

天主教輔仁大學圖書資訊學系碩士班碩士論文

指導老師：李正吉 博士

數位版權管理系統隱私權保護

應用於行動裝置之研究

**The Study on Privacy Protection of
Digital Rights Management for Mobile Devices**

研究生：陳致瑋 撰

中華民國一〇六年六月

私立輔仁大學圖書資訊學系碩士班
論文口試委員會審定書

陳致瑋 先生之碩士學位論文

數位版權管理系統隱私權保護應用於
行動裝置之研究

The Study on Privacy Protection of Digital Rights Management for
Mobile Devices

經本委員會審議合格，特此證明。

論文口試委員

指導老師

謝建成 (召集人)

李正吉

謝建成

李正吉

李俊達

李俊達

系主任

黃元鶴

黃元鶴

中華民國 106 年 06 月

誌謝(ACKNOWLEDGEMENTS)

時光荏苒，在圖書資訊學系短短兩年的時光一下子就過了，這當中真的要感謝的人太多了。首先，非常感謝我的指導老師，李正吉老師。經由老師悉心指導，得以在兩年的時間窺見資訊安全的學海。老師的指導不僅在學術上，更在生活中指引了方向，對於事情的嚴謹性、細心度經由老師的指導更加謹慎。能夠順利在兩年內完成碩士論文，真的非常感謝李正吉老師的幫助，謝謝老師。也非常謝謝賴彥銘學長，在研究上給我相當多的經驗談，也提供許多意見，並且幫助了論文的產生，謝謝麵包學長。另外，也要感謝我的兩位口試老師，謝建成老師與李俊達老師。老師們給予的建議更加完整了這本碩士論文，讓論文更臻完善。

圖書資訊學科對我來說是一片新天地，大學非本科系出身的我，對於圖資領域一知半解，經由課堂教授們的教導，引領我發現這片天地的事物。這當中我最想要感謝的是張淳淳老師、林呈漢老師。兩位老師在圖資領域都是非常優秀的人才，能夠在兩位老師退休前上到有關圖資相關的課程，真的非常幸運。謝謝圖資系的助教，靜宜、小童、懷倫、慶華，不論是在公事或是私事，四位助教都很照顧我們研究生，謝謝你們的幫助。十分感謝系上所有的老師，在我剛踏入碩士班的那年，因家中發生重大事故，系上的那時幫助對我來說非常重要，也讓我感受到系上的溫暖，謝謝圖資系，兩年前選擇圖資系真的是很棒決定。

再來，要感謝我的同學們維恩、靜蓮、彤玲、凱茵、郡慧以及翎絃學姊、家妘學姊、立安學長、志雍，我們一起共度這兩年的時光很難忘，沒有你們的陪伴、打氣與幫助，研究所生活不會如此豐富與光彩，畢業後，我會非常懷念這段時光。謝謝我的論文小夥伴，仲倫，我們一起 meeting、一起討論、一起度過了寫論文的時光，沒有彼此的激勵，我想我的論文無法順利完成，謝謝。

最重要的要感謝我的家人與好友，謝謝我的家人包容我所有的一切，壓力大時的暴躁脾氣、心情低落時的難過心情，謝謝我們家人給我最棒的環境讓我無顧

慮的完成碩士學位。謝謝我的好友們，特別是瑞玢、慧真、張平、培藝、翊如，你們的鼓勵是我前進的動力之一，你們的陪伴、玩樂是我充電重要來源，謝謝你們，也恭喜我們一起完成了碩士論文！

最後，也是我最要感謝的是我的媽媽，從小到大媽媽都沒有侷限我，對於我也是百分之百的信任，讓我嘗試許多事情。雖然媽媽沒有辦法親眼看到我拿到畢業證書，但我相信她一定是很高興與驕傲的。我還是完成了碩士學位，我沒有讓妳失望，謝謝媽媽 23 年養育之恩，我愛妳。

未來的生活藍圖雖然充滿挑戰，但這兩年的生活扎扎实實的充實了我，謝謝輔仁大學，謝謝圖資系的所有人事物，謝謝大家。



陳致瑋 謹誌於輔仁大學

2017 年 7 月

中文摘要

隨著科技的日新月盛，許多應用技術因應而生。現今，絕大部分的圖書文本、多媒體資料或是其他形式的軟體皆以數位的方式來儲存；傳統的內容資料，如紙本資料、音樂錄影帶等，也陸續將其數位化並且數位管理。透過網際網路的傳輸，各式各樣的數位內容以驚人的速度傳遍世界各地。然而，這樣的便捷也帶來了許多安全疑慮以及數位內容的隱私和版權保護問題。數位版權管理(Digital Rights Management, 以下簡稱 DRM)系統是一套限制受保護數位內容使用、修改和分發的讀取控制之技術，因此如何透過 DRM 系統來保護數位內容的隱私是一項重要的議題。另一方面，因應科技的發展趨勢，行動設備的設計被要求更短小輕薄並且提供人們能夠隨時隨地使用。因此，人們透過行動裝置來使用數位內容的機會大幅提高，DRM 系統也應該要能支援行動裝置的數位內容訪問。

本論文中，我們分析近幾年應用於 DRM 系統的相關研究，且因應行動裝置的需求，在 DRM 系統通訊協議中加入了生物特徵以及橢圓曲線密碼學的數學原理，透過生物特徵的認證使用者機制以及橢圓曲線密碼學的低運算成本來提出新的協議方案，以提高系統的安全和效率。提出之協議方案可分為三部分：(1) 克服 Mishra 等學者提出基於生物特徵的 E-DRM 協定所存在的使用者匿名問題和數位內容儲存問題，並提出更優越的機制；(2) 改良 Jung 等學者所提出基於生物特徵的醫療系統協議之伺服器密鑰竊取問題與使用者匿名問題，並且提出適用於 DRM 環境的機制；(3) 透過改良 Amin 等學者所提出基於 ECC 原理之雲端運算環境協議，提出低運算成本的 DRM 機制。上述三部分會根據安全性與效率分析證明，我們所提出的機制相較於過去的方法顯得更加安全及更有效率，並且更能應用在 DRM 系統。

關鍵詞：讀取控制、生物特徵、數位版權管理系統、橢圓曲線密碼學、行動裝置

ABSTRACT

With the rapid development of science and technology, many application technology was born. Today, most of the books, multimedia materials or other forms of software are digital stored; traditional content (such as paper materials, music videos, etc.,) will also be converted into digital contents. Through transmission by Internet, a wide range of digital contents at an alarming rate spread around the world. However, the convenience of the Internet has also brought a lot of security concerns and digital content privacy and copyright protection issues. Digital rights management system (DRM system) is a set of technologies that limit the use, modification and distribution of protected digital content. Therefore, how to protect the privacy of digital content using DRM system is an important issue. Besides, in response to the development trend of technologies, mobile devices are designed to be smaller and lighter. Mobile devices also offer greater convenience for people. As a result, the chances of using digital content on mobile devices are significantly increased by mobile users. So, we think that the DRM system should also be able to support the access of digital content on mobile devices.

In this study, we will analyze the related works on DRM system in recent years. And in response to the demand of mobile devices, the mathematical principle of biometrics and elliptic curve cryptography are added to DRM system communication protocol. Through the biometric-based user authentication mechanism and the low computational cost of elliptic curve cryptography to propose a new protocol which improve the secure and effective of the DRM system. The proposed protocol can be divided into three parts: (1) we overcome the weaknesses of Mishra et al.'s scheme, and improve a better scheme for DRM system; (2) we modify the disadvantages of Jung et

al.'s protocol which is suitable for EPR information system, and proposed the biometric-based protocol for the DRM system; (3) through the amendment of Amin et al.'s protocol based on ECC for cloud computing environment, we propose the low computational cost protocol for DRM system. The above three parts. As compared with their protocols, the security and performance analysis show that our propose protocols are more secure and efficient than related works, and proposed protocols are more suitable for the DRM system.

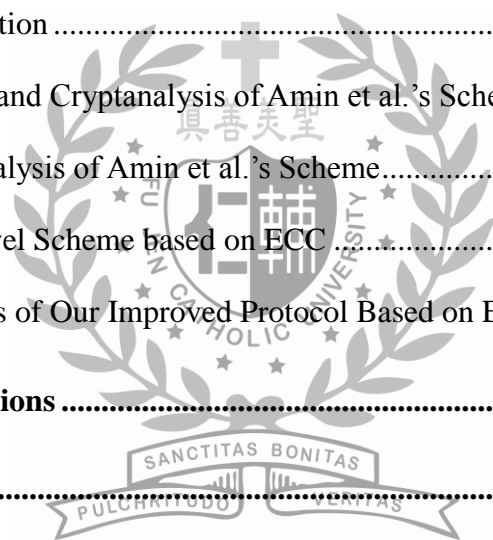
Keywords: Access control, Biometric, Digital Rights Management, ECC, Mobile device



TABLE OF CONTENTS

誌謝(ACKNOWLEDGEMENTS)		i
中文摘要		iii
ABSTRACT		iv
TABLE OF CONTENTS		vi
LIST OF TABLES		viii
LIST OF FIGURES		ix
Chapter 1 Introduction		1
1.1 Research Motivation		1
1.2 Research Subjects.....		4
1.3 Thesis Organization.....		5
Chapter 2 Preliminaries		7
2.1 A One-Way Hash Function.....		7
2.2 Biometrics Verification.....		7
2.3 Biometrics Fuzzy Extractor.....		8
2.4 ECC and its Complexity Assumptions		9
Chapter 3 An Efficient and Anonymous Scheme for E-DRM		10
3.1 Introduction		11
3.2 Review and Cryptanalysis of Mishra et al.'s E-DRM Scheme		13
3.3 The Security Weaknesses of Mishra et al.'s Scheme		21
3.4 Our Proposed Scheme for E-DRM.....		22
3.5 Analyses of Our Improved E-DRM Scheme.....		29

Chapter 4	A Biometric-Based Authentication Scheme for DRM.....	34
4.1	Introduction	34
4.2	Review and Cryptanalysis of Jung et al.'s Scheme	36
4.3	Cryptanalysis of Jung et al.'s Scheme	41
4.4	The Biometric-based Scheme for DRM.....	42
4.5	Analyses of Our Improved Biometric-based Protocol	47
Chapter 5	A Novel Authentication Scheme for DRM Based on Elliptic Curve Cryptography	53
5.1	Introduction	53
5.2	Review and Cryptanalysis of Amin et al.'s Scheme.....	57
5.3	Cryptanalysis of Amin et al.'s Scheme.....	61
5.4	The Novel Scheme based on ECC	61
5.5	Analyses of Our Improved Protocol Based on ECC	68
Chapter 6	Conclusions	75
References	77



LIST OF TABLES

Table 3.2.1. Notations of E-DRM scheme	14
Table 3.6.1. Performance comparisons of E-DRM scheme	33
Table 4.2.1. Notations of the biometric-based scheme.....	38
Table 4.5.1. The notations of Ban logic.....	48
Table 4.5.2. Security comparison among related schemes in Chapter 4	50
Table 4.5.3. Performance comparison among related schemes in Chapter 4.....	52
Table 5.2.1. Notations of the scheme based on ECC.....	58
Table 5.6.1. Performance comparison among related schemes in Chapter 5	74



LIST OF FIGURES

Fig 1.1.1. The basic architecture of the DRM system	2
Fig 3.2.1. Registration phase of Mishra et al.'s scheme	16
Fig 3.2.2. Key authorization phase of Mishra et al.'s scheme	18
Fig 3.4.1. Package phase of our improved E-DRM scheme	23
Fig 3.4.2. Registration phase of our improved E-DRM scheme	24
Fig 3.4.3. Authentication phase of our improved E-DRM scheme	26
Fig 3.4.4. Password change phase of our improved E-DRM scheme	29
Fig. 4.4.1 User registration phase of our improved biometric-based scheme	42
Fig 4.4.2. Authentication phase of our improved biometric-based scheme	45
Fig 5.4.1. License server registration phase of our improved DRM scheme based on ECC	62
Fig 5.4.2. User registration phase of our improved DRM scheme based on ECC	63
Fig 5.4.3. Authentication and content key obtaining phase of our improved DRM scheme based on ECC	67
Fig 5.4.4. Password renewal phase of our improved DRM scheme based on ECC	67

Chapter 1 Introduction

1.1 Research Motivation

Due to the rapid development of modern technology, the Internet has a fast and efficient transmission and distributive channels. Also, with the increase in the population using the Internet, the Internet becomes the fastest pipeline for consumers. Many traditional contents originally in their physical or broadcast forms such as paper documents, multimedia data, and a lot more that are worthy of careful preservation have also been converted into digital contents.

On the other hand, the booming advancement of the Internet has made it extremely easy and fast to spread all kinds of data around. [18, 20, 33] As the quantities of the digital contents put up and spread out on the Internet grow exponentially, people are getting more and more used to obtaining information and receiving entertainment through the Internet. The download times of digital contents are increased rapidly in many well-known music sites in domestic and foreign area, such as iTunes, KKBOX. It shows that the digital content market is booming.

The digital content market is booming, the legitimate download pipeline has been perfect established not yet. In many parts of the world, unauthorized downloading of digital contents remains a serious problem, causing great losses to the copyright owners. Therefore, the enforcement of copyright protection of digital contents is a big issue, and the development of an ideal digital rights management (DRM) system is essential so it can be guaranteed that only copyright owners or authorized users have access to the copyrighted digital media [8-9, 12, 26, 34, 44]. In general, the DRM system is designed to protect digital content from being used illegally by illegal users. Under the protection of the DRM system, digital contents can only be accessed by authorized users. In a

DRM system, the major source of intellectual property protection is data encryption.

We will brief introduce the DRM architecture and the roles involved:

Digital Rights Management system (DRM system)

- The core of digital content security

Content security is built on content encryption, and access control relies on identity verification. The core of a DRM system is the secure digital content delivery infrastructure. The access control to the digital content relies on a good user identity verification mechanism. Fig 1.1.1. shows the basic architecture of a DRM system, where there are four main roles involved: (1) the content provider (CP), (2) the content server (CS), (3) the license server (LS), and (4) the mobile user (MU) [7-9, 12, 18, 20, 26, 33-34, 44]. The four roles are described as follows:

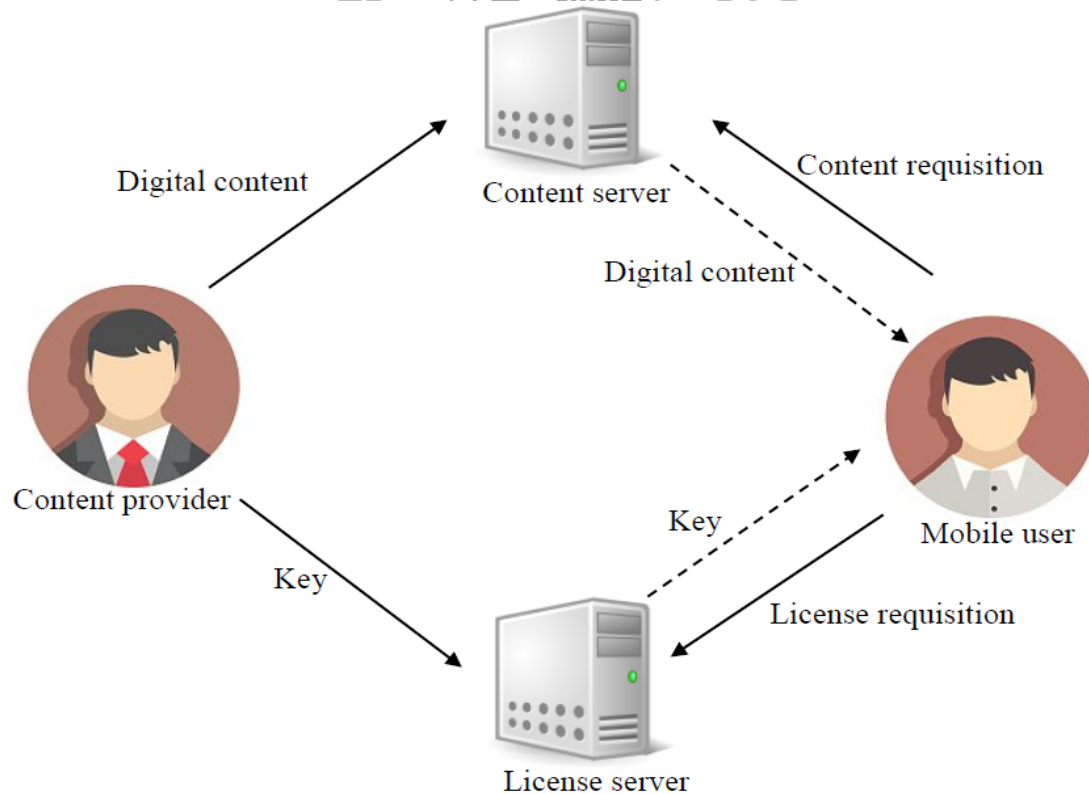


Fig 1.1.1. The basic architecture of the DRM system

1. The content provider (*CP*) means the owner or author of the digital content.

Having completed the creation of the digital content, *CP* uses a secret key to encrypt the digital content. Then, the secret key is transmitted to the license server through a secure channel. Meanwhile, the encrypted digital content is transmitted to the content server through a secure channel.

2. The content server (*CS*) means the server which stores the digital content.

Upon receiving the encrypted digital content from *CP*, *CS* puts it into the database. Then, *CS* displays the abstract of the digital content on a website open to the public.

3. The license server (*LS*) means the server which owns the secret key to the encrypted digital content.

Upon receiving the secret key from *CP*, *LS* puts it into the database. Later on, when *LS* receives a request from *MU* for the secret key, *LS* will authenticate *MU*. If *MU* passes the authentication, *LS* authorizes *MU* to use the secret key.

4. The mobile user (*MU*) means the person who wants to legally obtain the digital content.

Attracted to the abstract posted on the website, *MU* decides to access the digital content over the Internet. Now *MU* has to send a request to *CS* for the encrypted digital content and at the same time send a request to *LS* for the secret key. Upon receiving the requests, *LS* and *CS* both authenticate *MU*. Only when the identity of the user checks out can *MU* obtain the encrypted digital content from the *CS* and the secret key from *LS*. Then, using the secret key, *MU* can decrypt the encrypted digital content. That means the user's access to the digital content online is a success.

Conforming to the overall trend in technology, mobile devices are designed to be smaller and lighter and mobile devices also offer greater convenience. Hence, people are increasingly dependent on their mobile devices anytime, anywhere, and what they are doing. According to these characteristics, people will be using digital contents regardless of time and place because of the use of the mobile device [1-2]. On the other hands, when people use digital contents, opportunities are they will be using digital contents on their mobile devices. For these reasons, our proposed schemes are applied to mobile devices.

In order to quickly understand the DRM system environment and its information security issues, this study will review three related works which are published in the top journals [2, 16, 26]. Through these papers, a thorough understanding of its security protocol and discussion of individual weaknesses. Furthermore, we will propose improved protocols and more applicable to the DRM system environment.

1.2 Research Subjects

In this study, we focus on the privacy protection of digital contents in DRM system applications. There are three subjects in this thesis. The first subject is biometric verification for DRM system on mobile devices. In 2015, Mishra et al. proposed an anonymous enterprise digital rights management system for mobile devices [26]. Their scheme is based on biometric verification and overcomes some weaknesses of previous works. However, we found out that Mishra et al.'s scheme has some flaws. Hence, how to improve these flaws is the first goal of our thesis.

The second one is a novel anonymity digital rights management system authentication scheme based on biometric verification. The success of a DRM system

relies heavily on a good user authentication mechanism, and user identity verification through biometric information check is a great idea in that the biological characteristics are unique to each user and that such a mechanism releases the user of the trouble of keeping the login info safe from being stolen or mistaken or forgotten. To achieve our purpose, we will review and cryptanalysis Jung et al.'s scheme [16]. Although the environment of Jung et al.'s scheme is not suitable for DRM systems, the environmental architecture of Jung et al.'s scheme is similar to DRM systems. Hence, we proposed the new scheme for DRM system based on biometric and modified the weaknesses of Jung et al.'s scheme. Finally, we will compare performance and security analysis with other schemes to prove the proposed scheme is more suitable for DRM systems.

