replay attack to pass authentication. Therefore, the mutual authentication between the smart card and key agreement is necessary for the system structure [13].

In 1976, Diffie-Hellman [8] proposed an allotment of a public key algorithm based on discrete issues. However, their mechanisms do not use mutual authentication; therefore, the mechanism they proposed cannot fight man-in-the-middle attacks and replay attacks. In 2001, Wong et al. [43] proposed a mutual authentication key consultative mechanism. In the low-power wireless communications, the mechanism can resist replay attacks and man-in-the-middle attacks. However, in 2003, Shim [37] indicated that their mechanism cannot protect against the key share attacks. In 2004, Jiang et al. [15] proposed a key exchange protocol based on digital signatures and a one-way function of mutual authentication between the STB and smart cards. The advantages of the proposed mechanism include security, dynamic symmetric key, and mutual authentication. The mechanism also enables them to change the password and prevent smart card cloning and replay attacks. However, their proposed mechanism cannot provide the most efficient transmission between the STB and the smart card. In 2007, Hou et al. [11] proposed

another security mutual authentication mechanism between the STB and smart card. Their mechanism uses RSA encryption for the mutual authentication algorithm, which is used for encryption. The mechanism requires a considerable amount of computation, which is time-consuming for the smart card reader.

2.2 Review of Yoon et al.'s Method

The method by Yoon et al. [47] comprises five phases, which are the registration phase, login phase, mutual authentication phase, the key agreement phase, and the control word transmission phase. The authentication process is discussed sequentially, and the symbols used in this study are shown in Table 2.2. The method by Yoon et al. is shown in Figure 2.2.

Table 2.2 The notations used in Chapter 2

Symbol	Definition
SMS	Smart card subscription management system
STB	Set-top box
U	User
ID_C	Smart card identity
ID_S	STB identity
PW	User password
xs	STB secret value
$h(.)$	One-way hash function
$E_K(.)/E_K^{-1}(.)$	Symmetric encryption/decryption algorithm
$\oplus$	Exclusive or operation
g	A group of order p
p	An l-bit prime number

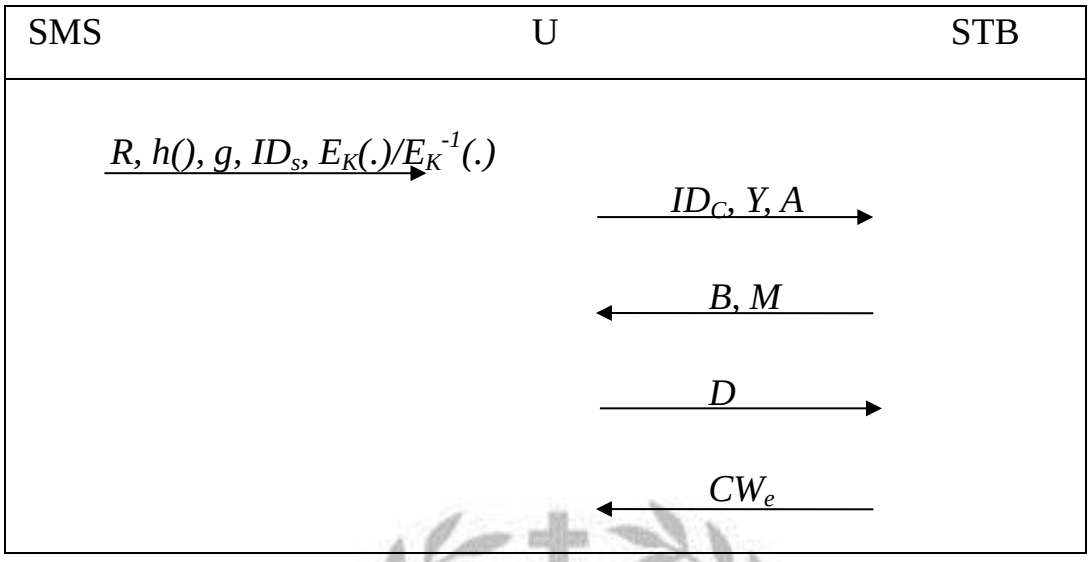

Figure 2.2 Yoon et al.'s mechanism

2.2.1 Registration phase

When a new user (U) wants to use their smart card identity (ID_C) and password (PW) to subscribe to a charged channel, they send ID_C and PW to the SMS. The SMS calculates R as $R=h(ID_C \oplus xs) \oplus h(PW)$, where xs is the STB secret value. SMS stores R , g, ID_S , $h(.)$, $E_K(.)$, $E_K^{-1}(.)$, MPK, and certain account information in the user's smart card and send it to the user.

2.2.2 Login phase

If the user wants to watch a subscribed program, they must insert their own smart card into the STB before entering the identity and password. The smart card subsequently generates a random number a, and follows the equation to calculate A, X and Y, and sends $\{ID_C, Y, A\}$ to

STB.

$A=g^a \bmod p$

$X=R \oplus h(PW)$

$=h(IDc \oplus xs) \oplus h(PW) \oplus h(PW)$

$=h(IDc \oplus xs)$

$Y=h(X, A, ID_C, ID_S)$

2.2.3 Mutual authentication phase

Upon receiving the login request, the STB and smart card require completing the following steps to accomplish mutual authentication:

Step 1: STB must verify the legitimacy of ID_C first. If illegal, STB rejects the request.

Step 2: STB computes $h(ID_C \oplus xs)$ and checks if $Y=h(h(ID_C \oplus xs), A, ID_C, ID_S)$. If true, STB receives the login request and proceeds to the next step; otherwise, the login request is rejected.

Step 3: STB generates a random number b in Z_q*, and computes B, K, and M as follow, and sends $\{B, M\}$ to the smart card for identification.

$B=g^b \bmod p$

$K=A^b=g^{ab} \bmod p$

$M=h(K, A, ID_C, ID_S)$

Step 4: The smart card computes $K=B^a=g^{ab} \bmod p$ and $M'=h(K, A, ID_C,$

ID_S), and checks if M'= M. If true, the smart card accepts STB identity and proceeds to the next step. Otherwise, the smart card declines to transfer.

Step 5: The smart card computes $D=h(K, B, ID_C, ID_S)$ and sends it to the STB. The STB checks if $D' =h(K, B, ID_C, ID_S)=D$. If true, the STB accepts the smart card identity. Otherwise, the STB rejects the smart card. The mutual authentication by Yoon et al. is shown in Figure 2.2.1.

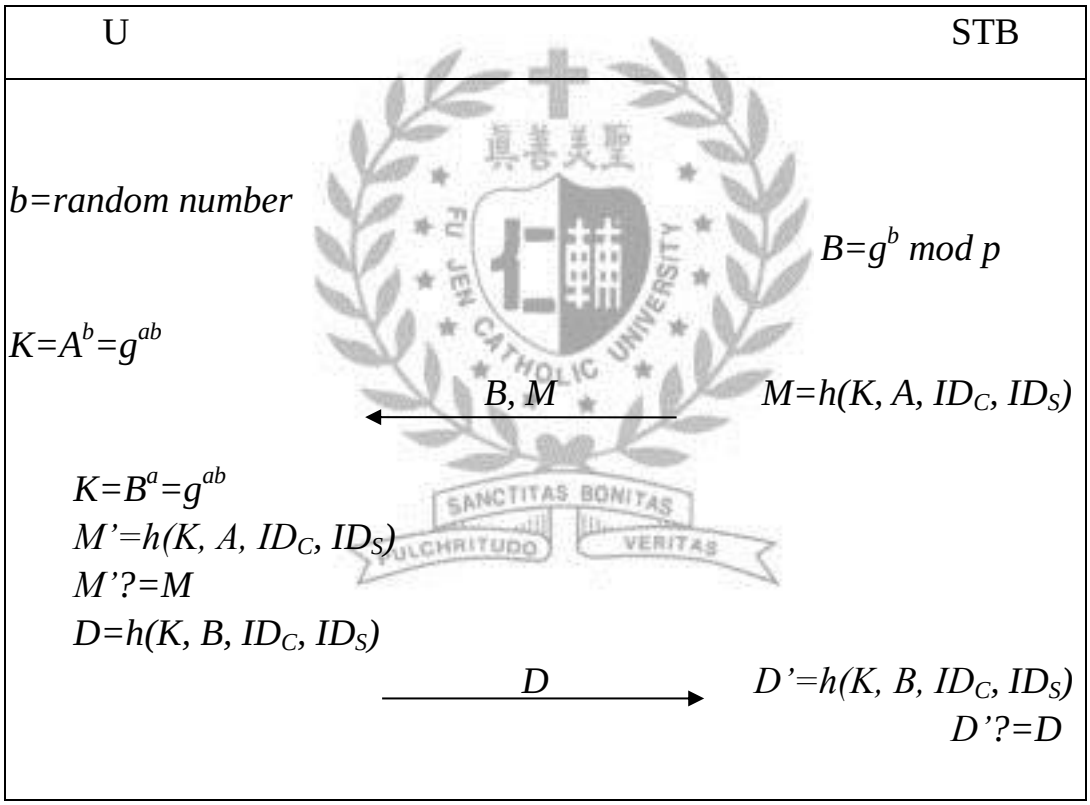

Figure 2.2.1 The mutual authentication phase of Yoon et al.'s method

2.2.4 Key agreement phase

If mutual authentication passes for both the STB and smart card, they can use the following equation to compute the common session key

$SK=h(K, ID_C, ID_S)$, which includes both the random number chosen by the STB and smart card.

2.2.5 *CW* transmission phase

After decrypting *CW* by using the conditional access system, the smart card employs *SK* to encrypt *CW* as $CW_e=E_{sk}(CW)$ before returning CW_e to the STB to descramble the program. The STB can decrypt *CW* as $CW=E_{sk}^{-1}(CW_e)$.

2.3 Analysis of Yoon et al.'s Method

This section proves that the secure key exchange method by Yoon et al. is not secure against certain attacks. This section analyzes the method by Yoon et al. by addressing security problems and describing the problems they encounter to prove that their method is not secure.

2.3.1 Man-in-the-middle attack

This study proves that the secure key exchange protocol by Yoon et al. is not secure against man-in-the-middle attacks and replay attacks. Though their protocol based on that of Diffie-Hellman can prevent attackers from intercepting information, it cannot prevent an attacker from intercepting information to execute replay attacks.

An attacker intercepts the $\{B, M\}$ from the STB before sending to the smartcard, and generates a random number m in Z^*q, computing B_{Ad}, K_{Ad}, M_{Ad} as follows, and sending $\{B_{Ad},M_{Ad}\}$ to the smart card for

identification.

$B_{Ad}=g^m \bmod p$

$K_{Ad}=A^m=g^{am}$

$M_{Ad}=h(K_{Ad}, A, ID_C, ID_S)$

Upon receiving messages from the attacker, the smart card computes $K_{Ad}=B^a{}_{Ad}=g^{am} \bmod p$, $M'_{Ad}=h(K_{Ad}, A, ID_C, ID_S)$ and checks if $M'_{Ad}=M_{Ad;}$, accepts the attacker's identity, and proceeds to the next step; otherwise, the smart card declines to transfer. The smart card computes $D_{Ad}=h(K_{Ad}, B_{Ad}, ID_C, ID_S)$ and sends it to the attacker, who verifies if $D'_{Ad}=h(K_{Ad}, B_{Ad}, ID_C, ID_S)=D_{Ad}$, and accepts the smart card and shares the key K_{Ad} with the smart card.