The third subject is a novel authentication scheme for anonymity and digital rights management based on elliptic curve cryptography. In generally, there are two paths from which most DRM system developers so far have chosen one to follow: (1) biometric verification and (2) smart card. Little has been mentioned about the possibility of constructing a DRM system based on elliptic curve cryptography (ECC). Moreover, in response of modern people's heavy dependence on their mobile devices, we think that elliptic curve cryptography (ECC) is a good idea to design a DRM scheme because it is a very good mobile device level security tool. In this section, we will review and cryptanalysis of Amin et al.'s scheme [2]. And then, with the security flaws mended, we shall propose an improved ECC-based protocol for DRM that is especially suitable for applications on mobile devices.

1.3 Thesis Organization

The remainder of this thesis is organized as follows. We introduce some mathematical tools which are used in our protocols in Chapter 2. In Chapter 3, we will

review Mishra et al.'s scheme for DRM system based on biometric verification [26] and propose an improved scheme. Then, we shall review the Jung et al.'s user authentication with key agreement scheme for the integrated EPR information system [16] and present out improved biometric-based protocol suitable for DRM system in Chapter 4. In Chapter 5, we describe the secure and privacy-aware user authentication scheme for mobile cloud computing environments [2] and propose a novel protocol for DRM system. Finally, the conclusion will be shown in Chapter 6.



Chapter 2 Preliminaries

In order to design excellent schemes for a DRM system, we will use some mathematical tools in our new protocols. In this section, we introduce those mathematical tools which involve (1) a one-way hash function; (2) biometric verification; (3) biometrics fuzzy extractor; (4) ECC and its complexity assumption, briefly introduced as follows.

2.1 A One-Way Hash Function

A one-way hash function is an algorithm $H: \{0, 1\}^* \rightarrow \{0, 1\}^n$ [21], which takes an arbitrary length string inputs $x \in \{0, 1\}^*$ and gives fixed length outputs $H(x) \in \{0, 1\}^n$. The fundamental property of one-way hash function is that its outputs are very sensitive to small perturbations in inputs [11, 25]. Hash functions are widely used in encryption algorithms along with databases to index and retrieve data items. The well-known hash functions are message digest hash functions and secure hash algorithms. The ideal hash function has following main properties.

One-way:

The computation of hash function for any given input is relatively easy process.

It is difficult to obtain message x from its hash value $H(x)$.

Collision-resistant:

It is difficult to find value x and y which satisfy $x \neq y$ and $H(x) = H(y)$.

2.2 Biometrics Verification

A biometric system is a pattern recognition system [15, 28-29]. Biometric verification permits one to establish an individual's identity. The biometric system

operates extracting a feature set from acquired data by acquired biometric data from an individual, then comparing the extracted features set against the template set in the database. Using biometric keys (e.g. faces, irises, and fingerprints) has advantage as follows: (1) biometric keys cannot be lost or forgotten, (2) biometric keys are difficult to share or copy, (3) biometric keys cannot be guessed, (4) biometric keys are difficult to steal [21].

2.3 Biometrics Fuzzy Extractor

Let $M = \{0, 1\}^v$ denotes a finite dimensional metric space, which consists of the biometric data points. Let $d : M \times M \rightarrow Z^+$ be a distance function, which can be used to calculate the distance between two points based on the metric chosen, where Z^+ is the set of all positive integers [6, 10, 12, 17].

A fuzzy extractor (M, l, t) extracts a nearly l -bit random string σ_i from its biometrics input B_i in an error-tolerant way, where t is the error tolerance threshold. If an input B'_i changes but remains close to B_i , the extracted σ_i remains the same. To recover σ_i from the biometrics input B_i , a fuzzy extractor also produces an auxiliary string τ_i , where σ_i remains uniformly random for a given τ_i .

- (1) Gen is a probabilistic generation procedure. Upon receiving biometric input B , the procedure will output a random string σ and a random auxiliary string τ .
- (2) Rep is a deterministic reproduction procedure. Upon receiving a close biometric input B^* and the corresponding random auxiliary string τ , the procedure will recover σ .

2.4 ECC and its Complexity Assumptions

Elliptic Curve Cryptography (ECC) is a kind of a public key cryptography. For each communication session, the user generally owns a pair of keys including a public key and a private key. The private key is only known to the specific user, while the public key is distributed to all users involved in the same communication session. Some public key algorithms including ECC require a set of predefined constants to be known to all users. ECC is defined over the elliptic curve $y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0$. Each different pair of (a, b) values gives a different elliptic curve. All points (x, y) that satisfy the above equation plus a point at infinity form an elliptic curve. The private key is a random number, and the public key is a point in the curve. The public key is obtained by multiplying the private key with the generator point G in the curve. [3, 4, 22]

Some complex problems can be created out of G_1 as follows:

1. Discrete Logarithm Problem (DLP)

Given two elements P and Q in G_1 , it is difficult to find $n \in Z_q$.

For example, $P = nQ$ if n exists.

2. Computation Diffie-Hellman Problem (CDHP)

Given P, xP, yP for $x, y \in Z_q$, it is difficult to compute xyP .

3. Bilinear Diffie-Hellman Problem (BDHP)

Given P, P^x, P^y, P^z for $x, y, z \in Z_q$, it is difficult to compute $\hat{e}(P, P)^{xyz} \in G_2$.

Chapter 3 An Efficient and Anonymous Scheme for E-DRM

With the rapid development of information science and network technology, Internet has become an important platform for the dissemination of digital content, which can be easily copied and distributed through the Internet. Although convenience is increased, it causes significant damage to authors of digital content. Digital rights management system (DRM system) is an access control system that is designed to protect digital content and ensure illegal users from maliciously spreading digital content. Enterprise Digital Rights Management system (E-DRM system) is a DRM system that prevents unauthorized users from stealing the enterprise's confidential data. User authentication is the most important method to ensure digital rights management. In order to verify the validity of user, the biometrics-based authentication protocol is widely used due to the biological characteristics of each user are unique. By using biometric identification, it can ensure the correctness of user identity. In addition, due to the popularity of mobile device and Internet, user can access digital content and network information at anytime and anywhere. Recently, Mishra et al. proposed an anonymous and secure biometric-based enterprise digital rights management system for mobile environment. Although biometrics-based authentication is used to prevent users from being forged, the anonymity of users and the preservation of digital content are not ensured in their proposed system. Therefore, in this paper, we will propose a more efficient and secure biometric-based enterprise digital rights management system with user anonymity for mobile environments.

3.1 Introduction

3.1.1 Background

With the rapid development of network technology, the Internet is a fast and efficient way for providing data transmission and information distribution. Due to the popularity of Internet, the digital content market has received many benefits. Digital content is one of the most important sources of information and entertainment. Digital technology for the digitalization of these traditional media (e.g., photos, cassettes, bibliographies, etc.) into digital content. Then digital content can be shared and transmitted to network users through the Internet. While the digital content market is booming and digital content can be easily distributed, illegitimate download and unauthorized distribution of digital content will cause some serious problems in many countries and industries. Therefore, provision of the copyright protection of digital content is an important issue in DRM system [18, 20, 33].

DRM system focuses on integrating the set of policies, technologies and tools for managing the access control on the digital contents. The main core of DRM system is to ensure digital contents' security. Digital content encryption and digital license are proposed for ensuring content security. Enterprise Digital Rights Management (E-DRM) system is the application of DRM system that ensures the secret documents of an enterprise from unauthorized access and many researchers have developed authentication mechanisms for securing the confidential data of an enterprise in E-DRM system. This chapter will focus on propose the mobile device and biometrics based authentication scheme for E-DRM system [8-9, 12, 26, 34, 44].

3.1.2 Related Works

In recent years, there are many literatures focus on design a secure and efficient

authentication scheme for digital rights management. For smart card based authentication schemes in DRM system, Zhang et al. proposed a three-party based DRM authentication scheme using smart card in 2009 [39]. In 2013, Yang et al. pointed out that Zhang et al.'s scheme fails to withstand insider and stolen smart card attacks. Then Yang et al. further proposed an enhanced version of DRM authentication scheme [37]. In the same year, Mishra et al. found that Yang et al.'s scheme cannot resist the denial of service and password guessing attacks [29]. In 2015, Zhang et al. proposed a provable secure and efficient digital rights management authentication scheme using smart card based on elliptic curve cryptography [38]. Zhang et al. demonstrated some weakness of Yang et al.'s scheme. For biometrics based authentication schemes in DRM system, Chen et al. proposed a secure and traceable E-DRM system for mobile device in 2008 [9]. Chen et al.'s scheme provided lower computational cost. In 2010, Chang et al. presented the cryptanalysis of Chen et al.'s scheme and pointed out that an attacker can easily intercept the key and use the key to obtain the confidential content of the enterprise and the mobile user cannot identify the tampering of message. In order to overcome these problems, Chang et al. further proposed an efficient and reliable E-DRM scheme for mobile environments [8]. In 2013, Chang et al. found that Chang et al.'s scheme still has some security weaknesses. The scheme in [8] cannot withstand stolen device attack and mobile user cannot optionally change his/her mobile device without the server assistant. Then Chang et al. further proposed a practical secure and efficient E-DRM authentication mechanism suitable for mobile environment [7]. In 2015, Mishra et al. demonstrated that the scheme in [7] cannot withstand privileged-insider and off-line password-guessing attacks. To repair these security weaknesses, Mishra et al. proposed an anonymous and secure biometric-based E-DRM system authentication scheme for mobile environment [26]. Unfortunately, in this paper, we

found that Mishra et al.'s scheme still has some flaws on digital content and content key and user anonymity cannot be achieved. Concerning the above-mentioned weaknesses, we will propose an effective anonymity and secure biometric-based enterprise digital rights management system.

3.2 Review and Cryptanalysis of Mishra et al.'s E-DRM Scheme

In this section, we first review Mishra et al.'s E-DRM scheme [26] and describe some security weaknesses on their scheme. The notations listed in Table 3.2.1. are used for describing Mishra et al.'s scheme as well as our scheme in the next section. The E-DRM scheme has six roles: (i) author of digital content, (ii) package server, (iii) content server, (iv) license server, (v) authorization authority and (vi) mobile user. Moreover, Mishra et al.'s scheme consists of four phases: (1) package phase, (2) registration phase, (3) key authorization phase and (4) password and biometric update phase and works as follows:

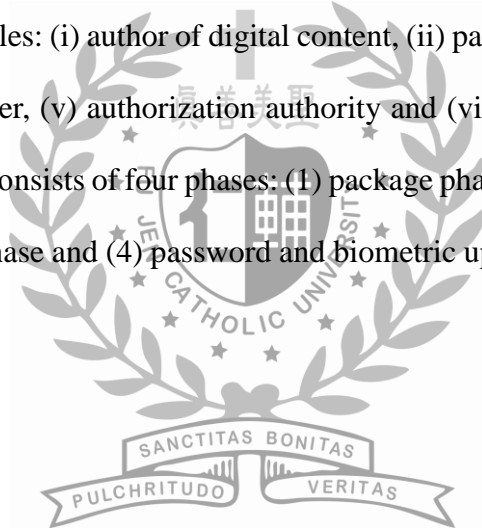


Table 3.2.1. Notations of E-DRM scheme

Notation	Description
MU	Mobile user
CS	Content server
LS	License server
PS	Package server
DC	Digital content
AA	Authorization authority
ID_{MU}	Identity of MU
ID_{DC}	Identity of digital content DC
$KEY_{ID_{DC}}$	Randomly generated symmetric key by PS
DID_{MU}	Anonymous identity of MU
DID_{DC}	Anonymous identity of DC
PW_{MU}	Unique password of MU
T_{MU}	Timestamp generated by MU
T_{LS}	Timestamp generated by LS
X	Secret symmetric key of LS
$Sym. Enc_K(.) / Sym. Dec_K(.)$	Symmetric encryption/decryption using key K
$H(.)$	One-way hash function
DRM-AP	DRM-enabled application
\oplus	Bitwise XOR operation
\parallel	String concatenation operation

3.2.1 Package Phase

In this phase, *PS* will package *DC* and *DC* is provided by the authors. After packaging *DC*, *PS* performs the content distribution with the help of *LS* and *AA*. The detailed steps of the packaging phase are described as follows.

Step1. *PS* randomly generates a symmetric key $KEY_{ID_{DC}}$ and uses $KEY_{ID_{DC}}$ to encrypt the digital content *DC* by computing $E(DC) = Sym.Enc_{KEY_{ID_{DC}}}(DC)$. *PS* generates the file header *CH* and uses its private key to generate two signatures for $E(DC)$ and *DC* by computing $Sig_{PS}(E(DC))$ and $Sig_{PS}(CH)$, respectively.

Step2. When the content packaging is finished, *PS* provides the content key seed to *LS* via a secure channel, where the key seed is the initial random seed number generated by *AA*. Furthermore, *PS* also provides the packaged content and content information to *CS*.

Step3. Upon receiving the key seed, *LS* securely stores the content key. Upon receiving the packaged content from *PS*, *CS* uploads the packaged content on the media servers and shows the content information on the website.

3.2.2 Registration Phase

In this phase, the *MU* must install the DRM-AP in his/her mobile device. Then *MU* uses his/her mobile device to perform the registration with remote DRM system. The registration phase of Mishra et al.'s scheme is summarized in Fig 3.2.1. The descriptions of registration phase are shown as follows:

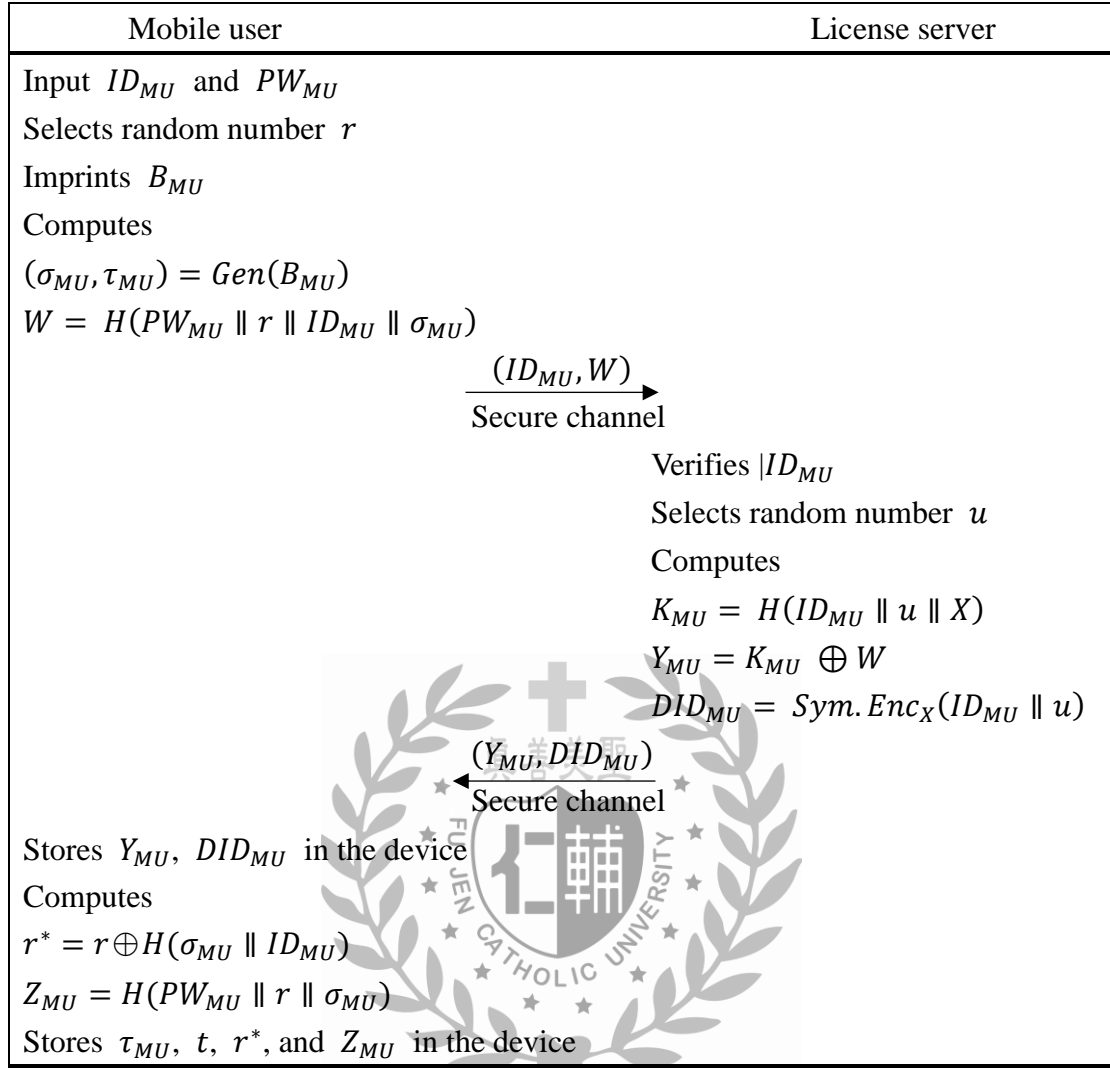


Fig 3.2.1. Registration phase of Mishra et al.'s scheme

Step1. The user MU selects a unique identity ID_{MU} and password PW_{MU} and imprints his/her personal biometrics B_{MU} at the sensor of his/her mobile device. Then the mobile device generates a random number r and applies the fuzzy generator function $Gen(.)$ to produce the biometric data key $Gen(B_{MU}) = (\sigma_{MU}, \tau_{MU})$. After that, MU computes the pseudo password $W = H(PW_{MU} \parallel r \parallel ID_{MU} \parallel \sigma_{MU})$ and sends the request message (ID_{MU}, W) to LS via a secure channel.

Step2. Upon receiving the registration request from MU , LS verifies ID_{MU} is

valid or not. If it is valid, LS generates a random number u and computes $K_{MU} = H(ID_{MU} \parallel u \parallel X)$ and $Y_{MU} = K_{MU} \oplus W$, where X is a secret key of LS . Moreover, LS computes $DID_{MU} = \text{Sym.Enc}_X(ID_{MU} \parallel u)$ and sends Y_{MU} and DID_{MU} to MU via a secure channel.

Step3. After receiving the response message from LS , MU stores Y_{MU} and DID_{MU} in his/her mobile device and computes $r^* = r \oplus H(\sigma_{MU} \parallel ID_{MU})$ and $Z_{MU} = H(PW_{MU} \parallel r \parallel \sigma_{MU})$. Finally, MU stores τ_{MU} , t , r^* , and Z_{MU} into his/her mobile device.