In the key agreement phase, the smart card using the shared key computes a common session key K_{Ad}, as follows:

$SK_{Ad}=h(K_{Ad}, ID_C, ID_S)$

In the CW transmission phase, the smart card using SK_{Ad} to encrypt CW as $CW_e=E_{SKAd}(CW)$ and sends CW_e to the attacker. The attacker can decrypt CW as $CW=E_{SKAd}{}^{-1}(CW_e)$. Therefore, the attacker can imitate the STB to trick the smart card into believing that it is communicating. The protocol by Yoon et al. is not secure because the same smart card can be used on different STBs, as shown in Figure 2.3.

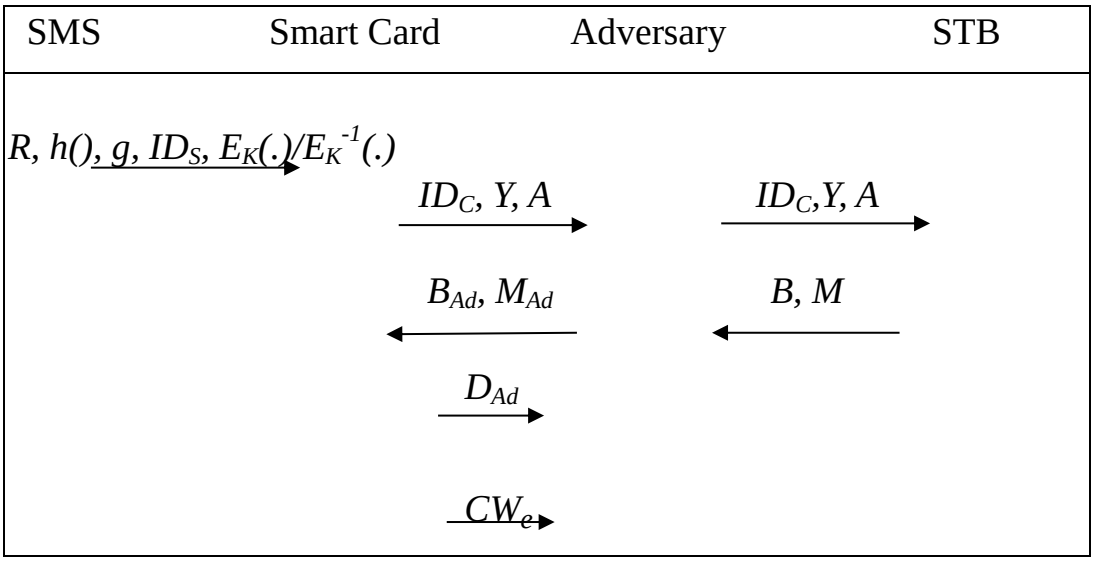

Figure 2.3 Man-in-the-middle attack on the Yoon et al.'s method

2.3.2 Replaying attack

When users use their smart cards to send data to the STB, the data are intercepted and replayed from the attacker. If the system does not have a security authentication mechanism, the attacker can log into the system.

2.3.3 Anonymity

In the process of transmitting data, the user does not hide the identity of their smart card, which reduces the security of data transmission. An attacker intercepts user identity of the smart card and other information. The user's other information can be combined via constant attempts. Using this information, the attacker can login illegally and pass authentication.

2.4 Our Improved Method

This section presents an improvement Method, which can avoid the common variety of attacks. The proposed structure comprises five phases: the registration phase, login phase, mutual authentication phase, the key agreement phase, and control word transmission phase. This study uses the symmetric key to encrypt the smart card's identity, and uses timestamps to prevent attackers from executing replay attacks. In mutual authentication, smart cards can hide user identities to prevent attackers from intercepting information. Therefore, users can feel at ease during authentication. The proposed Method is shown in Figure 2.4.

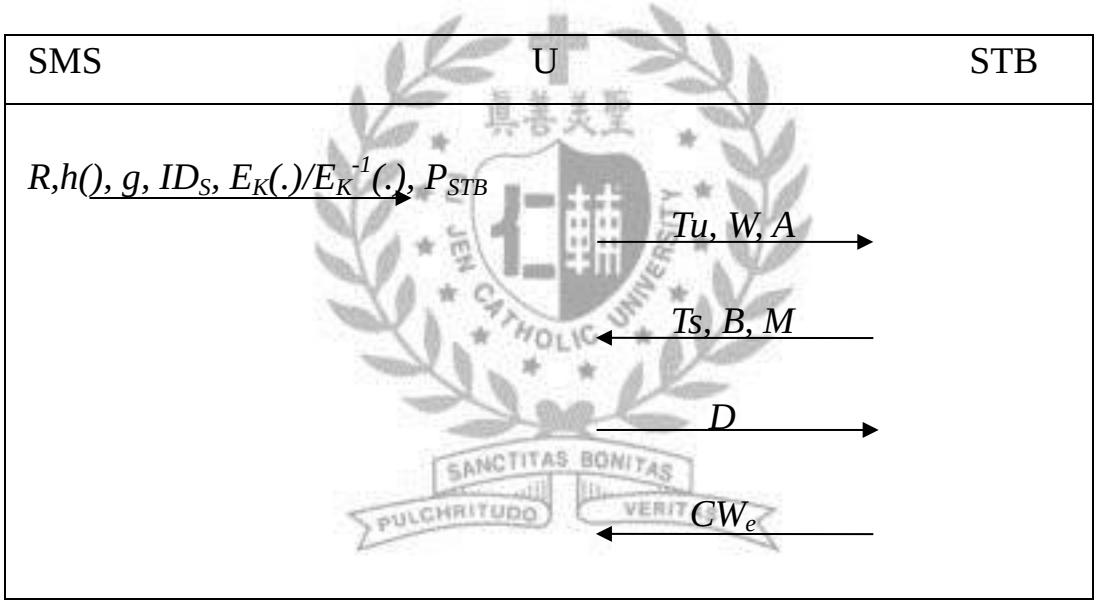

Figure 2.4 Our improved methodmethod

2.4.1 Registration phase

When a new user (U) wants to use their smart card identity (ID_C) and password to subscribe to a charged channel, the new user sends its ID_C and PW to the SMS. Then SMS calculates P_{STB}, R with the following equation:

$P_{STB}=g^e \bmod p$

$R=h(PW) \oplus E_{xs}(ID_C)$

xs is the STB secret value, and stores R , g, ID_S , $h(.)$, $E_K(.)$, $E_K^{-1}(.)$,$P_{STB,}$ MPK, and certain account information of the smart card, which can be sent to the user. The registration phase is shown in Figure 2.4.1.

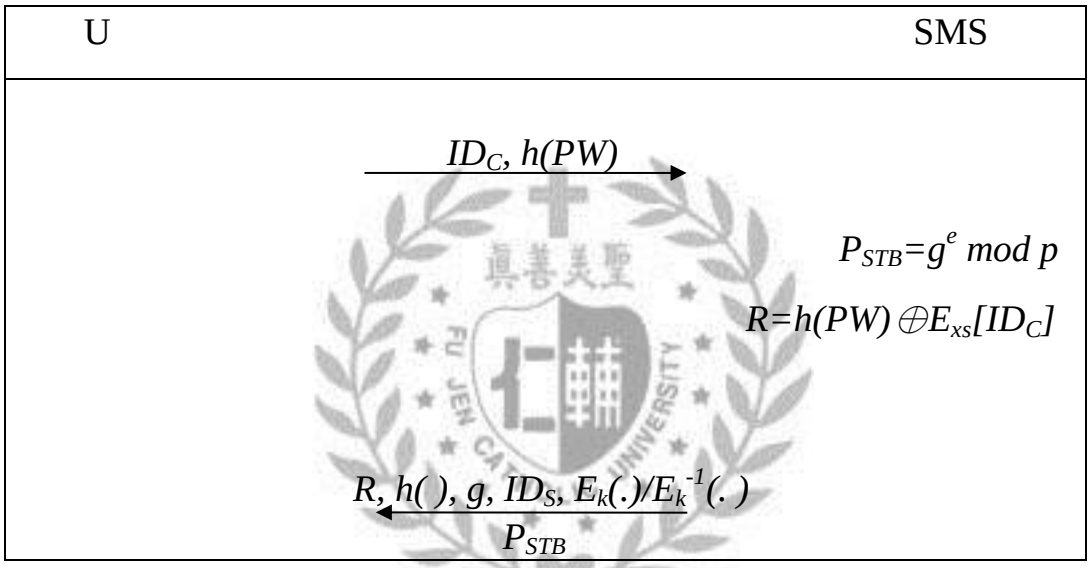

Figure 2.4.1 Registration phase of the proposed method

2.4.2 Login phase

If the user wants to watch a subscribed program, the user must insert its smart card into the STB. The user subsequently enters the identity and password. The smart card generates a random number a, and includes Tu (timestamp) before using these equations to calculate A, DH, X, and W, and sends $\{Tu, W, A\}$ to the STB.

$A=g^a \bmod p$

$DH=P^a_{STB}=g^{ae} \bmod p$

$X=R \oplus h(PW)$

$=E_{xs}(ID_C)$

$W=E_{DH}(X||Tu)$

2.4.3 Mutual authentication phase

Upon receiving the login request, the STB and smart card require completing the following steps to realize mutual authentication:

Step 1: The STB must check the legitimacy of ID_C by using the following equation. If illegal, the STB rejects this request.

$DH=A^e=g^{ae}$

$D_{DH}(W)=X||Tu$

$D_{xs}(X)=ID_c$

Step 2: The STB checks the timestamp of *Tu*. If invalid, the STB rejects the request. Otherwise, it proceeds to the next step.

Step 3: The STB generates a random number *b* in Z_q*, and computes *B*, *K*, and *M* as follows, before sending {*B*, *M*, *Ts*} to the smart card for identification.

$B=g^b \bmod p$

$K=A^b=g^{ab}$

$M=h(K, X, B, Ts, ID_C, ID_S)$

Step 4: The smart card computes $K=B^a=g^{ab} \bmod p$ and $M'=h(K, X, B, Ts, ID_C, ID_S)$, and checks if $M'=M$. If true, it accepts STB identity and proceeds to the next step. Otherwise, the smart card refuses

to transfer.

Step 5: The smart card computes $D=h(K, ID_C, ID_S)$, before sending to the STB, which computes $D'=h(K, ID_C, ID_S)$ and checks whether it is equal to D. If true, the STB accepts the smart card identity. Otherwise, the STB rejects the smart card. The login phase and authentication phase are shown in Figure 2.4.2.

2.4.4 Key agreement phase

If the smart card and STB pass the mutual authentication phase, the smart card uses the shared key to compute a common session key SK, as follows:

$SK=h(K, ID_C, ID_S, Tu, Ts)$.

2.4.5 CW transmission phase

Upon decrypting the CW by using the conditional access system, the smart card uses SK to encrypt CW as $CW_e = E_{SK}(CW)$ and sends CW_e to the STB, which can decrypt CW as $CW=E_{SK}^{-1}(CW_e)$. The user can use the CW to watch the subscribed programs.

2.5 Security Analysis of Our Improved Method

This study presented the proposed method for IPTVs, which not only realizes mutual authentication and key agreement, but also prevents certain attacks. This section analyzes the security of the proposed scheme below. Comparison between our Method and Yoon et al.'s method is

shown in Table 2.5.

2.5.1 Replaying attack

In the proposed method, the user and the STB use the timestamp *Tu* and *Ts*, respectively. If an attacker tries to use a captured wiretap login message { *Tu, W, A}* to execute a replay attack, the STB receives the message and can check the *Tu*. If the time expires, the STB rejects it.

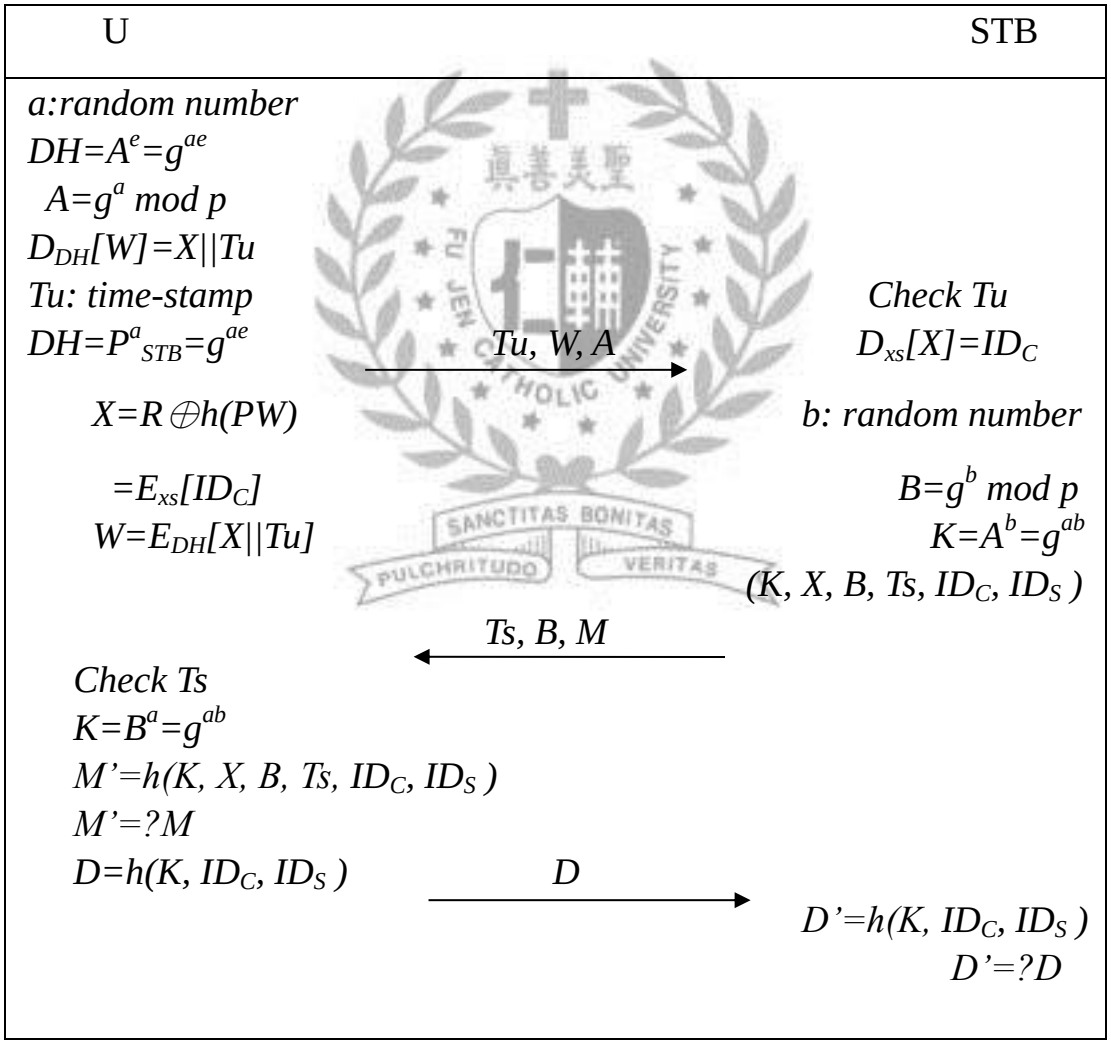

Figure 2.4.2 Mutual authentication of the proposed method

2.5.2 Smart card cloning

When a user’s smart card is lost or stolen, even if the attacker wants to use a copy of the smart card to log into the STB, the STB first checks the identity and password. Therefore, if an attacker does not have the password, they cannot pass the login phase. If attacker guessing the password, they cannot know the hash function of the smart card. The proposed Method thus cannot use a copy of a smart card to access to any STB.

2.5.3 Anonymous

During data transmission, an exposed identity of a user is dangerous. The proposed protocol uses the symmetric key to encrypt user identity. In the transfer process, user identities are hidden via encryption; even if an attacker intercepts the user's information, they cannot know the user's identity, and thus cannot impersonate them to pass authentication. Therefore, encryption of the identity of users is the optimal method for authentication security.

2.5.4 Password security

In the proposed Method, the STB does not require storing the security information of the smart card, including password and identity, which can prevent an attack on the STB to obtain the user password or *ID* of the smart card.

2.5.5 A masqueraded STB

If a masqueraded STB tries to trick the smart card, it must prepare a valid information message {*Ts, B, M*}. However, this is unfeasible because the STB cannot derive the information random number *b* and the session key *k* to compute the information {*B, M*}, and a replay attack can be discovered because of the timestamp *Ts*.

2.5.6 Impersonation attack

In the proposed method, the session key *SK* is generated as the output of a one-way hash function, with inputs being the concatenation of *K*, ID_C, ID_S, *Tu*, and *Ts*. The data *K*, ID_C, ID_S, *Tu*, and *Ts* can only be accessed by the smart card and the STB. The random number *r* is secret information for each session key, and thus, an impersonation attack is impossible. Furthermore, the session key is different in each communication; therefore, attacking and obtaining the *CW* with a known plaintext attack is difficult.

Table 2.5 Comparison between our method and Yoon et al.'s method

	Password	Replay attack	Smart card cloning	Middle attack	Anonymous identity
Yoon et al.'s protocol	O	X	O	X	X
Our protocol	O	O	O	O	O

Chapter 3

A Novel Frequency Billing Service in Digital Television System

DTV services are getting widespread use, requiring service providers to have effective methods for remotely configuring and managing DTV set-top boxes (STBs). Solutions for such remote management are becoming standards-based. In this thesis, we first propose a secure frequency billing service in DTV broadcasting. The frequency billing system can provide users a more convenient way for payment. For charging in traditional television, many billings are half-yearly done. However, in the proposed protocol, users can watch TV in their free time and take single billing method. As a result, users can choose the most suitable billing methods according to their requirements. Moreover, the proposed protocol is more efficient than other previously proposed protocols by eliminating exponentiation operations which are time-consuming computations. Finally, our protocol not only provides better way for DTV charging but also prevents two common serious problems in DTV broadcasting such as smart card cloning and replay attacks.

3.1 Preliminary

Billing system operators are now interacting with their viewers on many levels, offering them a greater program choice than ever before. Additionally, the deployment of a security system or conditional access (CA), as it is commonly called. Network operators have begun deploying DTV services — television and content-on-demand services delivered over managed broadband networks — to the home over the past few years. As DTV services mature and become more widely deployed [5, 11, 12, 16, 17, 25], service providers must have an efficient way to remotely configure and manage DTV set-top boxes (STBs), which terminate the DTV service in the user's home, render the content for display on the TV set, and allow user interaction via a remote control. DTV is a convergence service of broadcasting and telecommunication that delivers multimedia contents over the Internet. Recently, DTV services are being extended to mobile terminals. Mobile DTV enables to provide multimedia contents to subscribers anywhere, anytime, and even in motion through wire and wireless networks [39]. Mobile DTV services are undergoing security problems such as illegal access by unauthorized users [33], session key intercepting, illegal content distribution, etc. Therefore, mobile DTV services require basic security functions like user authentication, secure key exchange [3], and contents protection.

In this study, we propose a frequency billing service in DTV system and it has many advantages than traditional DTV system such as performance efficiency and more types of billing methods. If a user seldom watched television programs, it is unsuitable for him/her to use the traditional way for charging. To satisfy the variety of charging situations, we propose a frequency billing protocol that the fees will be charged according to user's watching time. On the other hands, the proposed protocol only uses exclusive-or operations between smart card

and STB. Thus, it is more efficient than other previous protocols such as Jiang et al.'s protocol [15] and Hou et al.'s protocol [11]. As shown in Figure 3.1, Subscriber Management System (SMS) provides billing system for users. Firstly, head end receives the satellite images via the encoder into digital images and sent satellite content to SMS. Then SMS will transfer a digital signal to the set-top box(STB) and users can watch the ordered channel via the STB.