3.2.3 Key Authorization Phase

The key authorization key phase of Mishra et al.'s scheme is summarized in Fig 3.2.2. In order to access the DC on user's mobile device, when MU wants to download the DC from the media server, user must own the content key to access the DC . In order to achieve authorization, a registered user first needs to download the packaged content and executes the authorized phase with the LS . If the user's verification holds, the LS will authorize the content key. The description of this phase is given in the following:

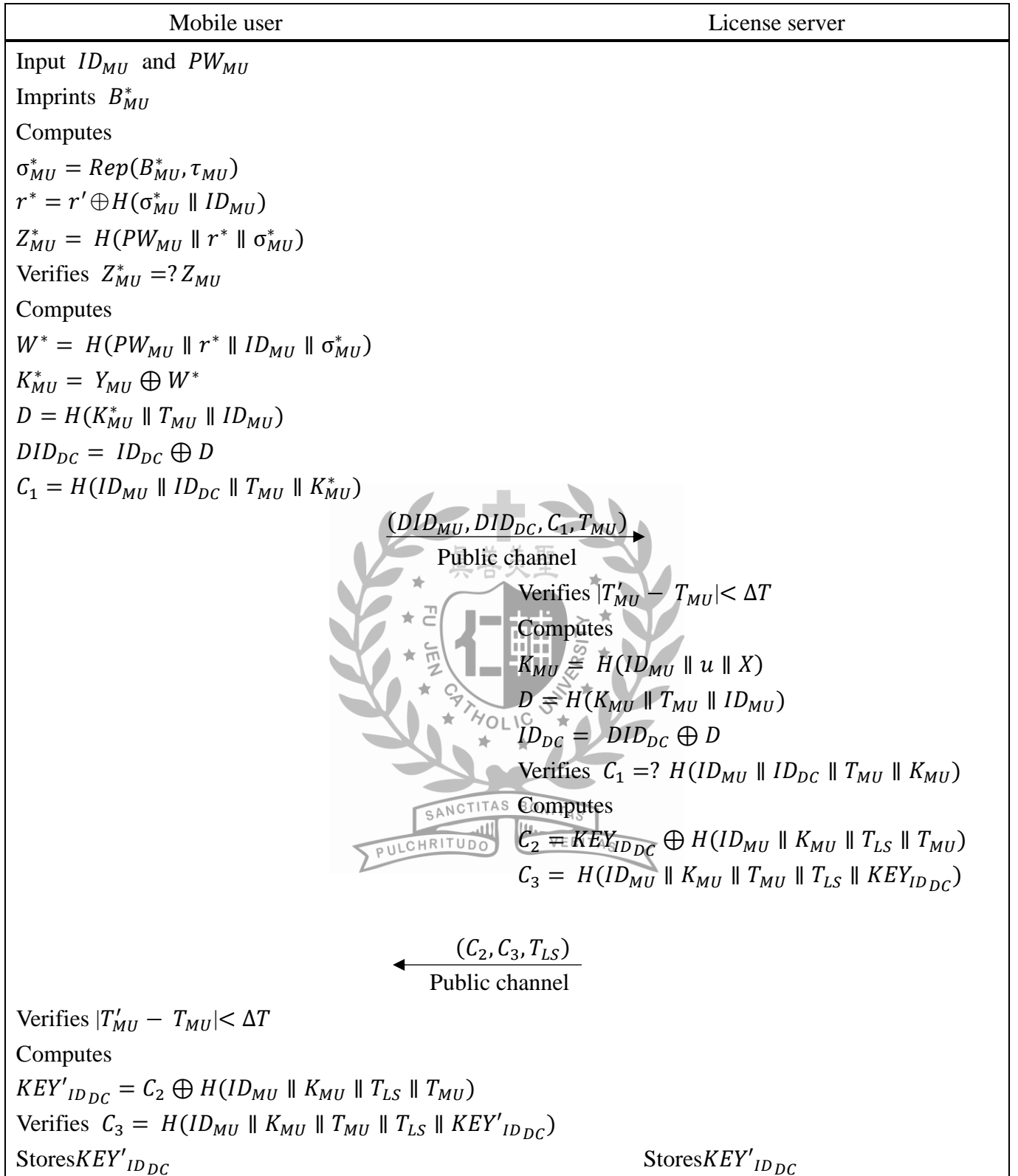


Fig 3.2.2. Key authorization phase of Mishra et al.'s scheme

Step 1. MU inputs the identity ID_{MU} and the password PW_{MU} in device and imprints the biometrics B_{MU}^* at the sensor of his/her mobile device. The DRM application (DRM-AP) uses $Ren(B_{MU}^*)$ fuzzy extractor function and τ_{MU} in the mobile device to compute $Rep(B_{MU}^*, \tau_{MU}) = \sigma_{MU}^*$. Then the DRM-AP computes $r' = r^* \oplus H(\sigma_{MU}^* || ID_{MU})$ and $Z_{MU}^* = H(PW_{MU} || r' || \sigma_{MU}^*)$ and checks the condition $Z_{MU}^* = Z_{MU}$ holds or not. If it does not hold, the password and biometrics verification fails and the session is terminated immediately. Otherwise, the DRM-AP computes $W^* = H(PW_{MU} || r^* || ID_{MU} || \sigma_{MU}^*)$, $K_{MU}^* = Y_{MU} \oplus W^*$, and $DID_{DC} = ID_{DC} \oplus D$, $D = H(K_{MU}^* || T_{MU} || ID_{MU})$ for the MU who wants to access the selected DC , where T_{MU} is the current timestamp generated by DRM-AP. In addition, the DRM-AP computes $C1 = H(ID_{MU} || ID_{DC} || T_{MU} || K_{MU}^*)$ and sends the log-in message $(DID_{MU}, DID_{DC}, C1, T_{MU})$ to LS via a public channel.

Step 2. Upon receiving the message $(DID_{MU}, DID_{DC}, C1, T_{MU})$ at time T'_{MU} , LS verifies the time delay in message transmission by checking the condition $|T'_{MU} - T_{MU}| < \Delta T$, where ΔT represents the maximum transmission delay or preset acceptable delay threshold. If it holds, LS retrieves the user identity ID_{MU} and u as $(ID_{MU} || u) = Sym.Dec_X(DID_{MU})$. Moreover, in order to retrieve ID_{DC} from DID_{DC} , LS computes $K_{MU} = H(ID_{MU} || u || X)$ and $ID_{DC} = DID_{DC} \oplus H(K_{MU} || T_{MU} || ID_{MU})$. LS verifies the situation $C1 = H(ID_{MU} || ID_{DC} || T_{MU} || K_{MU})$ holds or not. If the verification holds, LS computes $C2 = KEY_{IDDC} \oplus H(ID_{MU} || K_{MU} || T_{LS} || T_{MU})$ and $C3 = H(ID_{MU} || K_{MU} || T_{MU} || T_{LS} || KEY_{IDDC})$ and sends the message $(C2, C3, T_{LS})$ to mobile user MU .

Step 3. Upon receiving the message $(C2, C3, T_{LS})$ from LS at time T'_{LS} , MU verifies the time delay in message transmission by checking the condition $|T'_{LS} -$

$T_{LS}/<\Delta T$. If it is valid, MU computes $KEY'_{IDDC} = C2 \oplus H(ID_{MU} || K_{MU} || T_{LS} || T_{MU})$ and verifies the situation $C3 = H(ID_{MU} || K_{MU} || T_{MU} || T_{LS} || KEY'_{IDDC})$ holds or not. If the verification is invalid, the session is rejected. Otherwise, the content key is authenticated and MU can use the content key KEY'_{IDDC} to access the encrypted digital content in the future.

3.2.4 Password and Biometric Update Phase

In this phase, if MU wants to change his or her password and personal biometrics, they freely changes his or her password and biometrics. Because of security reasons without further contacting LS . This phase contains the following steps:

Step 1. MU inputs ID_{MU} and the password PW_{MU}^{old} in device and mobile user imprints the biometrics B_{MU}^{old} at the sensor of his/her device. The DRM-AP uses $Ren(B_{MU})$ fuzzy extractor function and τ_{MU} in the mobile device to compute $Rep(B_{MU}^{old}, \tau_{MU}) = \sigma_{MU}^{old}$. After that, the DRM-AP computes $r^{old} = r^* \oplus H(\sigma_{MU}^{old} || ID_{MU})$ and $Z_{MU}^{old} = H(PW_{MU}^{old} || r^{old} || \sigma_{MU}^{old})$ and checks the condition $Z_{MU}^{old} = Z_{MU}$ holds or not. If it does not hold, this phase fails and the session is terminated immediately. Otherwise, the DRM-AP computes $W^{old} = H(PW_{MU}^{old} || r^{old} || ID_{MU} || \sigma_{MU}^{old})$ and $K_{MU}^{old} = Y_{MU} \oplus W^{old}$.

Step 2. MU inputs the new password PW_{MU}^{new} in device and mobile user imprints the new biometrics B_{MU}^{new} at the sensor of his/her device. The DRM-AP computes $Gen(B_{MU}^{new}) = (\sigma_{MU}^{new}, \tau_{MU}^{new})$ and generates a random number r^{new} . After that, the DRM-AP further computes the pseudo password $W^{new} = H(PW_{MU}^{new} || r^{new} || ID_{MU} || \sigma_{MU}^{new})$, $Y_{MU}^{new} = K_{MU}^{old} \oplus W^{new}$, $r^{**} = r^{new} \oplus H(\sigma_{MU}^{new} || ID_{MU})$ and $Z_{MU}^{new} = H(PW_{MU}^{new} || r^{new} || \sigma_{MU}^{new})$ and updates the

stored parameters Y_{MU} , Z_{MU} , r^* and τ_{MU} with Y_{MU}^{new} , Z_{MU}^{new} , r^{**} and τ_{MU}^{new} in the mobile device, respectively.

3.3 The Security Weaknesses of Mishra et al.'s Scheme

In this section, we describe that Mishra et al.'s scheme has some drawbacks and the detailed descriptions are shown as follows.

3.3.1 The Problem of User Anonymity

Although Mishra et al.'s scheme uses anonymous identity $DID_{MU} = Sym.Enc_X(ID_{MU}||u)$ to hide MU 's real identity ID_{MU} , the anonymous identity DID_{MU} is never changed in MU 's future sessions. Just like every student has own school identity and other people do not know someone's real name, but others still can follow the unchanged school identity to track the specific student. As you can see, in step 1 of key authorization phase of Mishra et al.'s scheme, the log-in message $(DID_{MU}, DID_{DC}, C1, T_{MU})$ is transmitted to LS via a public channel. Therefore, if an adversary knows DID_{MU} , he/she can track the usage history of the anonymous identity DID_{MU} .

3.3.2 The Storage Problem of Digital Content and Content Key

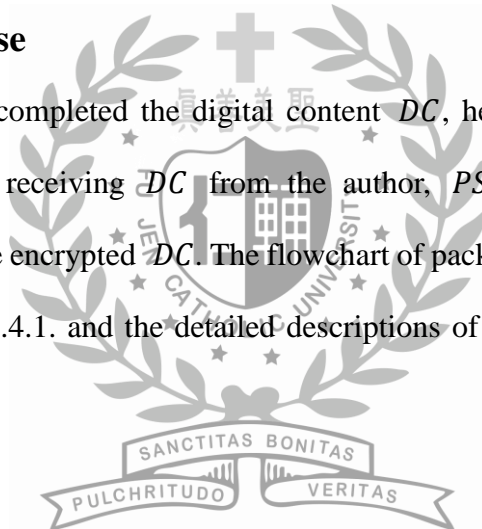
In Mishra et al.'s scheme, the encrypted digital content DC and the content key are stored in CS and LS , respectively. Because CS and LS do not encrypt their database and it might be a potential problem that the adversary attacks the server's database and steals the encrypted the digital content and content key seed. Then adversary can easily access the encrypted digital content by using the corresponding content key.

3.4 Our Proposed Scheme for E-DRM

In this section, in order to overcome the shortcomings of Mishra et al.'s scheme, we propose a novel biometrics-based authentication scheme for E-DRM system. The proposed scheme used the same notations listed in Table 1 and comprised of four phases (1) package phase, (2) registration phase, (3) authentication phase, and (4) password and biometric change phase. The E-DRM system architecture has five roles: (i) digital content author, (ii) package server, (iii) content server, (iv) license server, and (v) mobile user.

3.4.1 Package Phase

When the author completed the digital content DC , he/she delivers the digital content to PS . Upon receiving DC from the author, PS encrypts the DC and associates CH with the encrypted DC . The flowchart of package phase of our scheme is summarized in Fig 3.4.1. and the detailed descriptions of the packaging phase are shown as follows:



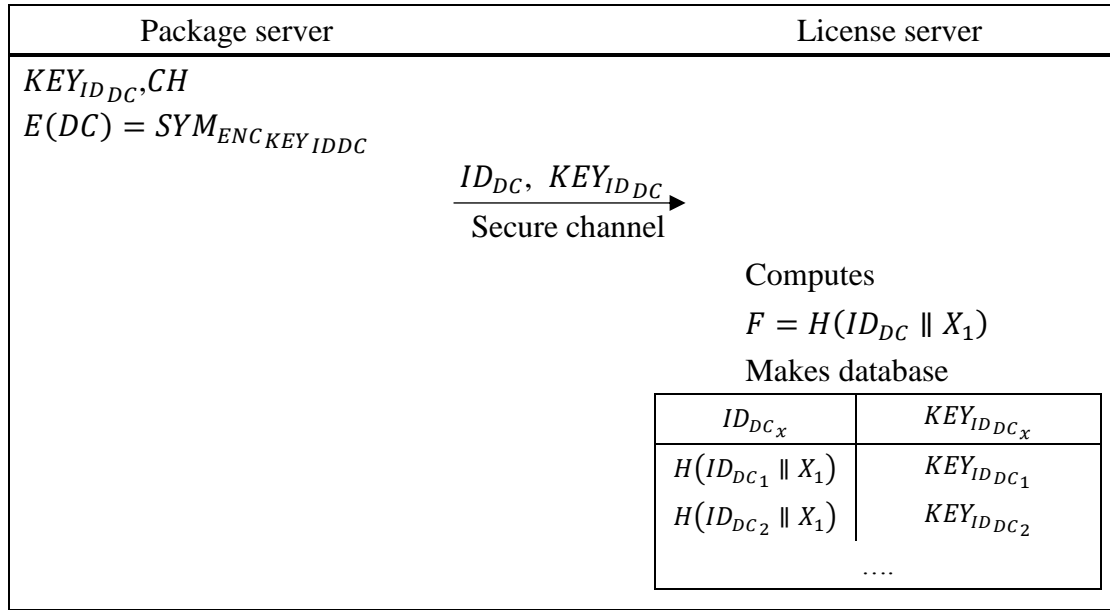


Fig 3.4.1. Package phase of our improved E-DRM scheme

Step1. Upon receiving the digital content from author, the *PS* generates a random key $KEY_{ID_{DC}}$ and computes $E(DC) = SYM_{KEY_{ID_{DC}}}(DC)$. Moreover, the *PS* associates a content header *CH* for each corresponding digital content, where the content header *CH* includes *PS* signature and encrypted digital content information.

Step2. Once the digital content packaging is completed, *PS* delivers the encrypted digital content and its corresponding content header *CH* to content server *CS*. In addition, *PS* delivers the content key $KEY_{ID_{DC}}$ and ID_{DC} to *LS* via a secure channel.

Step3. Upon receiving the packaged content from *PS*, *CS* uploads the encrypted digital content on their media database and displays the content information or content header on the website.

Step4. Upon receiving the key seed from *PS*, *LS* securely stores the content key and transmits the content key to the authorized users. Finally, *LS* computes $F = H(ID_{DC} \parallel X_1)$ and stores F and its corresponding $KEY_{ID_{DC}}$ into database.

3.4.2 Registration Phase

Before the access of the digital content, MU first installs the application DRM-AP in his or her mobile device. The registration phase of our scheme is summarized in Fig 3.4.2. The detailed descriptions of registration phase are shown as follows:

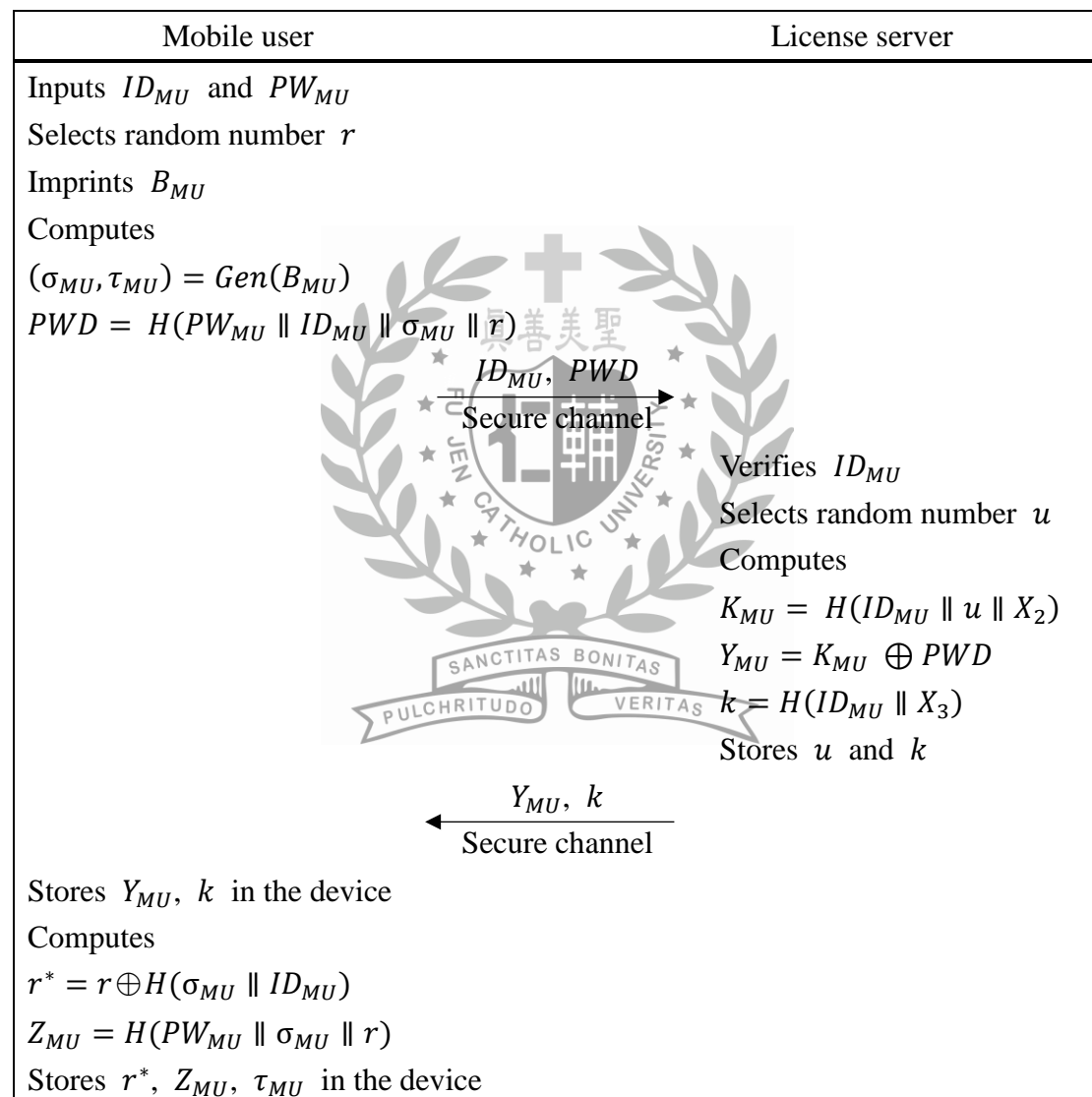


Fig 3.4.2. Registration phase of our improved E-DRM scheme

Step1. MU selects his/her favorite identity ID_{MU} and password PW_{MU} and imprints his/her personal biometrics B_{MU} at the sensor of his/her mobile device.

Then MU applies the $Gen(.)$ fuzzy generator function to produce the biometric data key $Gen(B_{MU}) = (\sigma_{MU}, \tau_{MU})$. After that, MU generates a random number r and computes $PWD = H(PW_{MU} \parallel ID_{MU} \parallel \sigma_{MU} \parallel r)$. Finally, MU sends the registration request message (ID_{MU}, PWD) to LS via a secure channel.

Step2. Upon receiving the registration request from MU , LS verifies ID_{MU} is valid or not. If the verification is correct, LS generates a random number u and computes $K_{MU} = H(ID_{MU} \parallel u \parallel X_2)$, $Y_{MU} = K_{MU} \oplus PWD$ and $k = H(ID_{MU} \parallel X_3)$. Finally, LS stores k and u and sends Y_{MU} and k to MU via a secure channel.

Step3. After receiving the response message from LS , MU stores Y_{MU} and k in his/her mobile device and computes $r^* = r \oplus H(\sigma_{MU} \parallel ID_{MU})$ and $Z_{MU} = H(PW_{MU} \parallel \sigma_{MU} \parallel r)$. In addition, MU stores τ_{MU} , r^* and Z_{MU} into his/her mobile device. At the end, MU 's mobile device has five values Y_{MU} , k , r^* , Z_{MU} and τ_{MU} .