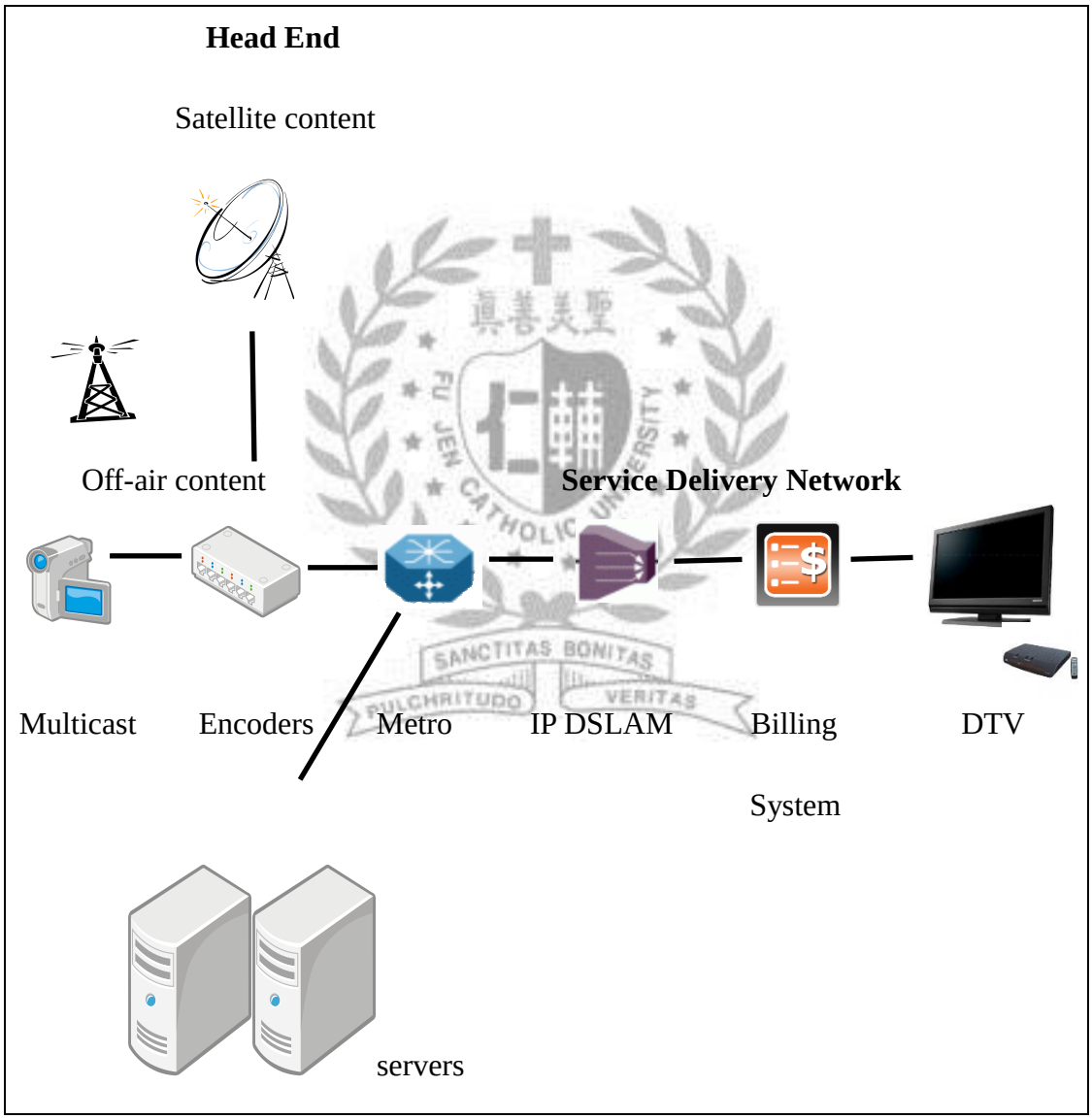

Figure 3.1 The proposed DTV structure

3.2 Proposed Scheme

Table 3.2 Notations used in the Chapter 3.

Notations	Description
ID_i	Identity of the user
C_i	Count of billing number for DTV system
PW_i	Password of the user
$\oplus$	Bitwise exclusive-or operation
$h(\cdot)$	One-way hash function
xs	Secret key of *STB*
$\|\|$	The string concatenation
no#	The registration number of the user
SMS	Smart card subscription management system
STB	Set-top box
Auth	The shared value between user, STB and SMS
Ts, *Tu*	Timestamps

In this section, we propose a frequency billing service in DTV system and the proposed protocol is mainly composed of four phases, registration phase, login and authentication phase, key agreement phase, and *CW* transmission phase. For convenience of description, notations used in this thesis are defined in Table 3.2.

3.2.1 Registration phase

When the frequency billing service starts, the user and SMS need to perform the following steps:

Step 1: The user selects a password PW_i and a random number α, computes $RPW = h(\alpha||PW_i)$ and sends RPW, ID_i, C_i to SMS for registration.

Step 2: When SMS receives the messages from the user, SMS computes ID_T, β and γ as follow:

$ID_T=(ID_i||C_i||no\#)$

$\beta=h(xs||ID_T)$

$\gamma= \beta \oplus RPW$

Where xs is the secret information generated by the SMS for STB and C_i is the number issued by SMS. C_i will store in SMS and user's smart card and it means the number of times that the user wants to watch TV.

Step 3: SMS stores γ, $Auth$ and α into user's smart card and issues it to him/her via a secure channel, where $Auth$ is the shared value between user, STB and SMS. Finally, the user stores α into smart card. We show the flowchart of registration phase in Figure 3.2.

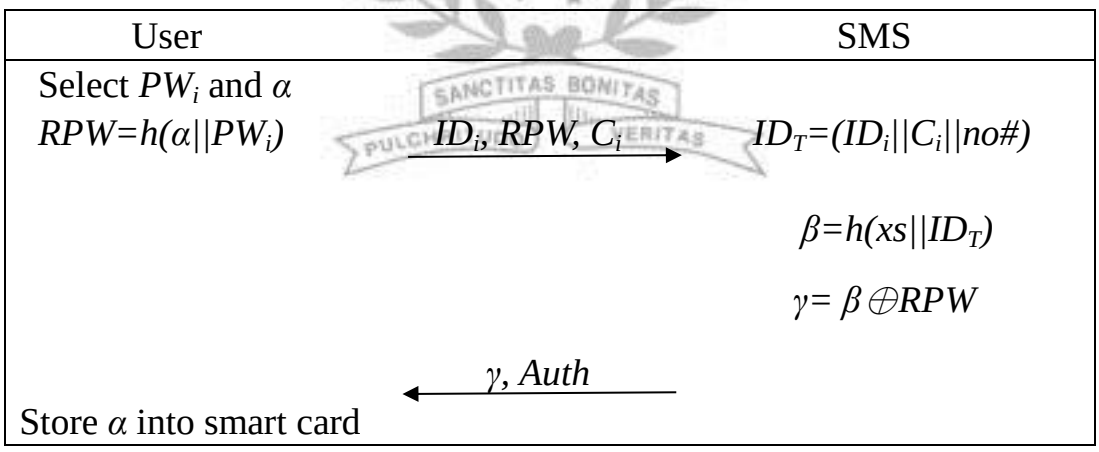

Figure 3.2 Registration phase

3.2.2 Login and authentication phase

When the user wants to use the DTV system, the user needs to complete mutual authentication with STB and he/she performs the following steps:

Step 1: The user uses the smart card and inputs the identity ID_i and password PW_i. Then smart card computes $RPW=h(\alpha||PW_i)$, $\beta= \gamma \oplus RPW$ and $\pi=h(Tu||\beta)$, where α is retrieved from smart card and Tu is user's current timestamp. In addition, the smart card chooses a random number ω, computes $AID_i = ID_i \oplus h(Auth||Tu||\omega)$ and sends AID_i, Tu, ω and π to STB, where $Auth$ is retrieved from smart card.

Step 2: When STB receives the message, it computes $ID_i=AID_i \oplus h(Auth||Tu||\omega)$ and checks the validity of Ci, no# and ID_i. If they are valid, STB computes $ID_T=(ID_i||C_i||no\#)$ and $\beta=(xs||ID_T)$ and checks whether $h(Tu||\beta) = \pi$. If it holds, STB computes $\varepsilon=h(\pi \oplus \beta \oplus Ts)$ and sends ε and Ts to the user, where Ts is STB's current timestamp.

Step 3: When the user receives the messages from STB, it computes $\varepsilon'=h(\pi \oplus \beta \oplus Ts)$ and checks whether $\varepsilon' = \varepsilon$. If it holds, STB is authenticated by the user and the user computes the share key $K=h(\varepsilon \oplus \beta \oplus Tu \oplus Ts)$ and sends K to STB.

Step 4: When STB receives the K from user, it computes $K' = h(\varepsilon \oplus \beta \oplus Tu \oplus Ts)$ and checks whether $K' = K$. If it holds, the user is authenticated by STB and the mutual authentication between user and STB is complete. Finally, STB replaces ID_T with $ID_T' = (ID_i || C_i - 1 || no\#)$ and updates smart card and SMS table.

We show the flowchart of login and authentication phase in Figure 3.2.1.

3.2.3 Key agreement phase

After the mutual authentication procedure, the user and the STB compute $SK = h(\varepsilon \oplus \beta \oplus Tu \oplus Ts \oplus Auth)$ which is taken as their session key SK. Note that SK will be used in CW transmission phase.

3.2.4 *CW* transmission phase

After decrypting the CW by conditional access system, user uses SK to compute $CW_e = E_{SK}(CW)$ and sends CW_e to STB, where $E_{SK}(CW)$ is encryption of data CW using symmetric key SK. Then, STB uses the common session key SK to reveal CW by computing $CW = D_{SK}(CW_e)$, where $D_{SK}(CW_e)$ is decryption of data CW_e using symmetric key SK. Finally, the user can use CW to watch the subscribe programs.

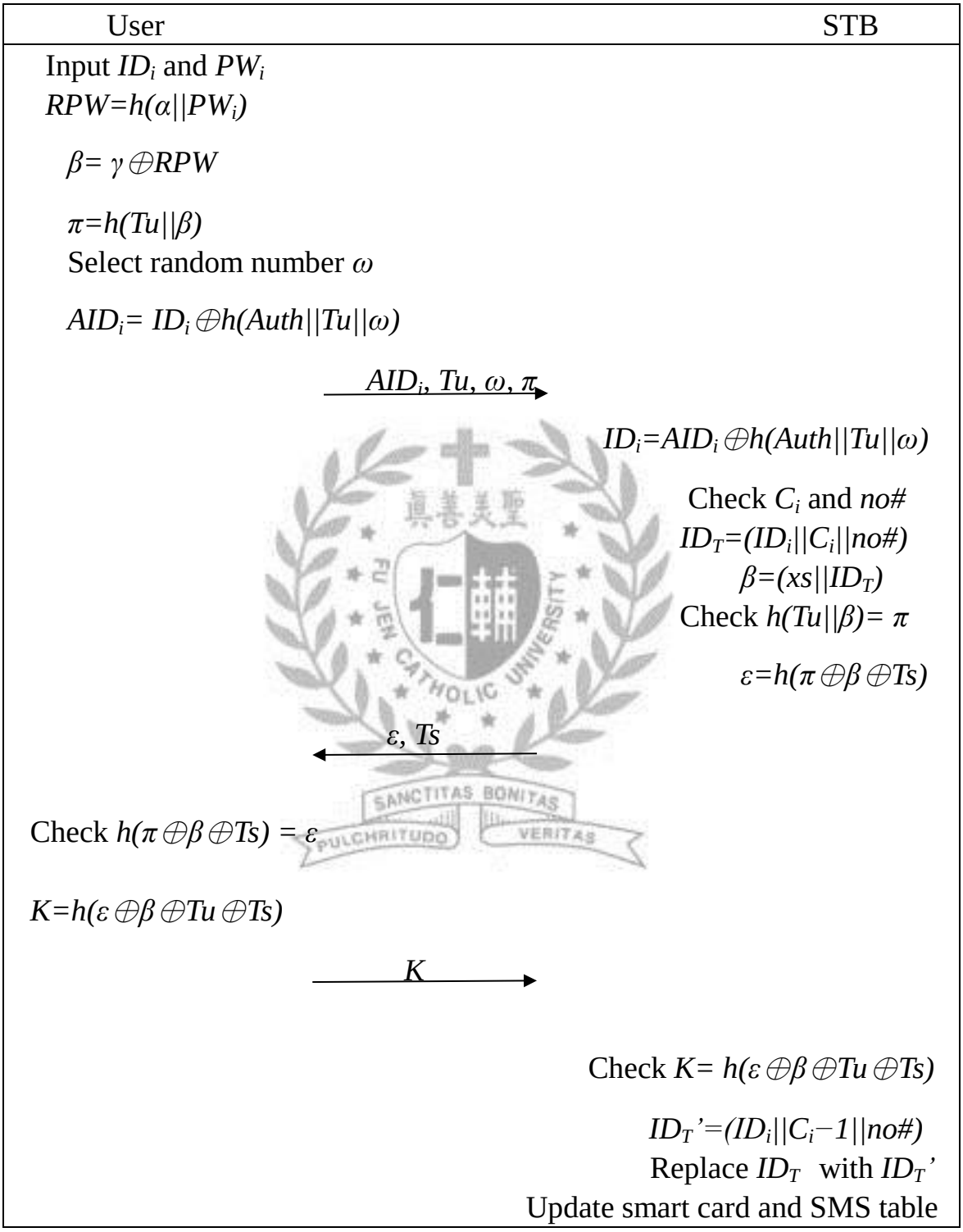

Figure 3.2.1 Login and authentication phase of the proposed protocol

3.3 Security Analysis of the Proposed Protocol

As mentioned in previous works, the following security features are critical for DTB broadcasting systems and we compare the proposed protocol with Hou et al. [11], Jiang et al. [15], Jun et al. [14], Yoon and Yoo [45] and Yoon et al. [46]. The security comparisons of the proposed protocol with other previously related protocols are given in Table 3.3.