3.4.3 Authentication Phase

In order to access the DC on user's mobile device, the mobile user must download the DC from the content server and own the corresponding content key to access the DC . To acquire the license, a registered user first needs to establish the authorized session with the license server LS . Once the user's verification holds, LS issues the content key and the flowchart of content key acquisition phase of our scheme is summarized in Fig 3.4.3. The detailed descriptions of this phase are given as follows:

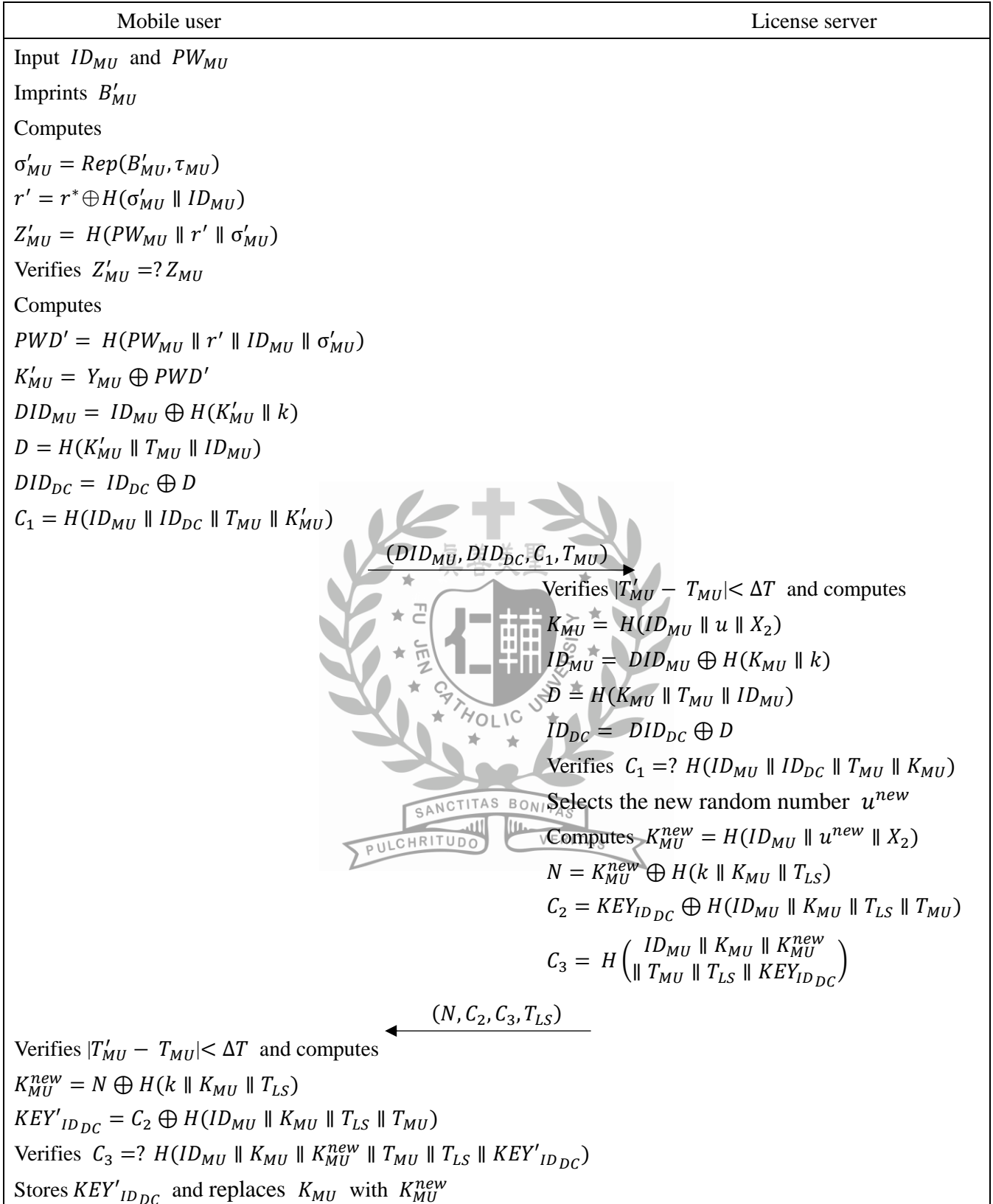


Fig 3.4.3. Authentication phase of our improved E-DRM scheme

Step 1. MU inputs the identity ID_{MU} and the password PW_{MU} in the mobile device and imprints his/her personal biometrics B'_{MU} at the sensor of MU 's mobile device. Then DRM-AP uses $Ren(B'_{MU})$ fuzzy extractor function and τ_{MU} in the mobile device to compute $Rep(B'_{MU}, \tau_{MU}) = \sigma'_{MU}$. Moreover, the DRM-AP computes $r' = r^* \oplus H(\sigma'_{MU} \parallel ID_{MU})$ and $Z'_{MU} = H(PW_{MU} \parallel r' \parallel \sigma'_{MU})$ and checks the equation $Z'_{MU} = Z_{MU}$ holds or not. If it does not hold, the password and biometrics verification fails and the session is terminated. Otherwise, for MU who wants to access the selected digital content DC , the DRM-AP computes $PWD' = H(PW_{MU} \parallel ID_{MU} \parallel \sigma'_{MU} \parallel r')$, $K'_{MU} = Y_{MU} \oplus PWD'$, $DID_{MU} = ID_{MU} \oplus H(K'_{MU} \parallel k)$, $D = H(K'_{MU} \parallel T_{MU} \parallel ID_{MU})$ and $DID_{DC} = ID_{DC} \oplus D$, where T_{MU} is the current timestamp generated by DRM-AP. After that, the DRM-AP computes $C_1 = H(ID_{MU} \parallel ID_{DC} \parallel T_{MU} \parallel K'_{MU})$ and sends the log-in message $(DID'_{MU}, DID_{DC}, C_1, T_{MU})$ to LS via the public channel.

Step 2. Upon receiving the message $(DID_{MU}, DID_{DC}, C_1, T_{MU})$ at time T'_{MU} , LS verifies the time delay in message transmission by checking the condition $|T'_{MU} - T_{MU}| < \Delta T$ holds or not. If it holds, LS computes $K_{MU} = H(ID_{MU} \parallel u \parallel X_2)$, $ID_{MU} = DID_{MU} \oplus H(K_{MU} \parallel k)$, $D = H(K_{MU} \parallel T_{MU} \parallel ID_{MU})$, and $ID_{DC} = DID_{DC} \oplus D$ and verifies the condition $C_1 = H(ID_{MU} \parallel ID_{DC} \parallel T_{MU} \parallel K_{MU})$ holds or not. If the verification holds, LS selects the new random number u^{new} and computes $K_{MU}^{new} = H(ID_{MU} \parallel u^{new} \parallel X_2)$, $N = K_{MU}^{new} \oplus H(k \parallel K_{MU} \parallel T_{LS})$, $C_2 = KEY_{ID_{DC}} \oplus H(ID_{MU} \parallel K_{MU} \parallel T_{LS} \parallel T_{MU})$ and $C_3 = H(ID_{MU} \parallel K_{MU} \parallel K_{MU}^{new} \parallel T_{MU} \parallel T_{LS} \parallel KEY_{ID_{DC}})$. Finally, LS sends the response message (N, C_2, C_3, T_{LS}) to MU .

Step 3. Upon receiving the message (N, C_2, C_3, T_{LS}) at time T'_{LS} , MU checks the condition $|T'_{LS} - T_{LS}| < \Delta T$ holds or not. If the time delay is valid, MU

computes $K_{MU}^{new} = N \oplus H(k || K_{MU} || T_{LS})$ and $KEY'_{IDDC} = C2 \oplus H(ID_{MU} || K_{MU} || T_{LS} || T_{MU})$ and verifies the equation $C3 = H(ID_{MU} || K_{MU} || K_{MU}^{new} || T_{MU} || T_{LS} || KEY'_{IDDC})$ holds or not. If it does not hold, the session is terminated. Otherwise, it means the content key is authenticated. Finally, MU uses the content key KEY'_{IDDC} to access the encrypted digital content and replaces K_{MU} with K_{MU}^{new} .

3.4.4 Password and biometric change phase

In this phase, the mobile user can change his/her password and personal biometrics without contacting the license server. The password and biometric change phase of our proposed scheme is summarized in Fig 3.4.4. The description of this phase is given in the following:

Step 1. MU inputs the identity ID_{MU} and the original password PW_{MU}^{old} in device and imprints the original personal biometrics B_{MU}^{old} at the sensor of mobile device. MU uses the biometric fuzzy extractor and the element value τ_{MU} which is stored in the device to computes $Rep(B_{MU}^{old}, \tau_{MU}) = \sigma_{MU}^{old}$. After that, the DRM-AP computes $r^{old} = r^* \oplus H(\sigma_{MU}^{old} || ID_{MU})$ and $Z_{MU}^{old} = H(PW_{MU}^{old} || \sigma_{MU}^{old} || r^{old})$ and checks whether the condition $Z_{MU}^{old} =? Z_{MU}$ holds or not. If it is valid, the DRM-AP computes $PWD^{old} = H(PW_{MU}^{old} || r^{old} || ID_{MU} || \sigma_{MU}^{old})$ and $K_{MU} = Y_{MU} \oplus PWD^{old}$.

Step 2. MU inputs his/her new password PW_{MU}^{new} in device and imprints the new personal biometrics B_{MU}^{new} at the sensor of his/her mobile device. The DRM-AP uses biometric fuzzy extractor function $Gen(B_{MU}^{new})$ to obtain $(\sigma_{MU}^{new}, \tau_{MU}^{new})$ and generates a random number r^{new} . After that, MU computes $PWD^{new} =$

$H(PW_{MU}^{new} || ID_{MU} || \sigma_{MU}^{new} || r^{new})$ and $Y_{MU}^{new} = K_{MU} \oplus PWD^{new}$. In addition, DRM-AP computes $r^{**} = r^{new} \oplus H(\sigma_{MU}^{new} || ID_{MU})$ and $Z_{MU}^{new} = H(PW_{MU}^{new} || \sigma_{MU}^{new} || r^{new})$. Finally, MU replaces the stored parameters Y_{MU} , Z_{MU} , r^* and τ_{MU} with Y_{MU}^{new} , Z_{MU}^{new} , r^{**} and τ_{MU}^{new} in the mobile device, respectively.

Mobile user	DRM-AP
Input ID_{MU} and PW_{MU}^{old} Imprints B_{MU}^{old}	Computes $\sigma_{MU}^{old} = Rep(B_{MU}^{old}, \tau_{MU})$ $r^{old} = r^* \oplus H(\sigma_{MU}^{old} ID_{MU})$ $Z_{MU}^{old} = H(PW_{MU}^{old} \sigma_{MU}^{old} r^{old})$ Verifies $Z_{MU}^{old} = ? Z_{MU}$ Computes $PWD^{old} = H(PW_{MU}^{old} ID_{MU} \sigma_{MU}^{old} r^{old})$ $K_{MU} = Y_{MU} \oplus PWD^{old}$
Inputs PW_{MU}^{new} , imprints B_{MU}^{new} $(\sigma_{MU}^{new}, \tau_{MU}^{new}) = Gen(B_{MU}^{new})$	$PWD^{new} = H(PW_{MU}^{new} ID_{MU} \sigma_{MU}^{new} r^{new})$ $Y_{MU}^{new} = K_{MU} \oplus PWD^{new}$ $r^{**} = r^{new} \oplus H(\sigma_{MU}^{new} ID_{MU})$ $Z_{MU}^{new} = H(PW_{MU}^{new} \sigma_{MU}^{new} r^{new})$ Replaces Y_{MU} , Z_{MU} , r^* and τ_{MU} with Y_{MU}^{new} , Z_{MU}^{new} , r^{**} and τ_{MU}^{new} in the device

Fig 3.4.4. Password change phase of our improved E-DRM scheme

3.5 Analyses of Our Improved E-DRM Scheme

In this section, we first analyze security of the proposed scheme in Section 5.1 and compare it with other related schemes in terms of performance in Section 5.2.

3.5.1 Security Analysis

In this subsection, we show that the proposed scheme satisfies security

requirements which not only overcome weaknesses of Mishra et al.'s scheme but also discuss previous papers did not satisfy these requirements [7-9, 26].

i. User Anonymity

In the proposed scheme, the registration phase license server provides $k = H(ID_{MU} \parallel X_3)$ to mobile user via the secure channel and stores k . In authentication phase, MU computes $DID_{MU} = ID_{MU} \oplus H(K'_{MU} \parallel k)$. After LS receives the authentication request message and checks MU 's identity, LS chooses the new random number u^{new} each authorization. An adversary cannot steal ID_{MU} from DID_{MU} due to the mobile user's identity ID_{MU} is masked with the secret value k and K_{MU} by license server. Only user and license server know the secret value k and K_{MU} . Moreover, an adversary cannot trace U_i 's identity because the value K_{MU} is always change for each communication. Therefore, the adversary cannot be linked between the mobile user and his/her real identity.

ii. Stolen Digital Content Encryption Key Attack

In the proposed scheme, the digital content author completes the digital content transfer to the package server and the package server package server encrypts the digital content and sends encryption key to the license server. The license server encrypts the digital content's identity ID_{DC} by using its secret key and the database stores the encrypted digital content's identity ID_{DC} and its corresponding encryption key $KEY_{ID_{DC}}$. Therefore, we assume that an adversary knows ID_{DC} , he/she cannot retrieve the encryption key. This shows that the proposed scheme provides the protection of digital content storage.

iii. Stolen Mobile Device Attack

If an adversary steals the user's mobile device, the adversary can retrieve the stored values k , Y_{MU} and Z_{MU} from the stolen mobile device. However, in the proposed scheme, an adversary cannot know mobile user's identity because ID_{MU} did not store in user's mobile. In addition, due to the user's identity ID_{MU} and password PW_{MU} are not store in his/her mobile device, it is difficult to compute the user's secret parameters K_{MU} from Y_{MU} , where $Y_{MU} = K_{MU} \oplus PWD$ and $PWD = H(PW_{MU} \parallel ID_{MU} \parallel \sigma_{MU} \parallel r)$. Moreover, the value σ_{MU} is generated by mobile user's biometric. Therefore, an adversary cannot obtain the user's secret value K_{MU} and the proposed scheme can prevent an adversary to maliciously obtain any useful information from the stolen mobile device.

iv. Mutual Authentication

In authentication phase of the proposed scheme, the mobile user computes DID'_{MU} by using the secret value k from license server. To achieve the property of mutual authentication between the user MU and the license server, the mobile user and the license server verifies the validity of $C_1 = H(ID_{MU} \parallel ID_{DC} \parallel T_{MU} \parallel K'_{MU})$ and $C_3 = H(ID_{MU} \parallel K_{MU} \parallel K_{MU}^{new} \parallel T_{MU} \parallel T_{LS} \parallel KEY'_{IDDC})$, respectively. In order to compute C_1 and C_3 , the mobile user's real identity ID_{MU} and secret value K_{MU} are needed and these two parameters are only known by the mobile user and the license server. As a result, only legitimate mobile user and the license server can compute C_1 and C_3 and the license server can verify the validity of mobile user's identity. Finally, the property of mutual authentication is provided in our proposed scheme.

v. Off-line Password-guessing Attack

For this attack, an adversary may collect the values C_1 and C_3 to derive the user's password in off-line manner. However, in order to derive the guessed password, the DRM-AP must know the mobile user's real identity ID_{MU} and the secret value K_{MU} , where $K_{MU} = H(ID_{MU} \parallel u \parallel X_2)$ is computed by license server and $K'_{MU} = Y_{MU} \oplus PWD'$ is computed by mobile user. Next, only legitimate mobile user can use σ_{MU} and B_{MU} to compute $PWD = H(PW_{MU} \parallel ID_{MU} \parallel \sigma_{MU} \parallel r)$ and the mobile user's identity ID_{MU} is masked with the secret value k and K_{MU} . Thus the adversary cannot obtain ID_{MU} . In addition, only the legitimate mobile user can imprint correct B_{MU} . Therefore, the proposed scheme is secure against the off-line password-guessing attack.

3.5.2 Performance Evaluation

In this subsection, we present the comparisons of computational cost during the authentication phase between the proposed scheme and other related works [7-9, 26]. For the convenience of evaluating the computational cost, we introduce some notations as follows:

T_h means the time complexity for computation of a one-way hash function $H(.)$.

T_{sym} means the time complexity for computation of a symmetric encryption or symmetric decryption.

T_{pub} means the time complexity for computation of a public key encryption or public key decryption.

T_{bi} means the time complexity for computation of a biometric fuzzy extractor function ($Gen(.)$ or $Rep(.)$).

Compared with these computations, T_{pub} is the most heavyweight operation as compared with other operations like T_{sym} , T_{bi} and T_h . As shown in Table 3.6.1., we can see that the proposed scheme requires less number of T_{sym} and our scheme and Mishra et al.'s scheme have the same computational cost on the operations of T_{pub} and T_{bi} which is more secure than Mishra et al.'s scheme.

Table 3.6.1. Performance comparisons of E-DRM scheme

Scheme	Phase	Mobile user	Server	Total
Chang et al. [8]	Package	-	$T_{sym} + 5T_{pub}$	$(6 F(\cdot) + 4)T_h$
	Registration	-	-	$+ 2T_{sym} + 7T_{pub}$
	Authorization	$(3 F(\cdot) + 2)T_h + T_{sym}$	$(3 F(\cdot) + 2)T_h + 2T_{pub}$	
Chang et al. [7]	Package	*	$T_{sym} + 6T_{pub}$	$14T_h + 2T_{sym}$
	Registration	$2T_h$	$2T_h$	$+ 6T_{pub}$
	Authorization	$4T_h + T_{sym}$	$8T_h$	
Mishra et al. [26]	Package	*	$T_{sym} + 2T_{pub}$	$16T_h + 4T_{sym}$
	Registration	$T_{bi} + 3T_h$	$T_h + T_{sym}$	$+ 2T_{pub} + 2T_{bi}$
	Authorization	$T_{bi} + 7T_h + T_{sym}$	$5T_h + T_{sym}$	
The proposed	Package		$T_h + T_{sym} + 2T_{pub}$	$22T_h + T_{sym}$
	Registration	$T_{bi} + 3T_h$	$2T_h$	$+ 2T_{pub} + 2T_{bi}$
	Authorization	$T_{bi} + 8T_h$	$9T_h$	

Chapter 4 A Biometric-Based Authentication Scheme for DRM

Due to the rapid development of computer technologies, many traditional contents have been digitized, adding to the immensity of digital contents. Through the Internet, various digital contents can be accessed and spread all over the world within the snap of a finger. However, such amazing swiftness and convenience have also brought various kinds of data security, privacy and copyright protection issues. Digital rights management (DRM) systems are access control technologies used to restrict the use, modification, and distribution of protected digital contents. The success of a DRM system relies heavily on a good user authentication mechanism, and user identity verification through biometric information check is a great idea in that the biological characteristics are unique to each user and that such a mechanism releases the user of the trouble of keeping the login info safe from being stolen or mistaken or forgotten. On the other hand, in response to modern people's prevalent use of mobile devices, DRM systems should also support mobile digital content access. In this paper, we shall propose a novel biometric-based authentication and anonymity scheme for DRM system. To develop our new scheme, we have carefully studied Jung et al.'s scheme, a biometric-based protocol whose architecture is similar to that of a DRM system but not quite the same, and modified it to fit the requirements of a DRM system environment. Our correctness check, security analysis, and performance evaluation have proved the superiority of our new scheme over related schemes.

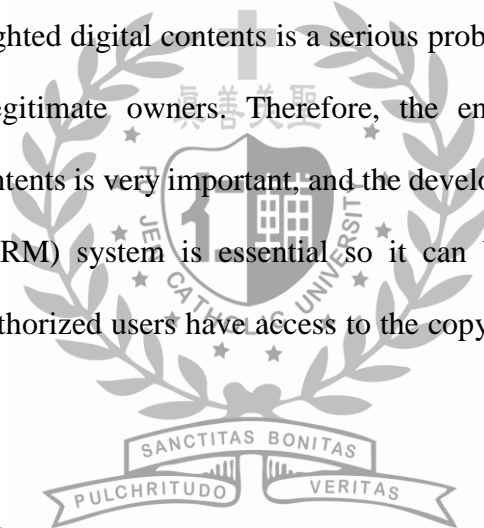
4.1 Introduction

4.1.1 Background

As a result of the advancement of computer technologies, more and more

traditional contents originally in their physical, analog, or broadcast forms such as paper documents or photos, compact cassettes, videotapes and a lot more have been converted into digital contents. In the meanwhile, the booming development of the Internet has connected exponentially growing numbers of people together and made it extremely easy and fast to spread all kinds of data around. In fact, legal access to copyrighted digital contents over the Internet is a swelling market because more and more people are now in the habit of getting informed and entertained online [13-14, 17, 23-25].

In fact, nowadays digital contents are way too easy to spread and to obtain on the Internet than they should. In many countries around the world, unauthorized downloading of copyrighted digital contents is a serious problem, causing great losses to the authors and legitimate owners. Therefore, the enforcement of copyright protection of digital contents is very important, and the development of an ideal digital rights management (DRM) system is essential so it can be guaranteed that only copyright owners or authorized users have access to the copyrighted digital media [5-7, 19-20, 27-32].



4.1.2 Related Works

In recent years, the topic of digital rights management has received a lot of attention, and many researchers have designed and offered their schemes in the hope of helping construct handy, practical digital rights management systems. In 2008, Chen proposed a secure and traceable E-DRM system based on mobile device [9], which is the first DRM authentication scheme to use biometric verification. In 2010, Chang et al. found some weaknesses in Chen's scheme, pointing out that an attacker could easily steal the digital content by using an intercepted key and that the mobile user would not be able to tell if anything had been tampered [8]. As an improved version of Chen's

scheme, Chang et al. proposed an efficient and reliable E-DRM protocol, which is also a DRM authentication scheme based on biometric verification for mobile environments. However, in 2013, Chang et al. pointed out that Chang et al.'s 2010 scheme was actually vulnerable to the stolen device attack and that the mobile user could not change passwords or biometric data on the mobile device [7]. To solve these problems, Chang et al. proposed a practical secure and efficient enterprise digital rights management mechanism suitable for mobile environment. In 2015, Mishra et al. showed that Chang et al.'s 2013 scheme was weak against the off-line password-guessing attack and the insider attack; to mend these security flaws, Mishra et al. proposed an anonymous and secure biometric-based enterprise digital rights management system for mobile environment [26].

Other than those schemes mentioned above that are especially designed for DRM systems, there are also authentication protocols to be applied in different systems that have a similar architecture to that of a DRM system. For example, Jung et al.'s scheme is designed for the integrated EPR information system [16], but the architecture of the scheme is quite applicable to the DRM system environment. Therefore, in this paper we shall review and cryptanalyze Jung et al.'s scheme and then offer our new scheme, which is a modified version of Jung et al.'s scheme especially for the DRM system.

4.2 Review and Cryptanalysis of Jung et al.'s Scheme

In this section, we review and cryptanalyze Jung et al.'s scheme [16]. Table 4.2.1. is a list of the notations used both in Jung et al.'s scheme and in our new scheme. Please note that Jung et al.'s scheme is especially designed for the integrated electronic patient records (EPR) information system, where patients' medical records are stored in cloud and only legally certified doctors or nurses can access the data. Since the architecture

of the EPR information system is similar to that of the DRM system, the basic structure of Jung et al.'s scheme is quite applicable to an authentication protocol for the DRM system. Jung et al.'s scheme has three phases, which are (1) the user registration phase, (2) the login and authentication phase, and (3) the password change phase. In the scheme, two roles are defined, which are: (1) the user (U_i) and (2) the EPR information system server (S_j). Jung et al.'s scheme goes as follows.



Table 4.2.1. Notations of the biometric-based scheme

Notation	Description
U_i	The mobile user
S_j	The EPR information system server (in Jung et al.'s scheme)
LS_j	The license server (in our scheme)
ID_i	The identity of U_i
PW_i	The password of U_i
B_i	The biometric information of U_i
K	The secret key of S_j
x	The secret key of LS_j
r_1	The random number generated by U_i
r_2	The random number generated by S_j
T_l	The timestamp
$h(.)$	One way hash function
$H(.)$	Bio-hash function
\parallel	Concatenation operator
\oplus	Bitwise XOR operator

4.2.1 User Registration Phase

In the user registration phase of Jung et al.'s scheme, the mobile user must provide a unique identity, a password and some biometric data on a registration request. Then, the user sends the registration request to the EPR information system server. Below are the details of Jung et al.'s registration phase.

Step 1: U_i inputs ID_i and PW_i and imprints B_i on his or her mobile device.

Then, U_i computes $RPW_i = h(PW_i \parallel H(B_i))$ and sends the registration request $\langle ID_i, RPW_i \rangle$ to S_j via a secure channel.

Step 2: Upon receiving the message, S_j verifies the user's identity. If it is valid, S_j computes $N = h(ID_i \parallel RPW_i)$ and $v = N \oplus K$, where K is S_j 's secret key. Then S_j issues a smart card with $(v, H(\cdot), h(\cdot))$ in it to U_i via a secure channel.

Step 3: Upon receiving the smart card, U_i computes $e = h(ID_i \parallel PW_i \parallel H(B_i))$. Finally, U_i inputs e into the smart card. Now the smart card stores $(v, H(\cdot), h(\cdot), e)$.

4.2.2 Login and Authentication Phase

In this phase, U_i establishes a common session key with S_j , and the two parties perform mutual authentication through a public channel. Jung et al.'s login and authentication phase goes as follows:

Step 1: First, U_i inserts the smart card, inputs ID_i and PW_i , and imprints B_i . Then, U_i computes $e' = h(ID_i \parallel PW_i \parallel H(B_i))$ and verifies whether e' and e are equal. If the verification fails, this session is terminated. Otherwise, U_i chooses a random number r_1 and computes $RPW_i = h(PW_i \parallel H(B_i))$, $N = h(ID_i \parallel RPW_i)$, $DID_i = ID_i \oplus N$, $C_1 = ID_i \oplus r_1$, and $C_2 = h(ID_i \parallel N \parallel r_1)$. Then U_i sends the authentication request $\langle DID_i, v, C_1, C_2 \rangle$ to S_j via an insecure channel.

Step2: Upon receiving the message, S_j computes $r'_1 = C_1 \oplus ID'_i$, $C'_2 = h(ID'_i \parallel v \oplus K \parallel r'_1)$. S_j verifies whether $C'_2 = C_2$. If C'_2 passes the verification, S_j chooses a random number r_2 and computes $a = r_2 \oplus h(r'_1 \parallel C'_2)$ and $b = h(C'_2 \parallel r_2 \parallel r'_1)$. Finally, S_j sends $\langle a, b \rangle$ to U_i via an insecure channel.

Step3: Upon receiving the message, U_i computes $r'_2 = a \oplus h(r_1 \parallel C_2)$ and $b' = h(C_2 \parallel r'_2 \parallel r_1)$. Then U_i verifies whether $b' = b$. If b' passes the verification, S_j is authenticated. U_i computes $C_3 = h(r_1 \parallel r'_2 \parallel C_2 \parallel h(ID_i \parallel RPW_i))$ and sends it to S_j via an insecure channel.

Step4: Upon receiving the message, S_j computes $C'_3 = h(r'_1 \parallel r_2 \parallel C'_2 \parallel v \oplus K)$ and verifies whether $C'_3 = C_3$. If C'_3 passes the verification, U_i is authenticated. S_j computes a session key $SK_{U_i, S_j} = h(r'_1 \parallel r_2 \parallel a \parallel b \parallel ID'_i)$, and U_i also computes $SK_{U_i, S_j} = h(r_1 \parallel r'_2 \parallel a \parallel b \parallel ID_i)$. Then, U_i and S_j communicate by using SK_{U_i, S_j} .

4.2.3 Password Change Phase

With a password change phase, Jung et al.'s scheme makes it possible for U_i to change passwords freely on the mobile device without having to be authenticated by S_j prior to the password change. Below are the details of Jung et al.'s password change phase.

Step1: U_i inserts the smart card, inputs ID_i and PW_i , and then imprints B_i . Then, U_i computes $e' = h(ID_i \parallel PW_i \parallel H(B_i))$ and verifies whether e' and

e are equal. After passing the verification of e' , U_i inputs a new password PW_i^{new} and computes $e^{new} = h(ID_i \parallel PW_i^{new} \parallel H(B_i))$. Finally, U_i replaces the current value e with e^{new} . Now the password change phase is finished.

4.3 Cryptanalysis of Jung et al.'s Scheme

Here we will point out a couple of weaknesses of Jung et al.'s scheme we have found. Below are the details.

4.3.1 Known Secret Key of Server

In Jung et al.'s scheme, the secret key of the EPR information system server can be easily figured out by an outsider. In the registration phase, upon receiving $\langle ID_i, RPW_i \rangle$, the EPR information system server computes $N = h(ID_i \parallel RPW_i)$ and $v = N \oplus K$, where K is the secret key. After that, the server sends $\langle v, h(\cdot), H(\cdot) \rangle$ to the user, who stores the data. In the login and authentication phase, the user computes an anonymous identity using N , where $N = h(ID_i \parallel RPW_i)$. In addition, v is stored in the smart card. Hence, the user can easily figure out the server's secret key K by computing $K = N \oplus v$.

4.3.2 User Anonymity Problem

In Jung et al.'s login phase, the log-in message includes U_i 's anonymous identity DID_i , where $DID_i = ID_i \oplus N$. However, since the anonymous identity DID_i stays the same and is used in each login communication, an attacker who does not know the real identity of the user can still trace the fixed DID_i . Then, by observing the long-term behavior of a specific anonymous identity DID_i , the attacker might be able to guess who the user is based on some background knowledge of the user's behavior patterns.

4.4 The Biometric-based Scheme for DRM

To develop a user authentication scheme for the DRM system that is applicable to mobile device users, we have adapted Jung et al.'s design and mended the weaknesses. Our new scheme also has three phases, and they are: (1) the user registration phase, (2) the login and authentication phase, and (3) the password and biometric data renewal phase. The details of our new scheme are as follows.

4.4.1 User Registration Phase

In the user registration phase, U_i provides a unique identity, a password and some biometric data on a registration request, which U_i sends to the license server (LS_j). The registration phase of the proposed scheme is illustrated in Fig. 4.4.1. and described in detail below.

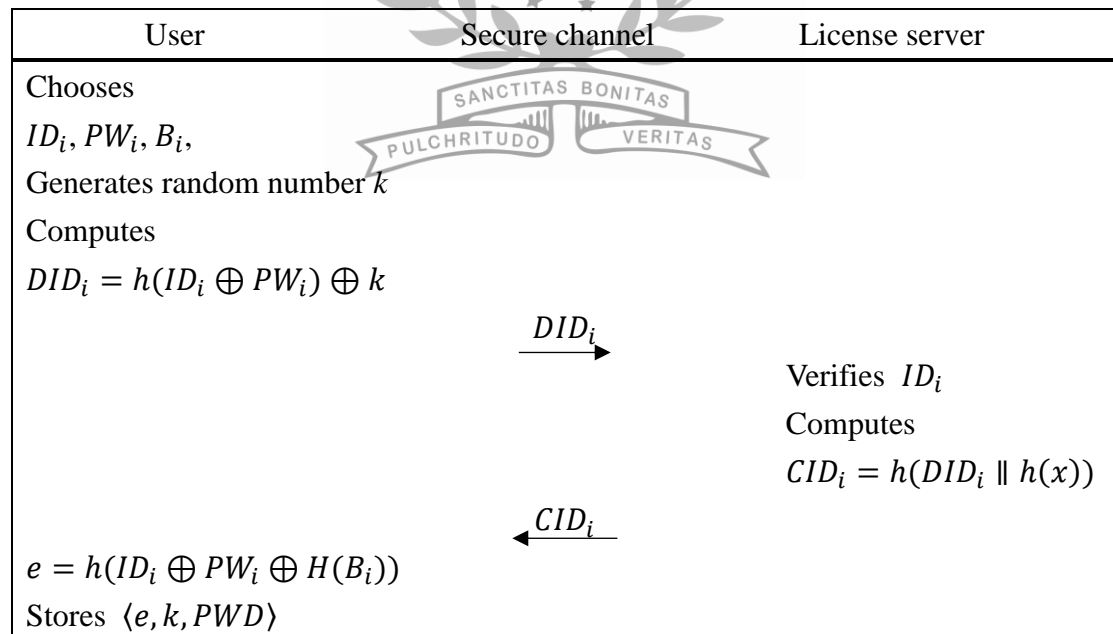


Fig. 4.4.1 User registration phase of our improved biometric-based scheme

Step 1: U_i inputs ID_i and PW_i , imprints B_i on his or her mobile device, and generates a random number k . After U_i computes $DID_i = h(ID_i \oplus PW_i) \oplus k$, U_i sends a registration request $\langle DID_i \rangle$ to LS_j through a private channel.

Step 2: Upon receiving the registration request, LS_j checks to confirm that this is a registered identity. If it is, the registration request is rejected, and the communication is terminated. Otherwise, S_j computes $CID_i = h(DID_i \parallel h(x))$, where x is LS_j 's secret key. Finally, LS_j sends $\langle CID_i \rangle$ to U_i through the private channel.

Step3: Upon receiving the message, U_i computes $e = h(ID_i \parallel PW_i \parallel H(B_i))$. U_i stores $\langle e, k, CID_i \rangle$ into the mobile device.

4.4.2 Login and Authentication Phase

In this phase, if U_i wants to access a digital content on his or her mobile device, U_i will need the content key. To achieve the goal, U_i establishes an authentication session with LS_j . Once the user's identity is verified, LS issues the content key. The login and authentication phase of our scheme is illustrated in Fig 4.4.2., and the detailed steps are given below.

Step1: U_i inputs ID_i and PW_i and imprints B_i on the mobile device. U_i verifies whether e' and e are equal, where $e' = h(ID_i \parallel PW_i \parallel H(B_i))$. If e' checks out, U_i generates two random numbers k^{new}, r_1 and computes $DID_i = h(ID_i \oplus PW_i) \oplus k$, $N_i = CID_i \oplus r_1$, $DID_i^{new} = h(ID_i \oplus PW_i) \oplus k^{new}$, $DID_{DC} = ID_{DC} \oplus r_1$, $F_i = DID_i^{new} \oplus r_1$ and $G_1 = h(DID_i^{new} \parallel ID_{DC} \parallel CID_i \parallel$

$r_1 \parallel T_i$), where ID_{DC} is the digital content U_i wishes to access, and T_i is the current timestamp generated by U_i . Finally, U_i sends the authentication request $\langle N_i, DID_i, DID_{DC}, F_i, G_i, T_i \rangle$ to LS_j through a public channel.



User	Public channel	License server
Inputs ID_i and PW_i Imprints B_i $e' = h(ID_i \oplus PW_i \oplus H(B_i))$ Verifies $e' =? e$ Generates k^{new} and r_1 Computes $DID_i = h(ID_i \oplus PW_i) \oplus k$ $N_i = CID_i \oplus r_1$ $DID_i^{new} = h(ID_i \oplus PW_i) \oplus k^{new}$ $DID_{DC} = ID_{DC} \oplus r_1$ $F_i = DID_i^{new} \oplus r_1$ $G_i = h(DID_i^{new} \parallel ID_{DC} \parallel CID_i \parallel r_1 \parallel T_i)$	$\langle N_i, DID_i, DID_{DC}, F_i, G_i, T_i \rangle$ Verifies $ T'_i - T_i < \Delta T_i$ Computes $CID_i = h(DID_i \parallel h(x))$ $r_1 = CID_i \oplus N_i$ $DID_i^{new} = F_i \oplus r_1$ $ID_{DC} = DID_{DC} \oplus r_1$ $G'_i = h(DID_i^{new} \parallel ID_{DC} \parallel CID_i \parallel r_1 \parallel T_i)$ Verifies $G'_i =? G_i$, searches $KEY_{ID_{DC}}$ Generates r_2 $CID_i^{new} = h(DID_i^{new} \parallel h(x))$ $N_j = CID_i \oplus r_2$ $F_j = CID_i^{new} \oplus r_2$ $Q_j = KEY_{ID_{DC}} \oplus r_2$ $G_j = h(CID_i \parallel CID_i^{new} \parallel r_2 \parallel KEY_{ID_{DC}} \parallel T_j)$	$\langle N_j, F_j, Q_j, G_j, T_j \rangle$ Verifies $ T'_j - T_j < \Delta T_j$ $r_2 = CID_i \oplus N_j$ $CID_i^{new} = F_j \oplus r_2$ $KEY_{ID_{DC}} = Q_j \oplus r_2$ $G'_j = h(CID_i \parallel CID_i^{new} \parallel r_2 \parallel KEY_{ID_{DC}} \parallel T_j)$ Verifies $G'_j =? G_j$ and stores $KEY_{ID_{DC}}$ Replaces CID_i and k with CID_i^{new} and k^{new}

Fig 4.4.2. Authentication phase of our improved biometric-based scheme

Step2: Upon receiving the message from U_i at time T'_i , LS_j first verifies the time delay in message transmission by checking whether $|T'_i - T_i| < \Delta T_i$, where ΔT_i represents the maximum transmission delay or preset acceptable delay threshold. If the verification is satisfied, LS_j computes $CID_i = h(DID_i \oplus h(x))$, $r_1 = CID_i \oplus N_i$, $DID_i^{new} = F_i \oplus r_1$, $ID_{DC} = DID_{DC} \oplus r_1$, $G'_1 = h(DID_i^{new} \parallel ID_{DC} \parallel CID_i \parallel r_1 \parallel T_i)$ and verifies whether $G'_1 = G_1$. If the authentication fails, the communication is terminated. Otherwise, LS_j searches and finds the key $KEY_{ID_{DC}}$ of the digital content and generates a random number r_2 . Then LS_j computes $CID_i^{new} = h(DID_i^{new} \oplus h(x))$, $N_j = CID_i \oplus r_2$, $F_j = CID_i^{new} \oplus r_2$, $Q_j = KEY_{ID_{DC}} \oplus r_2$, and $G_j = h(CID_i \parallel CID_i^{new} \parallel r_2 \parallel KEY_{ID_{DC}} \parallel T_j)$, where T_j is the current timestamp generated by LS_j . Finally, LS_j sends the information $\langle N_j, F_j, Q_j, G_j, T_j \rangle$ to U_i over the public channel.

Step3: Upon receiving the message from S_j at time T'_j , U_i first verifies the time delay in message transmission by checking whether $|T'_j - T_j| < \Delta T_j$, where ΔT_j represents the maximum transmission delay or preset acceptable delay threshold. If the condition is satisfied, U_i computes $r_2 = CID_i \oplus N_j$, $CID_i^{new} = F_j \oplus r_2$, $KEY_{ID_{DC}} = Q_j \oplus r_2$, and $G'_j = h(CID_i \parallel CID_i^{new} \parallel r_2 \parallel KEY_{ID_{DC}} \parallel T_j)$. Then U_i verifies whether $G'_j = G_j$. If the authentication is a success, U_i stores $KEY_{ID_{DC}}$ and replaces CID_i and k with CID_i^{new} and k^{new} .

4.4.3 Password and Biometric Data Renewal Phase

This phase is for U_i to freely change his or her password and biometric data on the mobile device without having to contact LS_j . Below are the details of the password and biometric data renewal phase.

Step1: After inputting ID_i , PW_i and imprinting B_i , U_i computes $e' = h(ID_i \parallel PW_i \parallel H(B_i))$ and verifies whether e' equals e . If $e' = e$, then U_i inputs a new password PW_i^{new} and imprints new biometric data B_i^{new} . U_i computes $e^{new} = h(ID_i \parallel PW_i^{new} \parallel H(B_i^{new}))$, and from now on the old value e is replaced with the new value e^{new} . This completes the password and biometric data change phase.

4.5 Analyses of Our Improved Biometric-based Protocol

This section will cover the correctness, security, and performance of the proposed scheme. First, we will use the result of a Burrows–Abadi–Needham logic (BAN logic) check to confirm the correctness of the proposed scheme [3, 35]. Then, we shall analyze the security of the proposed scheme to show that it satisfies some important security requirements and is strong against possible attacks. Finally, we will provide the result of a performance comparison among several related protocols to show the superior efficiency and cost-effectiveness of the proposed scheme.

4.5.1 Correctness Proof Based on BAN Logic

The BAN logic, which is a well-acknowledged method for the correctness check of cryptographic schemes, is used to analyze our authentication protocol [3, 35]. First, we will have some notations defined, goals set up, and an assumption made. Then, we will see how the BAN logic verification turns out. With A , B defined as participators and X as a formula, here are some instances to show the syntax and notations of the BAN logic.