Table 3.3 Security comparisons among the related protocols for DTV broadcasting systems

	A	B	C	D	E
Proposed protocol	O	O	O	O	O
Hou et al. [11]	O	X	X	O	X
Jiang et al. [15]	X	X	X	O	X
Jun et al. [14]	O	X	O	O	X
Yoon and Yoo [45]	O	X	X	O	X
Yoon et al. [46]	O	X	X	O	X

A: Resistance of replaying attack

B: Resistance of stolen-verifier attack

C: Provision of user anonymity and untraceability

D: Resistance of smart card cloning and stolen smart card attack

E: Provision of frequency billing service

O: Yes

X: No

3.3.1 Resistance of replaying attack

The timestamps *Tu* and *Ts* are employed in our protocol to avoid the replay attacks. We assume that an attacker may retransmit the intercepted messages $\{AID_i, Tu, \omega, \pi\}$ and $\{\varepsilon, Ts\}$ in Step 1 and Step 2 of login and authentication phase, respectively. However, the user and STB can easily detect this attack by checking timestamps *Tu* and *Ts*.

3.3.2 Resistance of stolen-verifier attack

Because SMS does not need to maintain a password table in server side and the user secures his/her password *PW* and smart card. Therefore, the proposed protocol can resist stolen-verifier attacks and provides high scalability for the user addition such that it is very practical for the applications with large number of users.

3.3.3 Provision of user anonymity and untraceability

In the proposed protocol, the user did not transmit his/her true ID_i over a public channel and the user generated AID_i instead of ID_i, where AID_i includes ID_i as $ID_i \oplus h(Auth||Tu||\omega)$. So, an attacker has no way of guessing ID_i without *Auth* and the proposed protocol can provide user anonymity and untraceability.

3.3.4 Resistance of smart card cloning

When a user's smart card is lost or stolen by an attacker, the attacker may massively duplicate the smart card and the secret information stored in the smart card may be extracted by the attacker. Since the attacker is unable to derive user's ID_i and PW_i from the smart card due to the protection of one-way hash function and the attacker does not have knowledge of STB's secret key *xs*. As a result, the proposed protocol can resist smart cloning and stolen smart card attacks.

3.3.5 Provision of frequency billing service

In the proposed protocol, the count of billing number C_i is store in user's smart card and SMS and the user needs to pass the authentication phase with STB. Moreover, after verification, STB updates old C_i with new C_i' and SMS records user's payment state in server side. Thus, the proposed billing service is suitable for DTV broadcasting systems.

3.4 Performance Analysis of the Proposed Protocol

Performance cost comparisons between the proposed protocol and other five related protocols in [11, 14, 15, 45, 46] are given in Table 3.4. Refer to Table 3; the registration phase of our proposed protocol uses two one-way hash function computations, one exclusive-OR computation and one random number. In the login phase, the proposed protocol uses three one-way hash function computations, two exclusive-OR computations, one random number and one timestamp. In the authentication and key

agreement phase, the proposed protocol uses seven one-way hash function computations, eleven exclusive-OR computations and one timestamp. For instance, as introduced in [41], one symmetric encryption/decryption is at least 100 times faster than one asymmetric encryption/decryption and one hashing operation is at least 10 times faster than a symmetric encryption/decryption in software implementation. In addition, one exponential operation is approximately equal to 60 symmetric encryptions/decryptions and it requires 0.0003s (second) to perform one one-way hashing operation, 0.0054s to perform one symmetric encryption/decryption and 0.036 to perform one point multiplication operation. In general, the computational costs of exclusive-OR operation, timestamp and random number generations are ignored because these kinds of operations have much lighter costs than one-way hash computations.

Table 3.4 Performance comparisons among the related protocols for DTV broadcasting systems

	Registration phase	Login phase	Authentication and key agreement phase
Proposed protocol	$2T(h)+1T(\oplus)+1T(r)$	$3T(h)+2T(\oplus)+1T(r)+1T(t)$	$7T(h)+11T(\oplus)+1T(t)$
Hou et al. [6]	$2T(h)+3T(\oplus)$	$3T(h)+4T(\oplus)+1T(r)+1T(e)+1T(t)$	$5T(h)+8T(\oplus)+1T(r)+1T(t)+1T(e)$
Jiang et al. [8]	$2T(h)+2T(\oplus)+1T(e)$	$2T(h)+1T(\oplus)+2T(r)+1T(e)$	$5T(h)+1T(r)+2T(e)$
Jun et al. [9]	$2T(h)+2T(\oplus)$	$2T(h)+2T(\oplus)+1T(e)$	$3T(h)+6T(\oplus)+2T(e)+2T(s)$
Yoon and Yoo [28]	$2T(h)+2T(\oplus)+1T(e)$	$2T(h)+1T(\oplus)+2T(r)+1T(e)$	$4T(h)+3T(e)+1T(r)$
Yoon et al. [29]	$1T(h)+1T(\oplus)$	$1T(h)+1T(\oplus)+1T(p)+1T(r)$	$7T(h)+1T(r)+2T(\oplus)+3T(p)$

$T(h)$: computation cost of one-way hash function

$T(\oplus)$: computation cost of exclusive-OR operation

$T(t)$: computation cost of time stamp

$T(r)$: computation cost of random number

$T(e)$: computation cost of modular exponentiation

$T(s)$: computation cost of symmetric encryption

$T(p)$: computation cost of point multiplication

Refer to Table 3.4.1, 640$T(h)$ are required for Hou et al.'s protocol, 2429$T(h)$ are required for Jiang et al.'s protocol, 3028$T(h)$ are required for Yoon et al.'s protocol, 1847$T(h)$ are required for Jun et al.'s protocol, 509$T(h)$ are required for Yoon et al.'s protocol and 32$T(h)$ are required for our proposed protocol. Obviously, in the proposed protocol, the total computational time of our protocol is lower than most of comparison protocols.

On the other hands, we present our evaluation results in this thesis. DTV broadcasting protocols proposed in the literatures can be categorized into those based on RSA and ECC. We compare the proposed DTV protocol with the best protocols in each category. All protocols were done on four-core 3.0-GHz machine with 16-GB memory and the results were averaged over 500 randomized simulation runs. Experimental evaluations were implemented on our simulator written in MATLAB. Detailed results of computation costs are presented in Figure 3.4.

Table 3.4.1 Comparisons of total computation time among the related protocols for DTV broadcasting systems

	Registration phase	Login phase	Authentication and key agreement phase	Total operations	Total computation time
Proposed protocol	0.00062s	0.00063s	0.00242s	32$T(h)$	0.00367s
Hou et al.[11]	0.00063s	0.18092s	0.00455s	640$T(h)$	0.1861s

Jiang et al.[15]	0.18062s	0.18062s	0.36121s	2429$T(h)$	0.72245s
Jun et al. [14]	0.00061s	0.18061s	0.36093s	1847$T(h)$	0.54154s
Yoon et al.[45]	0.18064s	0.18062s	0.54153s	3028$T(h)$	0.90279s
Yoon et al.[46]	0.00060s	0.03632s	0.14521s	509$T(h)$	0.18213s

s: second

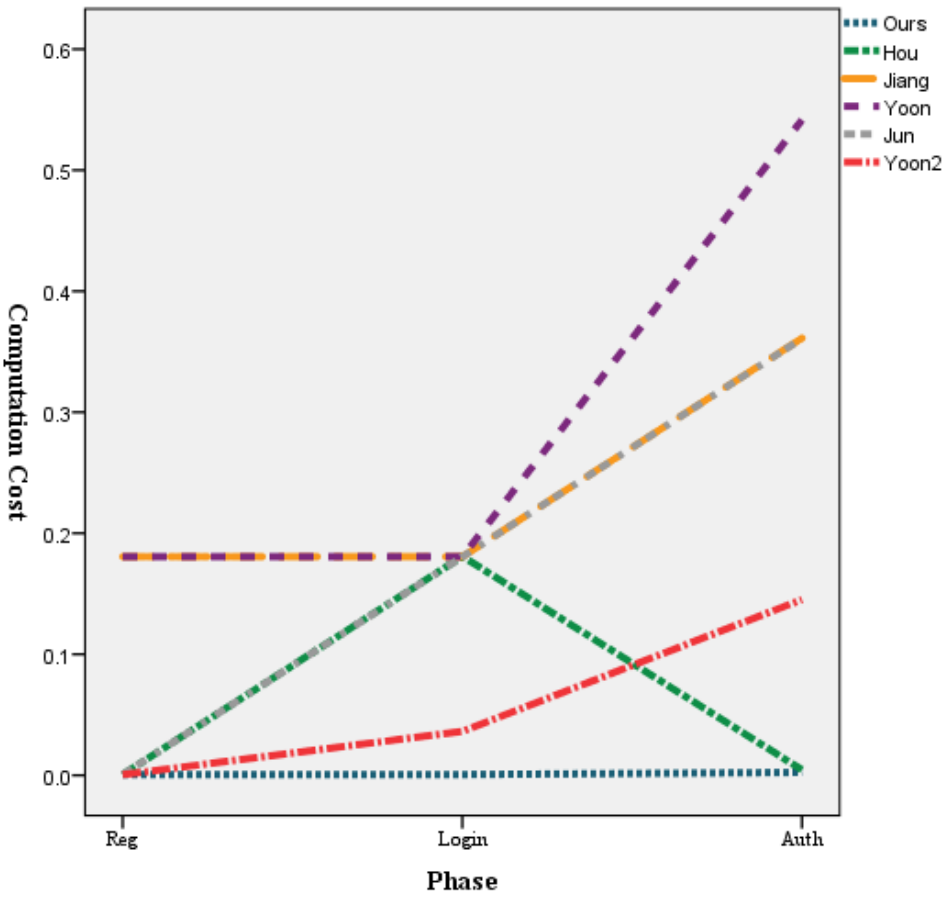

Figure 3.4 Performance evaluations

Chapter 4

A Practical RFID Authentication Mechanism for Digital Television

As information technology continuously progresses, more applied technologies are developed, such as radio frequency identification (RFID). In this thesis, we propose a novel digital television (DTV) structure that uses RFID for encryption. RFID is widely used for various applications because of its advantages such as an extended lifetime and security, and it is less affected by environmental constraints. The proposed mechanism uses RFID for encryption to withstand many attacks that the traditional system is vulnerable to, such as impersonation attack, replay attack and smart card cloning. Compared with other protocols, the proposed protocol is more secure and efficient. Thus, our proposed mechanism makes the DTV framework more complete and secure.

4.1 Preliminary

RFID was launched in 1940 and is currently used extensively every day for many applications. Tags are used in various areas, such as supply chain management, health care, and manufacturing. RFID encryption security is important because RFID forms part of network transmission. In a network environment, many security issues must be resolved, such as man-in-the-middle attack [5], spoofed tag attack [9], replay attack, mutual

authentication [6], and location privacy [7]. Mutual authentication protocol is essential for data transmission.

RFID and smart card are two popular technologies for market participants. Digital television (DTV) encryption protocols usually use smart cards for encryption [4, 10, 17, 22, 23]. In our proposed protocol, we use RFID to replace smart card for encryption due to its low-cost designs and high volume manufacturing to minimize investment required in implementation [26]. The difference between the design of authentication protocols in RFID-based systems and that in smart card-based systems is as follows [34]. RFID-based systems have common characteristics, including low cost, minimal security, minimal data storage, and read range optimized to increase speed and utility. Smart card-based systems have common characteristics, including mutual authentication, strong information security, strong contactless device security, authenticated and authorized information access, and support for information privacy [21, 35, 36, 48]. Compared with previous protocols based on smart cards, we provide better choice to enhance the security of the system using RFID technology. In general, users use the set-top box (STB) to watch television over a wired network at home. With the proposed protocol, users can watch TV over a wireless network after passing the RFID authentication process. There are many benefits to this approach. For example, when a user is outdoors, by using RFID tags for authentication, the user can watch TV in the car over a wireless network. Figure 4.1 shows the structure of our proposed DTV protocol. The proposed structure enables users to use wireless networks to watch TV in places where they cannot do it before. First, a user must use the RFID tag and enter his/her password to be authenticated by the RFID reader. Once the user is authenticated, he/she can watch TV through a wireless network. This research allows DTV to develop more applications and satisfy user

requirements in the future.

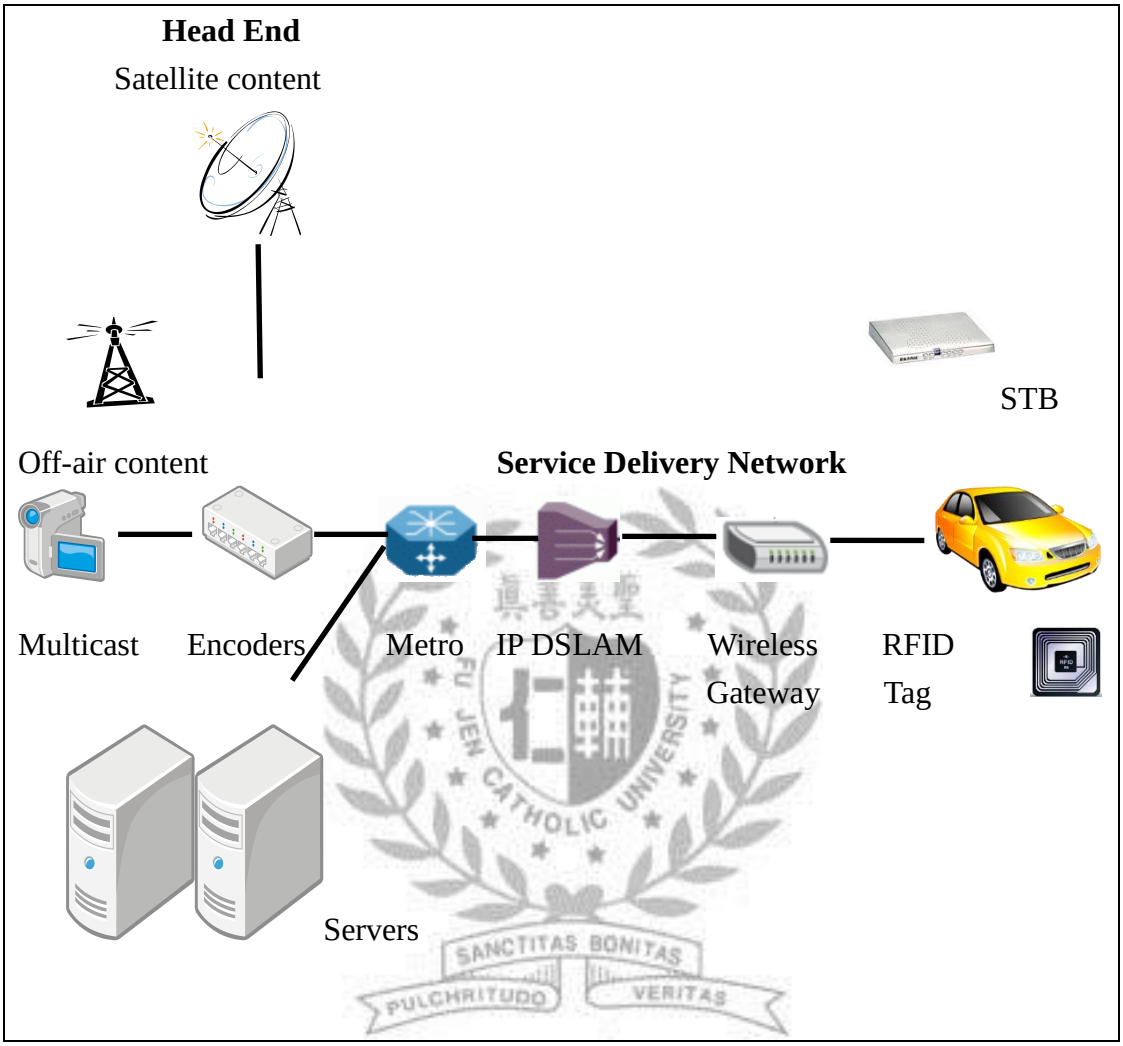

Figure 4.1 The structure of the proposed DTV protocol

4.2 Proposed Protocol

This section introduces the proposed protocol. There are three components in the proposed protocol:

1. Tag: for identification as accessed by the radio frequency signal
2. Reader: for tag access
3. Subscriber management system (SMS): back-end database server

responsible for recording all tag details

The notations used throughout this chapter are defined as follows:

- tag_i: The tag of user
- TID_i: The tag ID of user
- R: Tag reader
- $\oplus$: Bitwise exclusive-or operation
- ID_i: Identity of user
- PW_i: Password of user
- $h(\cdot)$: One-way hash function
- xs: Secret key of STB
- $||$: String concatenation
- $E_{TKIP}()$: TKIP (temporal key integrity protocol) encryption function
- MIC: Integrity code to verify the integrity
- $Auth$: Shared value between the R, STB, and SMS
- T_s, T_j: Timestamp
- $RFTag\{\ \}$: Write data into tag

4.2.1 Registration phase

Before using the DTV system, the user must perform registration to the SMS. The steps of the registration phase are as follows and shown in Figure 4.2:

Step 1: The user provides the password $h(PW_i)$ and user identity (ID_i) to the SMS server for registration.

Step 2: When the SMS server receives the password $h(PW_i)$ and the user identity (ID_i), it computes B_i and C_i as follows:

$$B_i=h(h(xs)||TID_i) \oplus Auth$$

$$C_i=B_i \oplus h(PW_i)$$

Where xs is a STB secret key generated by the SMS, and TID_i is a tag ID of user. The user can change his/her TID_i once login and authentication are complete.

Step 3: The SMS server stores $\{ID_i, C_i\}$ into the RFID tag and sends the tag to the user through a secure channel.

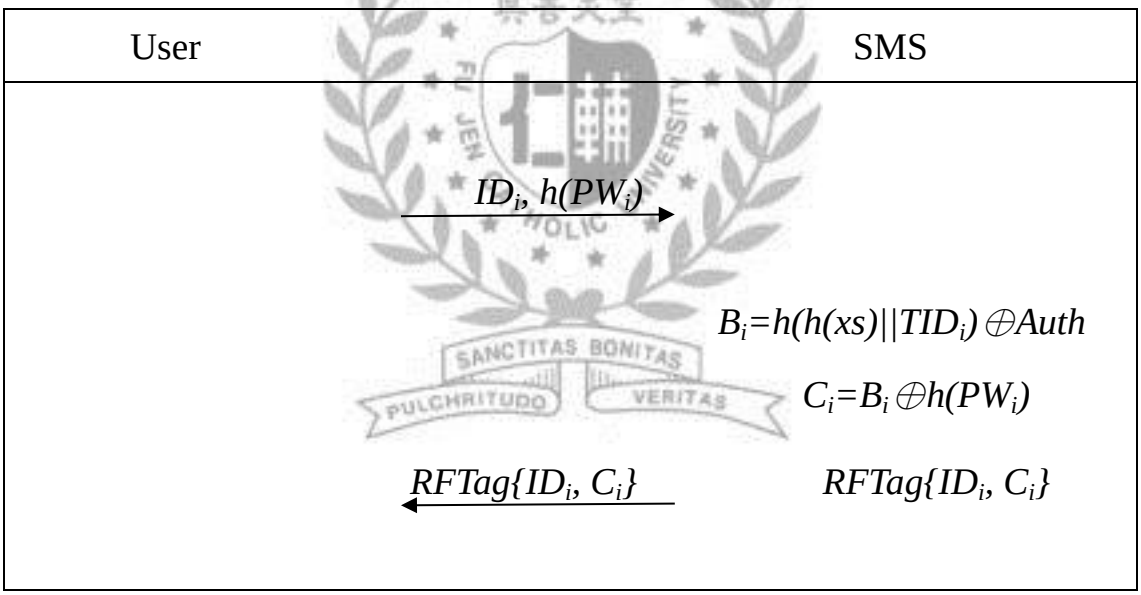

Figure 4.2 Registration phase

4.2.2 Login and authentication phase

When users want to use the DTV system, they must complete the mutual authentication with the STB. They can use ID_i, PW_i, and the RFID tag to pass authentication by performing the following steps:

Step 1: The user uses the RFID tag and inputs the correct user PW_i. The reader reads the user ID_i, tag_i and C_i. The user provides $h(PW_i)$ to the reader. Then, the reader computes B_i and D_i as follows:

$$B_i = C_i \oplus h(PW_i)$$

$$D_i = h(T_s || B_i) \oplus Auth$$

After computing B_i and D_i, the reader sends the encryption message $E_{TKIP}(TID_i || D_i || T_s) \,||\, MIC$ to the STB.

Step 2: When the STB server receives the encryption message, it confirms the integrity of the MIC, computes $B_i' = h(h(xs) || TID_i) \oplus Auth$, $D_i' = h(T_s || B_i') \oplus Auth$ and determines whether D_i' equals D_i. If true, the STB receives the login request, computes $E_i = h(D_i' \oplus B_i' \oplus T_j) \oplus Auth$, and sends encryption message $E_{TKIP}(E_i || T_j) || MIC$ to the reader. T_j is a timestamp created by the STB.

Step 3: When the reader receives the encryption message from the STB, it confirms the integrity of the MIC, computes $E_i' = h(D_i \oplus B_i \oplus T_j) \oplus Auth$, and determines whether E_i' equals E_i. If correct, mutual authentication of the user and STB is complete.

The steps of this phase are shown in Figure 4.3.