Table 4.5.1. The notations of Ban logic

Notation	Description
$A \equiv X$	A believes X is true
$A\triangleleft X$	A holds or sees formula X
$A \equiv B$	A believes B 's action. E.g., $A \equiv B \equiv X$ means that A believes B believes X is true
$A \sim X$	A once said formula X
$\#(X)$	X is fresh, which means X is recent or X is a nonce
$\langle C \rangle_X$	Combine condition C using X
$(C)_X$	Perform the hash operation on C using X
<u>Rule 1</u>	<u>Rule 2</u> can be derived from <u>Rule 1</u> .
<u>Rule 2</u>	E.g., $\frac{A \text{ creates random } X}{A \equiv\#(X)}$ means that A creates X , so A believes X is fresh

i. Goals

In order to check the correctness of our authentication protocol, we will set two goals. The legal user (U_i) and the legal server (LS_j) are the participators in our proposed scheme. Since U_i and LS_j must compute private values CID_i and CID_i^{new} to do mutual authentication, our scheme can be said to have the following two goals: (1) S_j believes that the value CID_i is true; (2) U_i believes that S_j holds or sees the value CID_i^{new} . These two goals are shown as G1 and G2 in the language of the BAN logic as follows:

$$G1. S_j|\equiv U_i\triangleleft CID_i$$

$$G2. U_i|\equiv S_j|\sim CID_i^{new}$$

ii. Assumption

In order to analyze our scheme by using the BAN logic, we have made an assumption as follows:

$$A1. U_i\triangleleft CID_i$$

iii. Verification

With the goals set up and assumption made, now we are ready to apply a BAN logic check to verify the correctness of our new scheme. The details and the steps of the proof are as follows:

Message 1. $U_i \rightarrow S_j : \{(r_1)_{CID_i}, (r_1)_{CID_i}, DID_i\}$

$$V1. S_j \triangleleft \{(CID_i)_{r_1}, (r_1)_{CID_i}, DID_i\}$$

$$V2. \frac{S_j \triangleleft DID_i, S_j \triangleleft h(x)}{S_j \triangleleft CID_i}$$

$$V3. \frac{S_j \triangleleft CID_i, S_j \triangleleft (r_1)_{CID_i}}{S_j \triangleleft r_1}$$

$$V4. \frac{S_j \triangleleft CID_i, S_j \triangleleft r_1, S_j \triangleleft (r_1)_{CID_i}}{S_j | \equiv U_i \triangleleft CID_i} \text{ (G1)}$$

Message 2. $S_j \rightarrow U_i : \{(r_2)_{CID_i}, (CID_i^{new})_{r_2}, (r_2, CID_i^{new})_{CID_i}\}$

$$V5. U_i \triangleleft \{(r_2)_{CID_i}, (CID_i^{new})_{r_2}, (r_2, CID_i^{new})_{CID_i}\}$$

$$V6. \frac{U_i \triangleleft CID_i, U_i \triangleleft (r_2)_{CID_i}}{U_i \triangleleft r_2}$$

$$V7. \frac{U_i \triangleleft r_2, U_i \triangleleft (CID_i^{new})_{r_2}}{U_i \triangleleft CID_i^{new}}$$

$$V8. \frac{U_i \triangleleft CID_i, U_i \triangleleft r_2, CID_i^{new}, (r_2, CID_i^{new})_{CID_i}}{U_i | \equiv S_j | \sim CID_i^{new}} \text{ (G2)}$$

According to V4, S_j believes that U_i holds the private value CID_i . Similarly, according to V8, U_i believes that S_j once said the private value CID_i^{new} . As a result, we can infer that our authentication protocol is correct.

4.5.2 Security Analysis

Besides fixing the problems of Jung et al.'s scheme, we shall also examine the

security of the proposed scheme by checking if it satisfies several important security requirements and if it is strong enough to withstand some possible attacks. Table 4.5.2. shows how the proposed scheme compares with several other schemes of DRM architecture [7-9, 26] in terms of some security standards. Then we will give proof as to why we can say that the proposed scheme lives up to all the security standards listed.

Table 4.5.2. Security comparison among related schemes in Chapter 4

Scheme/proposition	1	2	3	4	5	6
Chen [9]	x	✓	✓	✓	✓	-
Chang et al. [8]	x	✓	✓	✓	✓	-
Chang et al. [7]	x	x	✓	x	✓	x
Mishra et al. [26]	x	✓	✓	✓	✓	✓
The proposed scheme	✓	✓	✓	✓	✓	✓
1. Dynamic user anonymity	3. Mutual authentication		5. Replay attack resistance			
2. Stolen mobile device attack resistance	4. Insider attack resistance		6. Off-line password guessing attack resistance			

i. Dynamic User Anonymity

In the registration phase of the proposed scheme, U_i computes a mobile user anonymous identity DID_i using a random number k . After LS_j receives DID_i , LS_j computes a secret value CID_i and sends it to U_i . Then, for each communication, U_i computes a new anonymous identity DID_i^{new} using a new random number k^{new} , and LS_j also computes a new secret value CID_i . Since U_i and LS_j both generate their own random numbers for every communication, an attacker cannot relate any two messages exchanged, and therefore the real identity of U_i cannot be traced. This means

the proposed scheme satisfies the requirement of dynamic user anonymity.

ii. Stolen Mobile Device Attack Resistance

Since U_i has $\langle e, k, CID_i \rangle$ stored in his or her mobile device, an adversary can steal U_i 's mobile device and obtain the stored information. However, the adversary has no clue about the identity and the password, and there is no biometric data of U_i 's. As a result, the adversary cannot have e verified due to the lack of $\langle ID_i, PW_i B_i \rangle$. Therefore, the adversary can do nothing with the stolen mobile device.

iii. Mutual Authentication

U_i and LS_j must authenticate each other before any further steps can be taken. In the login and authentication phase of the proposed scheme, LS_j and U_i check whether G_i and G_j are correct respectively. Only when all the verifications are successful can the communication continue. Obviously, the proposed scheme satisfies the requirement of mutual authentication between user and server.

iv. Insider Attack Resistance

In the proposed scheme, the user does not directly provide his or her real identity and password; instead, in the registration phase as well as the login and authentication phase, what U_i sends to LS_j is DID_i , where $DID_i = h(ID_i \oplus PW_i) \oplus k$. Such a design keeps LS_j from learning PW_i , which is hidden by using the random number k . This means the proposed scheme can withstand the insider attack.

v. Replay Attack Resistance

Suppose that an adversary intercepts the user's login and authentication request

$\langle N_i, DID_i, DID_{DC}, F_i, G_i, T_i \rangle$. Since G_i includes a timestamp generated by U_i , the request is only valid during that very communication session. In other words, if the adversary tries to login to the server by replaying the intercepted login and authentication request, the authentication will fail because the request has expired. Therefore, we can say that the proposed scheme is secure against the replay attack.

vi. Off-line Password Guessing Attack Resistance

If an attacker has stolen the mobile device and knows $\langle e, k, CID_i \rangle$, the attacker still cannot obtain U_i 's password and cannot work out the value e by computing $e = h(ID_i \oplus PW_i \oplus B_i)$ due to the lack of U_i 's biometric data B_i . Therefore, the proposed scheme is secure against the password guessing attack.

4.5.3 Performance Analysis

To have a clue how well our new scheme can perform, we have made a comparison of computation cost among some related schemes [7-9, 26]. According to [11, 16] the actual cost of computation time for a one-way function T_h is 0.2ms. As Table 4.5.3 shows, among the related schemes, the proposed scheme is the one that uses the least one-way hash functions and therefore is the fastest of them all.

Table 4.5.3. Performance comparison among related schemes in Chapter 4

Scheme	Login and authentication phase	
	Number of one-way hash functions executed	Time cost
Chen [9]	14	≈ 2.8 ms
Chang et al. [8]	10	≈ 2.0 ms
Chang et al. [7]	14	≈ 2.8 ms
Mishra et al. [26]	16	≈ 3.2 ms
The proposed scheme	9	≈ 1.8 ms

Chapter 5 A Novel Authentication Scheme for DRM

Based on Elliptic Curve Cryptography

Due to the rapid development of computer science and associated technologies, various text documents, multimedia data, software and many other forms of contents are now created, stored, and processed digitally, and almost all traditional contents of special value such as paper documents, music or video tapes, and a lot more, if possible, have also been digitized and managed digitally. As the Internet makes data transmission easy and fast, digital contents of all kinds can be spread all over the world at a shocking speed. Along with such amazing swiftness and convenience, however, modern computer and communication technologies have also brought various kinds of issues associated with digital rights management. Digital rights management (DRM) systems are access control technologies used to restrict the use, modification, and distribution of proprietary hardware and copyrighted works. Now, in view of modern people's heavy dependence on their mobile devices, we consider it a good idea to design a DRM scheme on the basis of elliptic curve cryptography (ECC) because ECC is a very good mobile device level security tool. In this paper, we shall review Amin et al.'s 2016 scheme and point out some security weaknesses we have found. Then, with the security flaws mended, we shall propose an improved ECC-based protocol for DRM that is especially suitable for applications on mobile devices.

5.1 Introduction

5.1.1 Background

As a result of the fast development of computer technologies, data or media of all kinds including text documents, multimedia data, software and many other forms are

now put together and handled as digital contents. In addition, more and more traditional contents originally in their physical, analog, or broadcast forms such as paper documents, analog multimedia data, and a lot more that are worthy of careful preservation have also been converted into digital contents. On the other hand, the booming advancement of the Internet has made it extremely easy and fast to spread all kinds of data around. As the quantities of the digital contents put up and spread out on the Internet grow exponentially, people are getting more and more used to obtaining information and receiving entertainment through the Internet [18, 20, 33]. In fact, nowadays digital contents are way too easy to spread and to obtain than they should, especially on the Internet. In many parts of the world, unauthorized downloading of digital contents remains a serious problem, causing great losses to the copyright owners. Therefore, the enforcement of copyright protection of digital contents is a big issue, and the development of an ideal digital rights management (DRM) system is essential so it can be guaranteed that only copyright owners or authorized users have access to the copyrighted digital media [8-9, 12, 26, 34, 44].

Many traditional authentication schemes of DRM systems were constructed on the basis of the RSA cryptosystem or a smart card system. However, on the mobile device, RSA is too heavy a burden as far as the computation load is concerned. In 1987, Koblitz and Miller first proposed the elliptic curve cryptosystem (ECC). ECC operates at a much lower computation cost than RSA, and the reason is that ECC has a smaller key size than any traditional public key cryptosystem. For example, ECC uses a 160-bit key, whereas RSA uses a 1024-bit key. Therefore, compared with RSA, ECC is obviously far more suitable for mobile device applications, and that is why in this paper we will propose a novel authentication scheme for anonymity and digital rights management based on ECC [1, 24].

On the other hand, users of all kinds of digital contents may probably end up having to register with and login to multiple servers if different digital contents are provided by different servers and if there is not a mechanism to integrate separate servers into a system. This means digital content users have to keep multiple ID-password pairs, which is a lot of trouble. To put multiple servers together into an integrated system and make digital content access an enjoyable experience for the user, we will review Amin et al.'s 2016 scheme, which is suitable for multi-server environments, and propose our improved scheme based on ECC suitable for DRM systems [2, 13-14, 25].

5.1.2 Related works

In recent years, a lot of research efforts have been invested in the development of digital rights management systems. Generally speaking, there are two paths from which most DRM system developers so far have chosen one to follow: (1) biometric verification and (2) smart card. Little has been mentioned about the possibility of constructing a DRM system based on ECC. In 2015, Zhang et al. made a difference and proposed a provable secure and efficient digital rights management authentication scheme based on elliptic curve cryptography using smart cards [38]. Inspired by Zhang et al.'s work, we have also designed an ECC-based DRM authentication scheme that is an improved version of Amin et al.'s scheme [2]. Below is a quick review of the literature on DRM:

■ Biometric-verification-based works on DRM

In 2008, Chen proposed a secure and traceable E-DRM system based on mobile device [9]. Chen's scheme is the first DRM authentication scheme to use

biometric verification. Besides, the computation cost is low, so Chen's scheme is suitable for mobile device. In 2010, Chang et al. found some weaknesses in Chen's scheme. They pointed out that an attacker could easily intercept the key and steal the digital content, and the mobile user would not be able to tell if anything had been tampered [8]. In order to improve Chen's scheme, Chang et al. proposed an efficient and reliable E-DRM protocol for mobile environments. Similarly, Chang et al.'s protocol was a DRM authentication scheme based on biometric verification. In 2013, Chang et al. pointed out that Chang et al.'s 2010 scheme was vulnerable to the stolen device attack and would cause major trouble when the mobile user needed to change from an old mobile device to a new one [7]. To solve these problems, Chang et al. proposed a practical secure and efficient enterprise digital rights management mechanism suitable for mobile environment. In 2015, Mishra et al. showed that Chang et al.'s scheme was weak against the off-line password-guessing attack and the insider attack [26]. To mend these security flaws, Mishra et al. proposed an anonymous and secure biometric-based enterprise digital rights management system for mobile environment.

■ Smart-card-based works on DRM

In 2009, Zhang et al. proposed the first three-role DRM system authentication scheme using smart card [39]. In 2013, Yang et al. pointed out that Zhang et al.'s scheme was weak against the stolen smart card attack and the insider attack. In order to fix these weaknesses, Yang et al. proposed an enhanced digital rights management authentication scheme based on smart card [37]. Soon after, Mishra et al. demonstrated that Yang et al.'s scheme was vulnerable to the

password guessing attack and the denial of service attack [27]. In 2015, Zhang et al. also proposed a session key attack against Yang et al.'s scheme [38]. To surmount the weakness, Zhang et al. proposed a provable secure and efficient digital rights management authentication scheme using smart card based on elliptic curve cryptography.

In addition to those works mentioned above that were specifically designed to be applied in DRM systems, there may also be some schemes that were originally meant for something else but turn out to be just as applicable in DRM systems. For example, Amin et al.'s scheme is a design for multi-server environment, but the key concept of the scheme, namely the multi-server mode, can be applied to make a DRM system more practical and user-friendly. Therefore, in this research, we have built from Amin et al.'s multi-server mode and designed a secure authentication scheme for DRM [2]. This way, mobile users only need to register once, and then they can contact multiple servers. Hence, this paper shall review and cryptanalyze Amin et al.'s scheme and then offer an improved version that is suitable for DRM systems.

5.2 Review and Cryptanalysis of Amin et al.'s Scheme

In this section, we review and cryptanalyze Amin et al.'s scheme [2]. The notations used in the scheme are listed in Table 5.2.1. Please note that the same notations will also be used in our improved scheme. Amin et al.'s scheme includes four phases, which are (1) the server registration phase, (2) the user registration phase, (3) the login and authentication phase, and (4) the password renewal phase. Designed as a privacy-aware anonymous user authentication scheme for distributed mobile cloud computing environments, Amin et al.'s scheme defines three roles: (1) the system

administrator (SA), (2) the cloud server (SP_j), and (3) the user (U_i). Note that Amin et al.'s scheme is meant for multi-server environment. The details of the phases are as follows:

Table 5.2.1. Notations of the scheme based on ECC

Notation	Description
U_i	The user
SP_j/LS_j	The cloud server in Amin et al.'s scheme/ The license server in our scheme
SA	System administrator
ID_i	Identity of U_i
PW_i	Password of U_i
f_i	Biometric data of U_i
ID_{s_j}	Identity of SP_j/LS_j
S_j	Secret key of SP_j/LS_j
s	Master secret key of SA
p	Large prime number
P	Generator of group G_1
P_{pub}	Public key of system; $P_{pub} = sP$
T_l	Timestamp
a, b, c	Random numbers
\parallel	String concatenation operation
\oplus	Bitwise XOR operation

5.2.1 Server Registration Phase

In the server registration phase, SP_j chooses the identity ID_j and sends it to SA through a secure private channel. Then SA computes $S_j = \frac{1}{s+H_1(ID_j)}P$ and sends S_j

back to SP_j through a secure private channel.

5.2.2 User Registration Phase

In the user registration phase, the mobile user registers with the system administrator. The user registration phase runs as follows:

Step 1: U_i chooses an identity ID_i , a password PW_i , and provides some biometric data f_i , and then U_i sends ID_i and some personal credentials to SA through a private channel. Then SA verifies ID_i along with the personal credentials and computes $PK_j = H_1(S_j \parallel ID_{S_j})$ for all servers. Then SA sends $\langle (ID_{S_1}, PK_1), (ID_{S_2}, PK_2), \dots, (ID_{S_j}, PK_j) \rangle$ to U_i through a secure channel.

Step 2: Upon receiving the message, U_i encrypts it as $PKE = E_{H_1(ID_i \parallel PW_i \parallel f_i)}((ID_{S_1}, PK_1), (ID_{S_2}, PK_2), \dots, (ID_{S_j}, PK_j))$. U_i computes $F_i = H_1(ID_i \parallel PW_i \parallel f_i \parallel PK_1 \parallel PK_2 \parallel \dots)$ and stores $\langle PKE, F_i \rangle$ into the mobile device.

5.2.3 Login and Authentication Phase

In this phase, U_i establishes a common session with SP_j and performs mutual authentication through a public channel. The login and authentication phase goes as follows:

Step 1: U_i inputs ID_i, PW_i, f_i and decrypts PKE . The mobile device computes $F_i^* = H_1(ID_i \parallel PW_i \parallel f_i \parallel PK_1 \parallel PK_2 \parallel \dots)$ and verifies it with F_i . If F_i^* checks out, U_i selects SP_j 's information for login. U_i selects the random number $a_i \in Z_q^*$ and computes $K_{(x,y)} = a_i(PK_j P) = (K_{xij}, K_{yij})$, $A_i = a_i P$, $B_i = H_2(ID_i \parallel a_i P \parallel T_i \parallel K_{xij})$, and $IDK_i = E_{K_{xij}}(ID_i, T_i)$. And then U_i sends $\langle IDK_i, A_i, B_i, T_i \rangle$ to SP_j through a public channel.

Step 2: Upon receiving the message at time T_i^* , SP_j verifies $|T_i^* - T_i| \leq \Delta T_i$, where ΔT_i is the acceptable time delay. If T_i^* passes the verification, SP_j calculates $PK_j = H_1(S_j \parallel ID_{Sj})$, $K_{(x,y)} = a_i(PK_j P) = (K_{xij}, K_{yij})$, $(ID_i, T_i) = D_{K_{xij}}(IDK_i)$, and $B_i^* = H_2(ID_i \parallel a_i P \parallel T_i \parallel K_{xij})$. If $B_i^* \neq B_i$, SP_j rejects the communication. Otherwise, SP_j picks a random number $b_j \in Z_q^*$ and calculates $A_j = b_j P$, $B_j = H_2\left(\begin{matrix} ID_{Sj} \parallel b_j P \\ \parallel T_j \parallel K_{xij} \end{matrix}\right)$, $IDK_j = E_{K_{xij}}(ID_{Sj}, T_j)$, $K_{ij} = H_3(ID_i \parallel ID_{Sj} \parallel b_j PK_j(a_i P))$. Then SP_j sends $\langle IDK_j, A_j, B_j, T_j \rangle$ to U_i through an insecure channel.

Step 3: Upon receiving the message at time T_j^* , U_i verifies $|T_j^* - T_j| \leq \Delta T_j$. If T_j^* passes the verification, U_i calculates $(ID_{Sj}, T_j) = D_{K_{xij}}(IDK_j)$ and $B_j^* = H_2(ID_{Sj} \parallel b_j P \parallel T_j \parallel K_{xij})$. If $B_j^* \neq B_j$, U_i rejects the communication. Otherwise, U_i accepts the information $\langle A_j, B_j, T_j \rangle$ and the session key $K_{ij} = H_3(ID_i \parallel ID_{Sj} \parallel a_i PK_j(b_j P))$. So U_i authenticates SP_j .

5.2.4 Password Renewal Phase

This phase is for when U_i needs to change passwords and personal biometric data. For security reasons, U_i makes no contact with LS here. The password renewal phase goes as follows:

Step 1: U_i inputs ID_i, PW_i, f_i and decrypts PKE . The mobile device computes $F_i^* = H_1(ID_i \parallel PW_i \parallel f_i \parallel PK_1 \parallel PK_2 \parallel \dots)$ and verifies it with F_i . If F_i^* passes the verification, U_i inputs the new password PW_i^* or new biometric data f_i^* .

Step 2: The mobile device computes $PKE' = E_{H_1(ID_i \parallel PW_i^* \parallel f_i^*)}((ID_{S1}, PK_1), (ID_{S2}, PK_2), \dots, (ID_{Sj}, PK_j))$ and $F_i' = H_1(ID_i \parallel PW_i^* \parallel f_i^* \parallel PK_1 \parallel PK_2 \parallel \dots)$. Then the mobile device replaces $\langle PKE, F_i \rangle$ with $\langle PKE', F_i' \rangle$.

5.3 Cryptanalysis of Amin et al.'s Scheme

In this section, we will point out some weaknesses of Amin et al.'s scheme by demonstrating how some attacks can be launched to crack the security of the scheme.

5.3.1 Man-in-the-middle Attack

In the login and authentication phase, a malicious user can easily steal the private value K_{xij} . PK_j is an integer that is stored in each user's mobile device, so any legitimate but malicious user can compute other users' K_{xij} by using PK_j and A_i because $K_{xij} = PK_j \cdot A_i$. In Amin et al.'s scheme, if the illegal user intercepts the authentication message $\langle A_i \rangle$, then the illegal user will have the private value K_{xij} .

5.3.2 Forged User Identity Problem

In the authentication phase, if the server wants to obtain ID_i , the only way to do so is through IDK_i . However, any malicious user can fill in any ID_i and stay undetected by LS .

5.4 The Novel Scheme based on ECC

In order to develop a protocol suitable for the DRM system environment, we have modified Amin et al.'s protocol into a new scheme. The proposed scheme has four phases, which are (1) the license server registration phase, (2) the user registration phase, (3) the authentication and content key obtaining phase, and (4) the password renewal phase. The details of these four phases are as follows:

5.4.1 License Server Registration Phase

In the server registration phase, all the license servers must register with the

system administrator. The server registration phase runs as follows:

Step1: Any license server LS_j chooses an identity ID_{Sj} and sends it to SA through a secure channel.

Step2: Upon receiving the message, SA computes $S_j = \frac{1}{s+H_1(ID_j)}P$ and $PK_j = H_1(S_j \parallel ID_j)$, then SA stores PK_j and sends S_j to any license server LS_j through a secure channel.

Step3: Upon receiving S_j from SA , LS computes $PK_j = H_1(S_j \parallel ID_j)$ and then stores S_j and PK_j .

Fig 5.4.1. illustrates how the license server registration phase of the proposed scheme works.

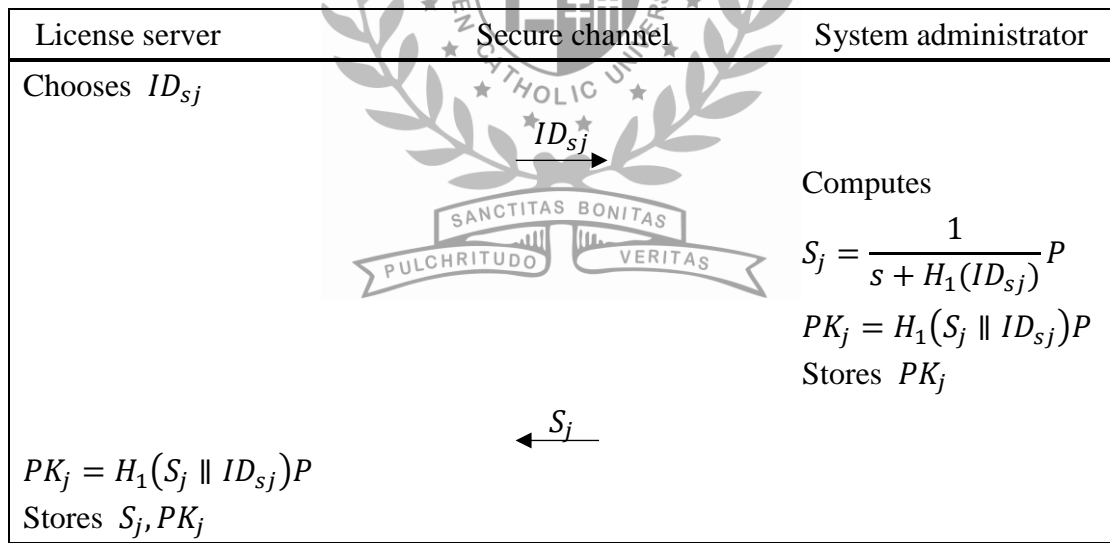


Fig 5.4.1. License server registration phase of our improved DRM scheme based on ECC

5.4.2 User registration phase

Before the mobile user U_i can obtain the digital content, U_i has to enter the

user registration phase and register with the system administrator. The user registration phase goes as follows: Fig 5.4.2 shows how the user registration phase of the proposed scheme works.

Step1: First U_i chooses a unique identity, a password, and offers some biometric data. U_i sends ID_i to SA through a secure channel. Upon receiving the message, SA verifies ID_i with some personal credentials. If the authentication fails, the registration will be canceled. If ID_i checks out, SA computes $V_{ij} = H_1(S_j || ID_i)$ and sends $\langle (ID_{s1}, PK_1, V_{i1}), (ID_{s2}, PK_2, V_{i2}), \dots, (ID_{sj}, PK_j, V_{ij}) \rangle$ to U_i through a secure channel.

Step2: Upon receiving the message, U_i encrypts it as $PKE = E_{H_1(ID_i || PW_i || f_i)}((ID_{s1}, PK_1, V_{i1}), (ID_{s2}, PK_2, V_{i2}), \dots, (ID_{sj}, PK_j, V_{ij}))$. U_i computes $F_i = H_1(ID_i || PW_i || f_i || PK_1 || PK_2 || \dots)$ and stores $\langle PKE, F_i \rangle$ into the mobile device.

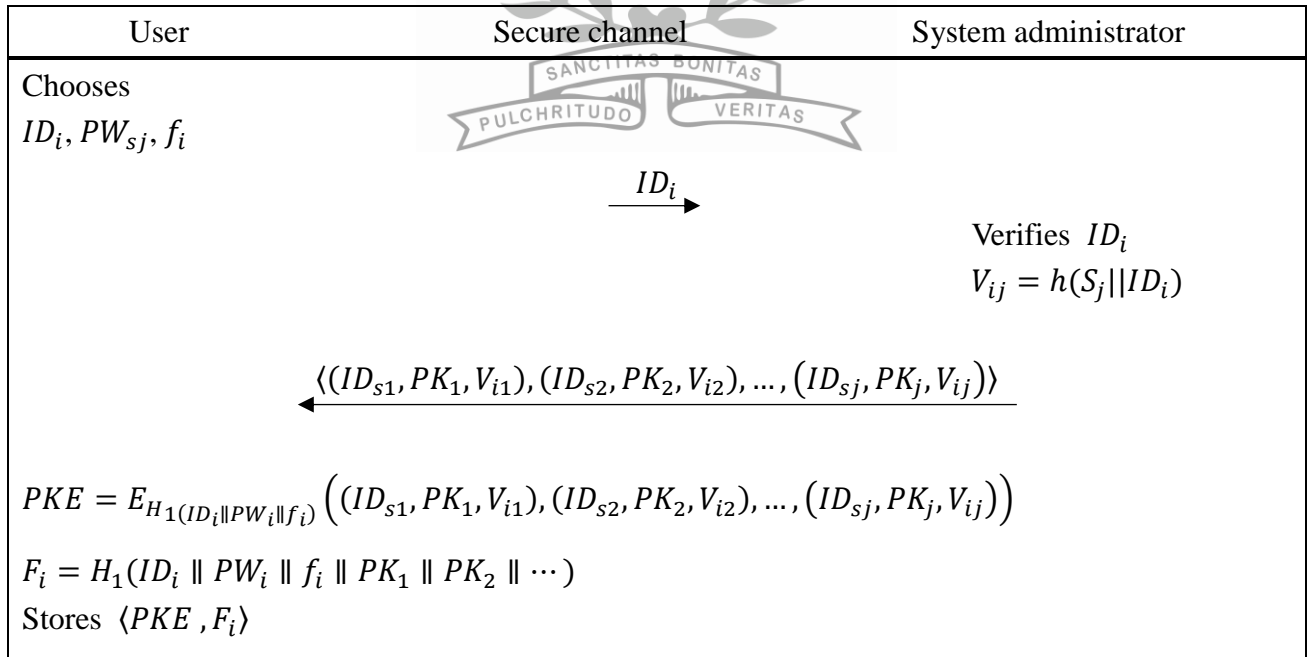


Fig 5.4.2. User registration phase of our improved DRM scheme based on ECC

5.4.3 Authentication and Content Key Obtaining phase

In this phase, U_i establishes the communication to obtain a digital content key with LS_j and performs mutual authentication through an insecure channel. The details of the authentication and content key obtaining phase are as follows:

Step 1: U_i inputs ID_i, PW_i and imprints f_i to decrypt PKE . The mobile device computes $F_i^* = H_1(ID_i \parallel PW_i \parallel f_i \parallel PK_1 \parallel PK_2 \parallel \dots)$ and verifies it with F_i . If the verification fails, U_i will not be able to log in. Otherwise, U_i selects the right license server LS_j where the digital content U_i desires is stored. U_i chooses the current timestamp T_i and the random number $a_i \in Z_q^*$. Then U_i selects the digital content identity ID_{DC} and computes $K_{(x,y)} = a_i(PK_j) = (K_{xij}, K_{yij})$, $A_i = a_iP$, $IDK_i = E_{K_{xij}}(ID_i, ID_{DC}, T_i)$, and $B_i = H_2(ID_i \parallel ID_{DC} \parallel a_iP \parallel T_i \parallel V_{ij} \parallel K_{xij})$. Finally, U_i sends $\langle IDK_i, A_i, B_i, T_i \rangle$ to LS_j through an insecure channel.

Step 2: Upon receiving the message from U_i at time T_i^* , LS_j verifies $|T_i^* - T_i| \leq \Delta T_i$, where ΔT_i is the acceptable time delay. If T_i^* checks out, LS_j calculates $K_{(x,y)} = H_1(S_j \parallel ID_{Sj})(A_i) = (K_{xij}, K_{yij})$, $(ID_i, ID_{DC}, T_i) = E_{K_{xij}}(IDK_i)$, $V_{ij} = h(S_j \parallel ID_i)$, and $B_i^* = H_2(ID_i \parallel ID_{DC} \parallel a_iP \parallel T_i \parallel V_{ij} \parallel K_{xij})$. LS_j verifies $B_i^* = B_i$. If B_i^* fails the verification, LS_j rejects the authentication. Otherwise, LS_j searches for $KEY_{ID_{DC}}$, which is the key of the digital content. Then LS_j chooses the current timestamp T_j and the random number $b_j \in Z_q^*$ and computes $A_j = b_jP$, $B_j = H_2(ID_{Sj} \parallel ID_{DC} \parallel KEY_{ID_{DC}} \parallel b_jP \parallel T_j \parallel V_{ij} \parallel K_{xij})$ and $IDK_j = E_{K_{xij}}(ID_{Sj}, ID_{DC}, KEY_{ID_{DC}}, T_j)$. Finally, SP_j sends $\langle IDK_j, A_j, B_j, T_j \rangle$ to U_i through a public channel.

Step 3: Upon receiving $\langle IDK_j, A_j, B_j, T_j \rangle$ at time T_j^* , U_i verifies $|T_j^* - T_j| \leq \Delta T_j$, where ΔT_j is the acceptable time delay. If T_j^* passes the verification, U_i computes $(ID_{sj}, ID_{DC}, KEY_{ID_{DC}}, T_j) = D_{K_{xij}}(IDK_j)$ and $B_j^* = H_2(ID_{sj} \parallel ID_{DC} \parallel KEY_{ID_{DC}} \parallel b_j P \parallel T_j \parallel V_{ij} \parallel K_{xij})$. Then U_i verifies $B_j^* =? B_j$. If B_j^* passes the verification, U_i will receive the digital content key $KEY_{ID_{DC}}$ and store $KEY_{ID_{DC}}$ in the mobile device.

Fig 5.4.3 shows how the authentication and content key obtaining phase works.



User	Public channel	License server
<p>Inputs ID_i and PW_i</p> <p>Imprints f_i</p> <p>Decrypts PKE and obtains $\{(ID_{s1}, PK_1), (ID_{s2}, PK_2), \dots, (ID_{sj}, PK_j)\}$</p> <p>Computes $F_i^* = H_1(ID_i \parallel PW_i \parallel f_i \parallel PK_1 \parallel PK_2 \parallel \dots)$</p> <p>Verifies $F_i^* =? F_i$</p> <p>Selects (ID_{sj}, PK_j, V_{ij}) and ID_{DC}</p> <p>Chooses the current timestamp T_i</p> <p>Random number $a_i \in Z_P$</p> <p>Computes $K_{(x,y)} = a_i(PK_j) = (K_{xij}, K_{yij})$</p> <p>$A_i = a_i P$, $IDK_i = E_{K_{xij}}(ID_i, ID_{DC}, T_i)$</p> <p>$B_i = H_2(ID_i \parallel ID_{DC} \parallel a_i P \parallel T_i \parallel V_{ij} \parallel K_{xij})$</p>	<p>$\langle IDK_i, A_i, B_i, T_i \rangle$</p> <p>Verifies $T_i^* - T_i < \Delta T_i$</p> <p>Computes $K_{(x,y)} = H_1(S_j \parallel ID_{sj})(A_i) = (K_{xij}, K_{yij})$</p> <p>$(ID_i, ID_{DC}, T_i) = D_{K_{xij}}(IDK_i)$</p> <p>$V_{ij} = H_1(S_j \parallel ID_i)$</p> <p>$B_i^* = H_2(ID_i \parallel ID_{DC} \parallel a_i P \parallel T_i \parallel V_{ij} \parallel K_{xij})$</p> <p>$B_i^* =? B_i$</p> <p>Chooses the current timestamp T_j</p> <p>Random number $b_j \in Z_P$</p> <p>$A_j = b_j P, IDK_j = E_{K_{xij}}(ID_{sj}, ID_{DC}, KEY_{ID_{DC}}, T_j)$</p> <p>$B_j = H_2(ID_{sj} \parallel ID_{DC} \parallel KEY_{ID_{DC}} \parallel b_j P \parallel T_j \parallel V_{ij} \parallel K_{xij})$</p> <p>$\langle IDK_j, A_j, B_j, T_j \rangle$</p>	<p>Verifies $T_j^* - T_j < \Delta T_j$</p> <p>Computes $(ID_{sj}, ID_{DC}, KEY_{ID_{DC}}, T_j) = D_{K_{xij}}(IDK_j)$</p> <p>$B_j^* = H_2(ID_{sj} \parallel ID_{DC} \parallel KEY_{ID_{DC}} \parallel b_j P \parallel T_j \parallel V_{ij} \parallel K_{xij})$</p> <p>$B_j^* =? B_j$, Obtains $KEY_{ID_{DC}}$</p>

Fig 5.4.3. Authentication and content key obtaining phase of our improved DRM scheme based on ECC

5.4.4 Password Renewal Phase

This phase is for when U_i wants to change passwords or personal biometric data, and this can be done by U_i alone. Fig 5.4.4 shows how the password renewal phase works. The details of the password renewal phase are as follows:

Step 1: U_i inputs ID_i, PW_i, f_i and decrypts PKE . The mobile device computes $F_i^* = H_1(ID_i \parallel PW_i \parallel f_i \parallel PK_1 \parallel PK_2 \parallel \dots)$ and verifies it with F_i . If F_i^* passes the verification, U_i inputs the new password PW_i^* or new biometric data f_i^* .

Step 2: The mobile device computes $PKE' = E_{H_1(ID_i \parallel PW_i^* \parallel f_i^*)}((ID_{s1}, PK_1, V_{i1}), (ID_{s2}, PK_2, V_{i2}), \dots, (ID_{sj}, PK_j, V_{ij}))$ and $F_i' = H_1(ID_i \parallel PW_i^* \parallel f_i^* \parallel PK_1 \parallel PK_2 \parallel \dots)$. Then, the mobile device replaces $\langle PKE, F_i \rangle$ with $\langle PKE', F_i' \rangle$.

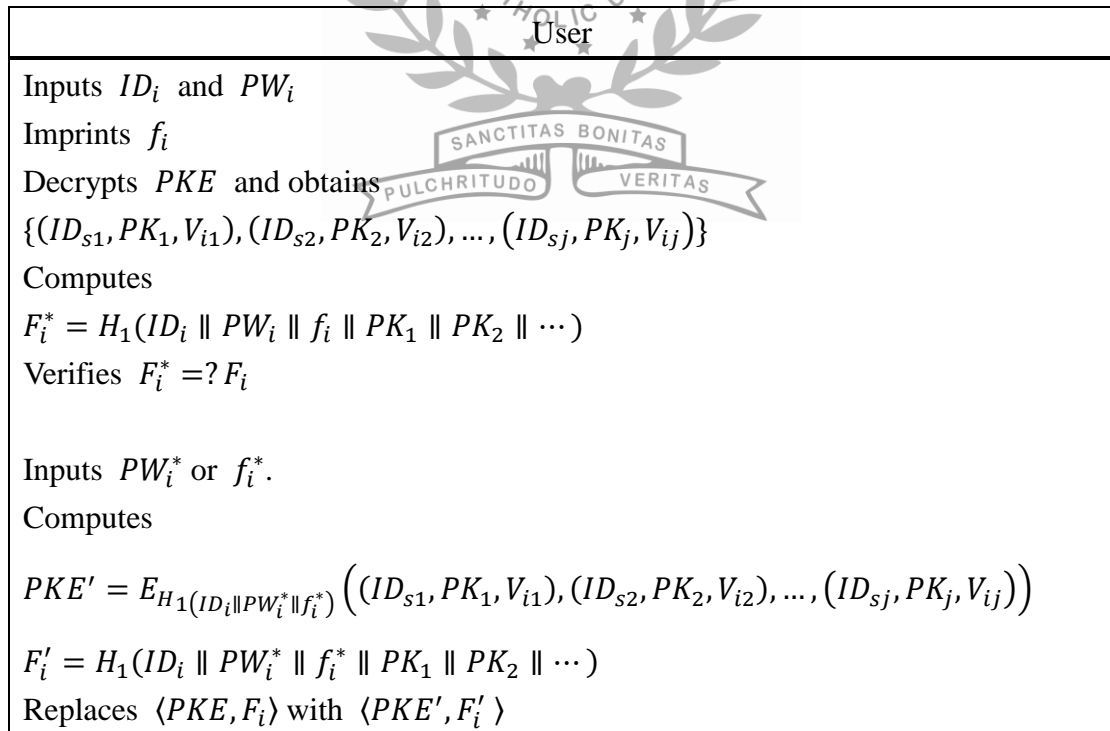


Fig 5.4.4. Password renewal phase of our improved DRM scheme based on ECC

5.5 Analyses of Our Improved Protocol Based on ECC

In this section, we shall analyze the correctness, security, and performance of our new scheme. First, we shall use the BAN logic [5, 35] to check the correctness of the scheme. Then, a security analysis will show if our new scheme can satisfy some important security requirements and if our new scheme is secure enough against some possible attacks. Finally, we shall evaluate the performance of our new scheme by comparing it with some related protocols.

5.5.1 Authentication Proof Based on BAN Logic

The BAN logic is a well-accepted method to analyze the correctness of cryptographic protocols [5, 35]. Here, we will have some notations defined, goals set up, and assumptions made first. Then, we will see how the BAN logic check turns out.

i. Notations

First of all, let's notice the syntax of the BAN logic. We define A , B as participators and X as a formula. Here are some instances to show the syntax and notations of the BAN logic.

- $A|\equiv X$ means A believes X is true.
- $A\triangleleft X$ means A holds or sees formula X .
- $A|\equiv B$ means A believes B 's action. E.g., $A|\equiv B|\equiv X$ means that A believes B believes X is true.
- $A|\Rightarrow X$ means A has complete control over X . This can be used to denote a certificate authority.
- $A|\sim X$ means A once said formula X .