4.2.3 Key agreement phase

If the user and STB pass the mutual authentication phase, the user uses the shared value to compute a common session key *SK*, as follows:

$SK=h(B_i, E_i, T_s, T_j)$

4.2.4 Control word transmission phase

After decrypting the control word (*CW*) in conditional access system, the user can use *SK* to encrypt *CW* as $CW_e=E_{SK}(CW)$, and sends CW_e to the STB. The STB can decrypt *CW* as $CW=E_{SK}^{-1}(CW_e)$. The user can use *CW* to watch subscribed programs.

4.2.5 Password exchange phase

If a user wants to change his/her password, he/she must first pass the login and authentication phase. The user should do the same procedure as registration phase and provide the new password $h(NPW_i)$ and user identity (ID_i) to the SMS. Then, the user can obtain the new tag $RFTag\{ID_i, C_i\}$ from the SMS.

4.3 Security Analysis of the Proposed Protocol

In this section, we will present security analysis of the proposed protocol and compares the proposed protocol with other related protocols [11, 14, 15, 45, 46] in terms of functionality and efficiency. Table 4.3 shows the security comparison between the proposed protocol and the existing

protocols.

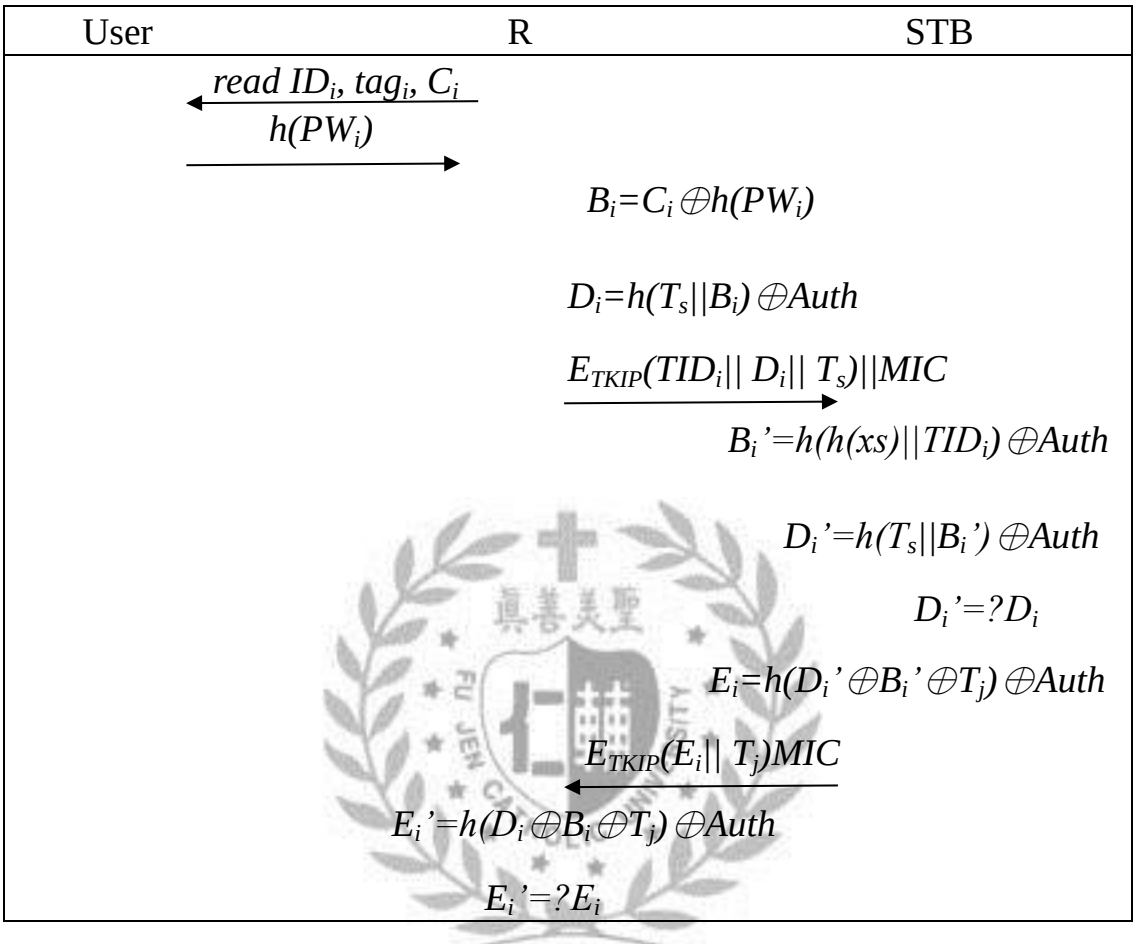

Figure 4.3. Login and authentication phase

4.3.1 Impersonation attacks

Impersonation attacks mean that an attacker can impersonate a legal user to login the system [27], or an attacker can impersonate a legal server to cheat a user. The latter is also called spoofing attacks. If an attacker wants to login our system, he/she must prepare the login message $E_{TKIP}(TID_i||D_i||T_s)||MIC$. However, the attacker cannot compute the login message without knowing C_i, PW_i, B_i, and $Auth$. Here, T_s is the timestamp of the login message. If a masquerading STB attempts to cheat the

requested RFID tag, it must prepare a valid reply message $E_{TKIP}(E_i||T_j)MIC$. However, it is infeasible to derive the value $E_{TKIP}(E_i||T_j)MIC$ and to generate E_i without knowing $D_i' \oplus B_i' \oplus T_j$. Therefore, our protocol can resist against impersonate attacks.

4.3.2 Smart card cloning

The proposed protocol is also resistant to smart card cloning. The proposed protocol uses RFID tag to replace the smart card. Unlike smart cards, RFID tags cannot be replicated, and each RFID tag label is unique. In [24], Lehtonen et al. have proposed an effective way to secure RFID systems against tag cloning. We can use their approach to prevent the tag cloning. Therefore, our RFID tag can resist against smart card cloning.

4.3.3 Mutual authentication

The proposed protocol provides explicit mutual authentication between the user and the STB. In Step 2 of the login and authentication phase, the STB computes $D_i'=h(T_s||B_i') \oplus Auth$ and determines whether D_i' equals D_i. If equal, the STB confirms the legitimate user. Only a legitimate user has a PW_i and C_i. Therefore, the STB authenticates user, and no one can forge the user. Users can also ensure that they are communicating with a legitimate STB by confirming that $E_i'=E_i$ in Step 3.

4.3.4 Replaying attacks

In our protocol, timestamps T_s and T_j are used to avoid replay attacks. If an attacker retransmits intercepted requests TID_i, D_i, and Ts in Step 1 and E_i, T_j in Step 2, the user and the STB can easily detect this by checking the timestamps [23].

4.3.5 Stolen-verifier attacks

Because the SMS does not store password verification tables, the proposed protocol can resist stolen-verifier attacks. In the proposed protocol, user only keeps password PW and the RFID tag and uses them for user authentication. The proposed protocol can prevent stolen-verifier attacks and provides high scalability for user additions, making it practical for large number of user [6]s.

4.3.6 McCormac Hack attacks

When an adversary redirects an RFID tag communication message to another STB, the STB has no information of session key without mutual authentication and key exchange. Therefore, the STB cannot decrypt the message redirected from the RFID tag [45].

Table 4.3 Security comparison between the proposed protocol and other related protocols

	A	**B**	**C**	**D**	**E**	**F**
Proposed protocol	O	O	O	O	O	O
Hou et al. [11]	X	O	X	O	X	X
Jiang et al. [15]	X	O	X	X	X	X
Yoon and Yoo [45]	X	O	O	O	X	X
Jun et al. [14]	O	O	X	O	X	O
Yoon et al. [46]	X	O	O	O	X	X

A: Impersonation attacks

B: Smart card cloning

C: Mutual authentication

D: Replaying attacks

E: Stolen-verifier attacks

F: McCormac Hack attacks

O: Yes

X: No

4.4 Performance Analysis of the Proposed Protocol

To provide better performance, the computing in each phase should require less time complexity. The previous section shows that the proposed protocol has more security, integrity and resistance to security

attacks. This section presents the performance advantages of the proposed protocol and compares it with other related protocols. Table 2 shows the performance comparison between the proposed protocol and other related protocols.

4.4.1 A verifier table is not required

In the proposed protocol, the server does not have to store the verification table. It results in rapid data access and means that private data are not stored on the server, thus improving security. In addition, users can select their own password in our proposed protocol. The server does not store and create user passwords. This enhances the speed of data transfer, and the server does not search for the user data from the database. This also enhances security, because private data do not exist on the server.

4.4.2 Message integrity is guaranteed

TKIP is an encryption protocol included as part of the IEEE 802.11i standard for wireless LANs (WLANs) [12]. It is used to achieve message integrity. The proposed protocol also uses the TKIP encryption technology in wireless networks. This protects data transfer security and is more efficient than other encryption technology.

4.4.3 Users can write messages on tags in the assigned sector and block

In proposed protocol, users can write data to the RFID tag. This improves efficiency because users can modify label data without going through a server. This saves user time and server load.

4.4.4 Exchanged messages are encrypted

The proposed protocol can provide that the exchanged messages are encrypted using TKIP encryption technology. This provides users with a high degree of security and an efficient transmission speed.

4.4.5 Transmission performance

The proposed protocol uses low-complexity computing, such as XOR, concatenation symbols and hashes. These encryption methods are efficient, and the proposed protocol can provide more efficient transmission than other protocols. Table 4.4 shows the comparison of the computation costs of other protocols.

Table4.4 Performance comparison between the proposed protocol and other related protocols

	Registration phase	Login phase	Authentication and key agreement phase
Proposed protocol	*2T(h)+2T(⊕)*	*1T(h)+2T(⊕)+ 1T(t)*	*6T(h)+8T(⊕)+1T(t)*
Hou et al. [11]	*2T(h)+3T(⊕)*	*3T(h)+4T(⊕)+ 1T(r) +1T(e)+1T (t)*	*5T(h)+8T(⊕)+1T (r) +1T(t)+1T(e)*
Jiang et al. [15]	*2T(h)+2T(⊕) +1T(e)*	*2T(h)+1T(⊕) +2T(r)+1T(e)*	*5T(h)+1T(r)+2T(e)*
Yoon and Yoo [45]	*2T(h)+2T(⊕) +1T(e)*	*2T(h)+1T(⊕)+ 2T(r) +1T(e)*	*4T(h)+3T(e)+1T(r)*
Jun et al. [14]	*2T(h)+2T(⊕)*	*2T(h)+2T(⊕)+ 1T(e)*	*3T(h)+6(⊕)+2T(e)+ 2T(s)*
Yoon et al. [46]	*1T(h)+1T(⊕)*	*1T(h)+1T(⊕)+ 1T(r) +1T(e)*	*7T(h)+1T(r)+2(⊕) +3T(e)*

T(*h*): computation cost of one-way hash function

T(⊕): computation cost of exclusive-OR operation

T(*t*): computation cost of time stamp

T(*r*): computation cost of random number

T(*e*): computation cost of modular exponentiation

T(*s*): computation cost of symmetric encryption

Chapter 5
Conclusions

In this thesis, we focused on the above three DTV protocols. In Chapter 2, we showed that the mechanism of Yoon et al. could not prevent replay attacks and man-in-the-middle attacks, and the identity of users was not anonymous. We proposed a security and anonymity key exchange protocol for IPTVs, which employs timestamps to prevent replay attacks, and uses the Diffie-Hellmen key technique to protect the privacy of the STB and users. This study proved that the protocol can achieve anonymity and resist certain attacks. Therefore, the proposed mechanism is suitable for use in IPTVs.

In Chapter 3, we propose a billing service in DTV system, user charging is one of the important issues in DTV broadcasting system that needs to be adequately addressed. In this thesis, we propose a frequency billing protocol in DTV broadcasting system. We analyze the proposed protocol with other related protocols in terms of security and performance. In brief, compared with the other related protocols, while providing relatively more security features, our proposed protocol not only provides much better security features but also achieves much higher performance efficiency. As a result, the proposed protocol is well suited for DTV broadcasting systems with low-power computing devices.

In the Chapter 4, we propose an RFID authentication system for

DTV. The proposed DTV system is different from the traditional system. Traditional DTV encryption uses smart cards, but the proposed protocol uses RFID for encryption. This provides improved security and convenience. Compared with other protocols, the proposed protocol is more secure and efficient. Moreover, the proposed protocol also allows users to watch TV in locations other than their homes. Finally, the proposed protocol enables the development of more convenient and secure DTV. In future work, we will add some new features for IPTV, like cloud DTV system, biometric- based STV system, VANET system for DTV, this will make more extensive for DTV development.

References

[1] E. Cruselles, J. L. Melus, and M. Soriano, “An overview of security in Eurocrypt conditional access system,” *IEEE Global Telecommunications Conference*, vol. 1, pp. 188–193, 1993.

[2] M. G. Chung, Member, and Y. Kim, “An integrated scheme for authentication and access control in a digital TV environment,” *IEEE International Conference on Consumer Electronics*, pp. 1-2, 2008.

[3] T.H Chen, G. Horng, and C.S. Yang, “Public key authentication schemes for local area networks,” *Informatica*, vol. 19, no. 1, pp. 3-16, 2008.

[4] Y. Y. Chen, M. L. Tsai, and J. K. Jan, “The design of RFID access control protocol using the strategy of indefinite-index and challenge-response,” *Computer Communications*, vol. 34, no. 3, pp. 250-256, 2011.

[5] H. Y. Chien, “Secure access control schemes for RFID systems with anonymity,” *in Proceedings of the 7th International Conference on Mobile Data Management*, pp. 96-96, 2006.

[6] H. Y. Chien, “SASI: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity,” *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 3, pp. 337-340, 2007.

[7] H. Y. Chien, and C. H. Chen, “Mutual-authentication protocol for RFID conforming to EPC class 1 generation 2 standards,” *Computer Standards & Interfaces*, vol. 29, no. 2, pp. 254-259, 2007.

[8] W. Diffie and M. E. Hellman, “New directions in cryptography,” *IEEE Transaction on Information Theory*, vol. 22, no.6, pp. 644-654, 1976.

[9] T. Dimitriou, “A lightweight RFID protocol to protect against traceability and cloning attacks,” *in Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pp. 59-66, 2005.

[10] M. Garcia, A. Canovas, M. Edo, and J. Lloret, “A QoE management system for ubiquitous IPTV devices,” *IEEE International Conference on Mobile Ubiquitous Computing*, pp.147-152, 2009.

[11] T. W. Hou, J. T. Lai, and C. L. Yeh, “Based on cryptosystem secure communication between set-top box and smart card in DTV broadcasting,” *IEEE Region 10 Conference TENCON*, pp.1-5, 2007.

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

[13] M. S. Hwang, C. C. Lee, J. Z. Lee, and C. C. Yang, “A secure protocol for bluetooth piconets using elliptic curve cryptography,” *Telecommunication Systems*, Vol. 29, No. 3, PP. 165-180, July 2005.

[14] E. Jun, H. S. Rhee, S. W. Jung, and D. H. Lee, “A fingerprint-based user authentication scheme using smart cards in IPTV environments,” *IEEE International Conference on Information Science*, pp. 1-8, 2010.

[15] T. Jiang, Y. Hou, and S. Zheng, “Secure communication between set-top box and smart card in DTV broadcasting,” *IEEE Transaction on Consumer Electronics*, vol. 50, no. 3, pp. 882-886, 2004.

[16] T. Jiang, S. Zheng, and B. Liu, "Key distribution based on hierarchical access control for conditional access system in DTV broadcast," *IEEE Transaction on Consumer Electron*ics, vol. 50, no.1, pp. 225-230, 2004.

[17] N. Kogan, Y. Shavitt, and A. Wool, "A practical revocation scheme for broadcast encryption using smart cards," *IEEE Transactions on Information and System Security*, vol. 9, no. 3, pp. 325-351, 2006.

[18] F. Kamperman and B. V. Rijnsoever, "Conditional access system interoperability through software downloading," *IEEE Transaction on Consumer Electron*ics, vol. 47, no.1, pp.47-53, 2001.

[19] W. Kanjanarin and T. Amornraksa, "Scrambling and key distribution scheme for digital television," *IEEE International Conference on Networks*, pp. 140-145, 2001

[20] T. Kim and H. Bahn , "Implementation of the storage manager for an IPTV set-top box," *IEEE Transactions on Consumer Electronics*, vol. 54, no. 4, pp. 1770-1775, 2008.

[21] S. Y. Kang, D. G. Lee, and I. Y. Lee, "A study on secure RFID mutual-authentication scheme in pervasive computing environment," *Computer Communications*, vol. 31, no. 18, pp. 4248-4254, 2008.

[22] C. C. Lee, C. T. Li, T. Y. Chen, P. H. Wu, and C. T. Chen, "A new key exchange protocol with anonymity between STB and smart card in IPTV broadcasting," IEEE *International Conference on Wireless Communications, Networking and Mobile Computing (WiCom 2011)*, pp. 23-25, 2011.

[23] J. S. Lee, H. S. Rhee and D. H. Lee, "Efficient and secure communication between set-top box and smart card in IPTV broadcasting," *IEEE International Conference on Convergence and*

Hybrid Information Technology, pp. 307-310, 2008.

[24] P. Y. Lau, S. Park, J. Yoon, J. Lee, "Pay-as-you-use on-demand cloud service: *an IPTV case*," *IEEE International Conference on Electronics and Information Engineering*,vol. 1, pp. 272- 276, 2010.

[25] W. B. Lee, H. B. Chen and C. C. Cheng, "Secure communication between set-top box and smart card for fair use in DTV broadcasting," *IEEE International Conference on Intelligence and Security Informatics*, pp. 156 – 158, 2010.

[26] S. M. Lee, Y. J. Hwang, D. H. Lee, and J. I. Lim, "Efficient authentication for low-cost RFID systems," *International Conference on Computational Science and its Applications*, pp. 619-627, 2005.

[27] C. C. Lee, I. E. Liao, and M. S. Hwang, "An efficient authentication protocol for mobile communications," *Telecommunication Systems*, vol. 46, no. 1, pp. 31-41, 2011.

[28] M. Lehtonen, D. Ostojic, A. Ilic, and F. Michahelles, "Securing RFID systems by detecting tag cloning," *Proceedings of the 7th International Conference on Pervasive Computing*, pp. 291-308, 2009.

[29] B. Macq and J. Quisquater, "Cryptology for digital TV broadcasting," *Proceedings of the IEEE*, vol. 83, no. 6, pp. 944-957, 1995.

[30] J. Moon, J. Kim, J. Park, E. Paik, and K. Park, "A dynamic conditional access system for IPTV multimedia systems," *IEEE International Conference on Systems and Networks Communications*, pp. 224-229, 2009.

[31] J. Moon, J. Kim, J. Park, and E. Paik, "Achieving interoperability in conditional access systems through the dynamic download and

execution of cryptographic software for the IPTV system," *IEEE International Conference on Convergence and Hybrid Information Technology*,vol. 2, pp. 380-385, 2008.

[32] N. Prasertsatid, "Implementation conditional access system for pay-TV based on java card," *IEEE Conference on Computational Electromagnetic and its Application* in *3rd*, 2004.

[33] S. Park and S. Jeong, "Mobile IPTV: approaches, challenges, standards, and QoS support," *IEEE Internet Computing*, vol. 13, no. 3, pp.23-31, 2009.

[34] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "The evolution of RFID security," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 62-69, 2006.

[35] C. M. Roberts, "Radio frequency identification (RFID)," *Computers & Security*, vol. 25, no. 1, pp. 18-26, 2006.

[36] P. Rotter, "A framework for assessing RFID system security and privacy risks," *in IEEE Pervasive Computing* , vol. 7, no. 2 pp. 70-77, 2008.

[37] K. Shim, "Cryptanalysis of mutual authentication and key exchange for low power wireless communication," *IEEE Communication Letters*, vol. 7 , no. 5, pp.248-250, 2003.

[38] H. Shirazi, J. Cosmas, and D. Cutts, "A cooperative cellular and broadcast conditional access system for Pay-TV systems," *IEEE Transactions on Broadcasting*, vol. 56, no. 1, pp. 44-57, 2010.

[39] E. Shihab, F. Wan, L. Cai, A. Gulliver and N. Tin, "Performance analysis of IPTV traffic in home networks," *IEEE Global Telecommunications Conference*, pp. 5341-5345, 2007.

[40] C.P. Schnorr, “Efficient identification and signatures for smart cards,” *In Crypto’89 LNCS*, vol. 434, pp. 688-689 1990.

[41] B. Schneier, Applied Cryptography, Protocols, Algorithms, and Source Code in, second ed., C. John Wiley and Sons Inc., 1996.

[42] F. K. Tu, C. S. Laih, and H. H. Tung, “On key distribution management for conditional access system on pay-TV system,” *IEEE Transaction on Consumer Electron*ics, vol. 45, no. 1, pp. 151-158, 1999.

[43] D. S. Wong and A. H. Chan, “Mutually authentication and key exchange for low power wireless communications,” *IEEE Military Communications Conference*, vol. 1, pp. 39-43, 2001.

[44] J. S. Wey, J. Lüken, and J. Heiles, “Standardization activities for IPTV set-top box remote management,” *IEEE Internet Computing*, vol. 13, no. 3, pp. 32-39, 2009.

[45] E. J. Yoon and K. Y. Yoo, “Robust key exchange protocol between set-top box and smart card in DTV broadcasting,” *Institute of Mathematics and Informatics*, vol. 20, no. 1, pp. 39-150, 2009.

[46] E. J. Yoon and K. Y. Yoo, “ECC-based key exchange protocol for IPTV service,**”** *IEEE International Conference on Information Science*, pp. 547-552, 2011.

[47] E. J. Yoon and K.Y. Yoo, “A new secure key exchange protocol between STB and smart card in DTV broadcasting,” *WISI 2006, LNCS 3917, Springer,* pp. 165-166, 2006.

[48] X. Yan and X. Liu, “Evaluating the energy consumption of the RFID tag collision resolution protocols,” to appear in *Telecommunication Systems*, doi: 10.1007/s11235-011-9563-8, 2011.

[49] Y. Zhu, W. Liu, L. Dong, W. Zeng and H. Yu, “High performance adaptive video services based on bitstream switching for IPTV systems,” *IEEE Consumer Communications and Networking Conference*, pp. 1-5, 2009.