- $\#(X)$ means X is fresh, which means X is recent or X is a nonce.
- $A \overset{X}{\leftrightarrow} B$ means X is a secret key or secret information shared between A and B .
- $\overset{X}{\rightarrow} A$ means X is the public key for A and X^{-1} is the private key for A .
- $\{M\}_X$ means plain text M is encrypted by X .
- $\frac{Rule\ 1}{Rule\ 2}$ means $Rule\ 2$ can be derived from $Rule\ 1$. e.g., $\frac{A\ creates\ random\ X}{A\ |\equiv\ \#(X)}$ means that A creates X , so A believes X is fresh.

ii. Goals

In order to check the correctness of our proposed scheme, we will set two goals. The goals of our scheme are stated in the syntax of the BAN logic. The legal user U_i , the legal server LS_j are the participants in our proposed scheme. Since U_i and LS_j must both compute the private value V_{ij} and both make sure that the other party also has V_{ij} , we can state the goals of our scheme as: LS_j believes that U_i holds or sees formula V_{ij} , and U_i believes that LS_j also holds or sees formula V_{ij} . The goals of the proposed scheme are shown as G1 and G2 in the language of the BAN logic below.

$$G1. LS_j | \equiv U_i \triangleleft V_{ij}$$

$$G2. U_i | \equiv LS_j \triangleleft V_{ij}$$

iii. Assumptions

In order to analyze our scheme by using the BAN logic, we have made some assumptions as follows:

$$A1. U_i |\equiv \#(a_i)$$

$$A2. LS_j |\equiv \#(b_j)$$

$$A3. U_i \triangleleft V_{ij}$$

$$A4. LS_j \triangleleft V_{ij}$$

$$A5. LS_j \triangleleft S_j$$

$$A6. U_i \triangleleft PK_j$$

iv. Verification

With the goals set up and assumptions made, now we can apply a BAN logic check to verify the correctness of our new scheme. The details and the steps of the proof are as follows:

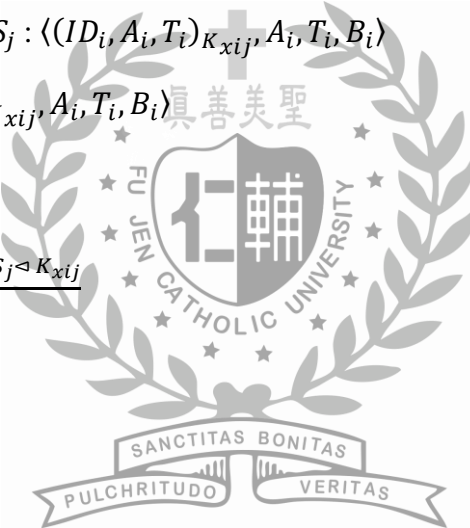
Message 1. $U_i \rightarrow LS_j : \langle (ID_i, A_i, T_i)_{K_{xij}}, A_i, T_i, B_i \rangle$

$$V1. LS_j \triangleleft \langle (ID_i, A_i, T_i)_{K_{xij}}, A_i, T_i, B_i \rangle$$

$$V2. \frac{LS_j \triangleleft A_i, LS_j \triangleleft S_j}{LS_j \triangleleft K_{xij}}$$

$$V3. \frac{LS_j \triangleleft (ID_i, A_i, T_i)_{K_{xij}}, LS_j \triangleleft K_{xij}}{LS_j \triangleleft ID_i}$$

$$V4. \frac{LS_j \triangleleft ID_i, LS_j \triangleleft S_j}{LS_j \triangleleft V_{ij}}$$

$$V5. \frac{LS_j \triangleleft V_{ij}, LS_j \triangleleft B_i}{LS_j \models U_j \triangleleft V_{ij}}$$


Message 2. $LS_j \rightarrow U_i : \langle (A_j, T_j)_{K_{xij}}, A_j, T_j, B_j \rangle$

$$V6. U_i \triangleleft \langle (A_j, T_j)_{K_{xij}}, A_j, T_j, B_j \rangle$$

$$V7. \frac{U_i \models \#(a_i), U_i \triangleleft PK_j}{U_i \triangleleft K_{xij}}$$

$$V8. \frac{U_i \triangleleft (A_j, T_j)_{K_{xij}}, U_i \triangleleft K_{xij}, U_i \triangleleft (A_j, T_j)}{U_i \models LS_j \triangleleft K_{xij}}$$

$$V9. \frac{U_i \models LS_j \triangleleft K_{xij}, U_i \triangleleft V_{ij}, U_i \triangleleft B_j}{LS_j \models U_j \triangleleft V_{ij}}$$

Finally, we can infer that the authentication and content key obtained is correct. According to V5, LS_j can correctly verify that U_i owns the private value V_{ij} . According to V9, U_i can also correctly verify that LS_j owns the private value V_{ij} . Now we can be sure that the proposed scheme is correct and that the scheme can truly achieve the goals.

5.5.2 Security Analysis

Here, the security of the proposed scheme will be examined by checking if it satisfies several important security requirements raised by some related works [2, 7, 8, 26-27, 37-39, 44]. Our discussions will include information leakage attack resistance, user and digital content anonymity, user untraceability, mutual authentication, and password guessing attack resistance.

i. Information Leakage Attack Resistance

In the authentication and content key obtaining phase of our scheme, a malicious user is not be able to steal the private value K_{xij} . The attacker will have difficulty computing K_{xij} because K_{xij} is secret information and is unknown to the attacker, where $K_{xij} = PK_j(a_i) = (K_{xij}, K_{yij})$, $PK_j = H_1(S_j \parallel ID_{S_j})P$, $A_i = a_iP$. Even if the attacker has intercepted messages $\langle IDK_i, A_i, B_i, T_i \rangle$ during transmission on the public channel, in spite of the knowledge of $A_i = a_iP$, the attacker still cannot compute K_{xij} because of the lack of PK_j . If the attacker wants to impersonate the user, the attacker must own $H_1(S_j \parallel ID_{S_j})$ or a_i . However, both values are masked in PK_j and A_i , and they are hard to retrieve because of the DLP. Hence, it is difficult to compute K_{xij} and decrypt the encrypted information.

ii. User and Digital Content Anonymity

The attacker cannot obtain the user's identity ID_i or the content's identity ID_{DC} through the authentication and content key obtaining phase, so our proposed scheme can withstand the user impersonation attack and retain digital content anonymity. Assume the attacker has intercepted the message and knows $\langle IDK_i, DID_{DC}, A_i, B_i, T_i \rangle$. The message $\langle IDK_i, DID_{DC}, B_i \rangle$ includes the user's identity and the digital content's identity, but both ID_i, ID_{DC} are under the protection of the private value K_{xij} . Therefore, the proposed scheme satisfies the requirement of user and digital content anonymity.

iii. User Untraceability

If the attacker has intercepted all messages exchanged in the authentication and content key obtaining phase, it is still difficult for the attacker to trace the user. The reason is that all the transmitted messages carry the random numbers a_i, b_j and timestamps T_i, T_j . Therefore, the proposed scheme satisfies the requirement of user untraceability.



iv. Mutual Authentication

In the authentication and content key obtaining phase, Step 2 is where LS_j authenticates U_i by computing B^*_i and verifying $B^*_i =? B_i$. Likewise, Step 3 is where U_i authenticates LS_j by computing B^*_j and verifying $B^*_j =? B_j$. Therefore, we can say that our proposed scheme satisfies the requirement of mutual authentication between U_i and SP_j .

v. Password Guessing Attack Resistance

Suppose the attacker has intercepted the messages during transmission and now knows $\langle IDK_i, DID_{DC}, A_i, B_i, T_i \rangle$. In $\langle IDK_i, DID_{DC}, B_i \rangle$, there are the user's identity and the digital content's identity, but ID_i, ID_{DC} are both protected by the private value K_{xij} , which is an unknown value to the attacker that a password guessing attack will not be able to crack.

5.5.3 Performance Analysis

Up to the present time, little research has been done to apply ECC to the field of DRM system development, so our study is a pioneering research. As a result, to see how well our new scheme can perform, we can only compare our scheme with some other ECC-based multi-server schemes with a similar architecture to that of a DRM system. Our performance comparison is on computation cost for authentication [2, 13, 42]. The following crypto-operations are used to calculate computation cost [31, 36]. The notations used in Table 5.6.1 are defined as follows:

T_{bp} : Approximate time needed to run a bilinear pairing operation ≈ 22.05 ms.

T_{pm} : Approximate time needed to run an elliptic curve scalar point multiplication operation ≈ 7.35 ms.

T_m : Approximate time needed to run a multiplication operation ≈ 0.02 ms.

T_{padd} : Approximate time needed to run an ECC point addition operation ≈ 0.01 ms.

T_{eld} : Approximate time needed to run a symmetric key encryption or decryption operation ≈ 0.13 ms.

T_h : Approximate time needed to run a one-way hash function operation ≈ 0.0004 ms.

Table 5.6.1. Performance comparison among related schemes in Chapter 5

Scheme	Computation cost for authentication	Approximate time spent (ms)
Hsieh et al.'s [13]	$2T_{bp} + 14T_{pm} + 4T_m + 15T_h$	≈ 147.42
Zhao et al.'s [42]	$2T_{bp} + 12T_{pm} + TG_H + 2T_{padd} + 7T_h$	≈ 132.35
Amin et al.'s [2]	$4T_{pm} + 5T_{eld} + 8T_h$	≈ 30.05
Ours	$4T_{pm} + 5T_{eld} + 6T_h$	≈ 30.05

As Table 5.6.1. shows, among the related schemes, our new protocol and Amin et al.'s scheme give the best performance on authentication. The difference between the two is merely two one-way hash function operations, which is well negligible. As the comparison results reveal, our new scheme is a protocol especially designed for DRM system environment that is capable of giving an impressive performance.



Chapter 6 Conclusions

In this study, we proposed three schemes for DRM system. In Chapter 3, we first introduce the DRM architecture and its related literatures. Then we showed that Mishra et al.'s scheme has digital content key storage problem and user's anonymity problem. In order to overcome the weaknesses found in Mishra et al.'s scheme, we have proposed a secure and enhanced biometric-based authentication scheme for enterprise digital rights management system. Compared with Mishra et al.'s scheme and other related schemes, our proposed scheme is efficient in terms of computational overheads. Through the informal security analysis, we have shown that our scheme is secure against some well-known attacks including stolen digital content key attack, stolen mobile device attack and off-line password-guessing attack and also supports extra important features which are necessary for an idle enterprise digital rights management system.

In Chapter 3, we have proposed a novel and secure authentication protocol for DRM system. Our new scheme uses biometric data for user identity verification because the biological characteristics are unique to each user and cannot be stolen or mistaken or forgotten. As an improved version of Jung et al.'s work, the proposed scheme provides better security protection and is especially designed for DRM systems. A BAN logic check has verified the correctness of our new protocol; besides, our security comparison and performance comparison have established that our new protocol offers the best security protection and is the fastest and most cost-effective scheme among similar protocols for DRM system.

In Chapter 4, we have proposed a novel scheme for the secure authentication of a DRM system. To design a protocol applicable to a mobile device environment, we

have decided to build our system security on the basis of ECC due to the low computation demand. In addition, the proposed scheme runs well in a multi-server scenario, so it is very suitable for applications where users get to access digital contents from different service providers, which also means our new protocol can be very useful when a platform is to be created to integrate a big number of servers into an entirety. As an improved version of Amin et al.'s work, our new protocol offers better security protection and is especially designed for DRM systems. A BAN logic check has verified the correctness of our new protocol, and some security discussions have established that our new protocol satisfies requirements of user and digital content anonymity, user untraceability, as well as mutual authentication and is secure against information leakage attacks and password guessing attacks. Finally, our performance analysis has revealed that the proposed scheme offers the best computation cost performance and is the fastest among related schemes.



References

- [1] R. Amin and G. P. Biswas, "An improved rsa based user authentication and session key agreement protocol usable in TMIS," *Journal of Medical Systems*, vol. 39, no. 8, pp. 1-14, 2015.
- [2] R. Amin, S. K. Hafizul Islam, G.P. Biswas, Debasis Giri, Muhammad Khurram Khan, and Neeraj Kuma, "A more secure and privacy-aware anonymous user authentication scheme for distributed mobile cloud computing environments," *Security and Communication Networks*, vol. 9, pp.4650-4666, 2016
DOI: 10.1002/sec.1655
- [3] M. S. Anoop, "Elliptic curve cryptography," *An Implementation Guide*, 2007, online acces:2017/05/07,
URL:http://www.infosecwriters.com/text_resources/pdf/Elliptic_Curve_AnnopMS.pdf
- [4] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," In *Proceeding of Cryptology — CRYPTO 2001, Lecture Notes in Computer Science*, Santa Barbara, California, USA, 19-23 Aug., vol. 2139, pp. 213-229, 2001.
- [5] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Transactions Computer Systems*, vol. 8, no. 1, pp. 18-36, 1990.
- [6] A. Burnett, F. Byrne, T. Dowling, and A. Duffy, "A biometric identity based signature scheme," *International Journal of Network Security*, vol. 5, no. 3, pp. 317-326, 2007.
- [7] C. C. Chang, S. C. Chang, and J. H. Yang, "A practical secure and efficient enterprise digital rights management mechanism suitable for mobile environment," *Security and Communication Networks*, vol. 6, no. 8, pp. 972-984, 2013.

- [8] C. C. Chang, J. H. Yang, and D. W. Wang, "An efficient and reliable E-DRM scheme for mobile environments," *Expert Systems with Applications*, vol. 37, no. 9, pp. 6176-6181, 2010.
- [9] C. L. Chen, "A secure and traceable E-DRM system based on mobile device," *Expert Systems with Applications*, vol. 35, no. 3, pp. 878-886, 2008.
- [10] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," in *Proceeding of Advances in Cryptology-EUROCRYPT*, Interlaken, Switzerland, 2-6 May, pp. 523-540, 2004.
- [11] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198-208, 1983.
- [12] D. He, N. Kumar, J. H. Lee, and R. Sherratt, "Enhanced three-factor security protocol for consumer USB mass storage devices," *IEEE Transactions on Consumer Electronics*, vol. 60, no. 1, pp. 30-37, 2014.
- [13] W. B. Hsieh and J. S. Leu, "An anonymous mobile user authentication protocol using self-certified public keys based on multi-server architectures," *The Journal of Supercomputing*, vol. 70, no. 1, pp. 133-148, 2014.
- [14] Q. L. Huang, Y. Yang, J. Fu, and X. Niu, "Secure and privacy-preserving DRM scheme using homomorphic encryption in cloud computing," *The Journal of China Universities of Posts and Telecommunications*, vol. 20, no. 6, pp. 88-95, 2013.
- [15] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4-20, 2003.
- [16] J. K. Jung, D. W. Kang, D. H. Lee, and D. H. Won, "An improved and secure anonymous biometric-based user authentication with key agreement scheme for

the integrated EPR information system,” *Plos One*, vol. 12, no. 1, 2017.
doi:10.1371/journal.pone.0169414

- [17] K. Kamal, A. Ghany, M. A. Moneim, N. I. Ghali, A. E. Hassanien, and H. A. Hefny, “A Symmetric Bio-Hash Function Based On Fingerprint Minutiae and Principal Curves Approach,” In *Proceeding of 3rd International Conference on Mechanical and Electrical Technology, (ICMET-China)*, Dalian, China, 26-27 Aug., vol. 1, pp. 405-410, 2011.
- [18] H. Kim, Y. Lee, and Y. Park, “A robust and flexible digital rights management system for home networks,” *Journal of Systems and Software*, vol. 83, no. 12, pp. 2431-2440, 2010.
- [19] N. Koblitz, “Elliptic curve cryptosystems,” *Mathematics of computation*, vol. 48, no. 177, pp. 203-209, 1987.
- [20] W. Ku and C. Chi, “Survey on the technological aspects of digital rights management,” In *Proceeding of International Conference on Information Security*, Toulouse, France, 23-26 Aug., vol. 3225, pp. 391-403, 2004.
- [21] C. T. Li and M. S. Hwang, “An efficient biometric-based remote user authentication scheme using smart cards,” *Journal of Network and Computer Applications*, vol. 33, issue. 1, pp. 1-5, 2010.
- [22] C. T. Li, C. Y. Weng, C. C. Lee, and C. C. Wang, “A hash based remote user authentication and authenticated key agreement scheme for the Integrated EPR information system,” *Journal of Medical Systems*, vol. 39, no. 11, pp. 1-11, 2015.
- [23] Y. Liu, C. C. Chang, and S. C. Chang, “A group key distribution system based on the generalized Aryabhata remainder theorem for enterprise digital rights management,” *Journal of Information Hiding and Multimedia Signal Processing*, vol. 6, no. 1, pp. 140-153, 2015.

- [24] V. Miller, "Use of elliptic curves in cryptography," In *Proceedings of the Advances in Cryptology (CRYPTO '85)*, Berlin, Heidelberg, 18-22 Aug., vol. 218, pp. 417-426, 1986.
- [25] D. Mishra, A. K. Das, and S. Mukhopadhyay, "A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards," *Expert Systems with Applications*, vol. 41, no.18, pp. 8129-8143, 2014.
- [26] D. Mishra, A. K. Das, and S. Mukhopadhyay, "An anonymous and secure biometric-based enterprise digital rights management system for mobile environment," *Security and Communication Networks*, vol. 8, no. 18, pp. 3383-3404, 2015.
- [27] D. Mishra and S. Mukhopadhyay, "Cryptanalysis of Yang et al.'s digital rights management authentication scheme based on smart card," *Recent Trends in Computer Networks and Distributed Systems Security*, vol. 420, pp. 288–297, 2014. DOI: 10.1007/978-3-642-54525-2_26
- [28] S. Pankanti and A. K. Jain, "Biometric recognition: security and privacy concerns," *IEEE Security Privacy Magazine*, vol. 1, no. 2, pp. 33-42, 2003.
- [29] N. Ratha, K. Karu, S. Chen, and A. K. Jain, "A real-time matching system for large fingerprint databases," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 18, no. 8, pp. 799-813, 1996.
- [30] V. Rosset, C. Filippin, and C. Westphall, "A DRM architecture to distribute and protect digital contents using digital licenses." In *Proceedings of Advanced Industrial Conference on Telecommunications/Service Assurance With Partial and Intermittent Resources Conference/E-learning on Telecommunications Workshop (Telecommunications 2005)*, Lisbon, Period, 17-20 Jul., pp. 422-427, 2005.

- [31] S. Shin, H. Yeh, and K. Kim, "An efficient secure authentication scheme with user anonymity for roaming user in ubiquitous networks," *Peer-to-Peer Networking and Applications*, vol. 8, no. 4, pp. 674-683, 2015.
- [32] D. R. Stinson, "Some observations on the theory of cryptographic hash functions," *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 259–277, 2006.
- [33] S. R. Subramanya and B. K. Yi, "Digital rights management," *IEEE Potentials*, vol. 25, no. 2, pp.31-34, 2008.
- [34] C. Wang, P. Zou, Z. Liu, and J. Wang, "CS-DRM: a cloud-based SIM DRM scheme for mobile Internet," *EURASIP Journal on Wireless Communications and Networking*, 2011, online access:2017/04/23, DOI: 10.1155/2011/837209.
- [35] J Wessels and B.V. Finance, "Application of BAN-logic," 19 April, 2001, online access:2017/05/07
URL: <http://www.win.tue.nl/ipa/archive/springdays2001/banwessels.pdf>
- [36] L. Xu and F. Wu, "Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care," *Journal of medical systems*, vol. 29, no. 2, pp. 1-9, 2015.
- [37] H. W. Yang, C. C. Yang, and W. Lin, "Enhanced digital rights management authentication scheme based on smart card," *IET Information Security*, vol. 7, no. 3, pp. 189–194, 2013.
- [38] Y. Zhang, M. K. Khan, J. Chen, and D. He, "Provable secure and efficient digital rights management authentication scheme using smart card based on elliptic curve cryptography," *Mathematical Problems in Engineering*, vol. 2015, pp. 1-16, 2015
URL: <http://dx.doi.org/10.1155/2015/807213>.
- [39] Y. C. Zhang, L. Yang, P. Xu, and Y. S. Zhan, "A DRM authentication scheme based on smart-card," In *Proceedings of the International Conference on Computational*

Intelligence and Security, Beijing, China, 11-14 Dec., pp. 202–207, 2009.

- [40] W. Zeng and K. Liu, “Sensitivity analysis of loss of corporate efficiency and productivity associated with enterprise DRM technology,” In *Proceedings of 2012 Seventh International Conference on Availability, Reliability and Security (ARES)*, Prague, Czech Republic, 20-24 Aug., 2012.
- [41] W. Zeng and A. Van Moorsel, “Quantitative evaluation of enterprise DRM technology,” *Electronic Notes in Theoretical Computer Science*, vol. 275, pp. 159-174, 2011. DOI:10.1016/j.entcs.2011.09.011.
- [42] D. Zhao, H. Peng, S. Li, and Y. Yang, “An efficient dynamic id based remote user authentication scheme using self-certified public keys for multi-server environment,” *arXiv preprint arXiv:1305.6350*, 2013, online access:2017/05/07 URL: <https://arxiv.org/pdf/1305.6350.pdf>
- [43] Y. Zhao, X. Chen, H. Ma, Q. Tang, and H. Zhu, “A new trapdoor-indistinguishable public key encryption with keyword search,” *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 3, no. 12, pp. 72-81, 2012.
- [44] P. Zou, C. Wang, Z. Liu, and D. Bao, “Phosphor: a cloud based DRM scheme with SIM Card,” In *Proceedings of Web Conference (APWEB) 2010 12th International Asia-Pacific*, Busan, South Korea, 6-8 Apr., pp. 459-463, 2010.