CONVERTIBLE DRM SYSTEM BASED ON IDENTITY-BASED ENCRYPTION

Chou-Chen Yang[1], Ju-Chun Hsiao[1], Hung-Wen Yang[2], Jyun-Yi Jiang[1]

[1]Department of Management Information Systems, National Chung Hsing University
[2]Department of Computer Science and Engineering, National Chung Hsing University

cc.yang@nchu.edu.tw, g9729001@mail.nchu.edu.tw,
phd9410@cs.nchu.edu.tw, g9629004@mail.nchu.edu.tw

ABSTRACT

With the rapid growth of the Internet, acquiring digital contents over the Internet has become commonplace. Most traditional items can be translated into digital form. That is to say the digital contents can be distributed easily and rapidly to users over the Internet. Unfortunately, situations of piracy are common and become more serious, since the digital contents can be copied and distributed easily through Internet. Thus, Digital Rights Management (DRM) is a popular tool used to protect digital contents with cryptographic technology. But there are many different DRM encryption formats that are adopted by different content providers, causing consumers can't play their contents on devices with different DRM format even though they bought it legally. In this paper, we employ identity-based encryption to allow a conversion between different DRM systems. Through the conversion process, the digital content can be used at different DRM systems and hold the legitimate use of the right.

KEYWORDS

Digital Content, Digital Rights Management (DRM), Identity-Based Encryption (IBE), Piracy

1. INTRODUCTION

Recently, the network technologies are booming and the bandwidth has been raised a lot, meanwhile, the searching engine is convenient on Internet. There is a trend that consumers look for music or multimedia film on Internet instead of traditional retail shops. If digital content providers can offer a delicate commercial model selling digital contents on Internet, e.g. iTunes store [1], it will soon be accepted by consumers.

For providers, the technology of Digital Rights Management (DRM) is a reliable tool to ensure that their merchandise will be used in pre-authorized purpose. There are many researches [2, 3, 4] that came up with different file protection structures to protect digital contents. But for consumers, unfortunately, different provider adopts different DRM system, for the time being, it restricts that consumers can only play content on particular device, such as Apple—FairPlay [9] and Microsoft—Windows Media Right Management (WMRM) [10]. Both of them, the client agent retrieves user's device hardware serial number then uploads it to register server to generate user's account. After receiving hardware serial number, the FairPlay server returns a encrypted content key by AES to client agent, but the WMRM server calculates asymmetrical key pair by RSA and embeds the private key into DLL file then returns it to the client agent. Obviously, these two DRM systems use different encryption technology and the encrypted contents can't be shared compatibly. Therefore, consumer's devices, which equip with specific DRM functionality, can only play one kind of DRM format file. The poor license portability is the main drawback of present DRM technology. How to resolve this issue to improve DRM acceptability is our target in this paper. Also for this reason, Jeong et al. [5] proposed a scheme

to convert DRM contents between different systems. In their proposal, they successfully solve the compatible problem in two different DRM systems, but their scheme has the chance that content encrypted key may be stolen by device owner in delivering phase.

In this paper, we proposed another scheme that uses the identity-based encryption concept to deliver content encrypted key on unreliable channel. The remaining parts in this paper, section 2 introduces the DRM technology and identity-based encryption. Section 3 presents our scheme and how to work on different conversion demand. Section 4 discusses the security analysis of our scheme. Section 5 is conclusions.

2. RELATED WORKS

2.1. Digital Rights Management

Because of the popularization of network infrastructure and maturity of the network environment, a lot of traditional items can be translated into the digital contents. With the rapid growth of the Internet, acquiring digital contents over the Internet has become commonplace. That is to say the digital contents can be distributed easily and rapidly to users over the Internet. Therefore, many digital content providers sell digital contents for raising revenues. Recent study predicts that the revenues for digital music may come to US$5.6 billion in 2006 [6].

Unfortunately, situations of piracy are common and become more serious, since the digital contents can be copied and distributed easily through Internet. Thus, if the digital contents are not protected or managed well, then the user may be duplicated and the digital content be distributed easily and quickly through the Internet to a large number of recipients. For instance, Napster [7] is a company offering an exchange platform for mp3 music files. Because everyone can easily search and find the music files through Napster huge music catalog, many piracies are violating the copyright of those right-holders.

According to the 2004 commercial piracy report of IFPI, the illegal music sales reached about US$4.5 billion in 2003 [8]. Thus, digital piracy will be the major problem of these digital content providers. However, in recent year, Digital Rights Management (DRM) has become an emerging issue. In order to prevent the piracy to magnify, Digital Rights Management technology will be act an important role in future. Many digital content providers expect the concept of the DRM will solve the problem of the digital piracy.

2.2. DRM Architecture

In general, there are four parties and one important framework in the DRM system architecture, that is, the content provider, the distributor, the license server, the consumer and trusted computing framework. Further information is as follow.

- Content Provider: A content provider is an entity that offers the encrypted content and establishes rules and licenses. In general, to protect the digital content, the symmetric or asymmetric cryptosystem is adopted, such as AES or RSA. The main responsibility of content provider is to hold the rights to duplicate or distribute the content.

- Distributor: The distributor is an entity that enables the encrypted content available to the consumer. A distributor enables a new distribution channel for the content provider. In general, the distributor always sets the encrypted content on its website over the Internet. Therefore, the consumer can connect to the website of the distributor and download the encrypted content.

- License server: The duty of the license server is to issue the license to consumer and handle the financial transaction data. The license server is responsible for collecting payment from the consumer and portioning out the fee to the content provider and distributor.

- Consumer: This refers to people who use DRM system to acquire the digital content by downloading from the distributor and purchase license for playing the content.

Trusted computing framework: In DRM environment, all DRM application and service are all built on the trusted computing framework. The trusted computing framework is responsible for secure distribution, execution environment, and license enforcement, supporting cryptographic functions and key management, and tamper resistance.

2.3. Audio DRM Conversion between Different DRM Content Formats

We briefly describe Jeong et al.'s scheme in this section. In their conversion process, both source and target devices install an audio DRM conversion program. The conversion program replaces the pre-existent DRM module function on the device, and manages all related works about protective files, e.g. the user's public / private key pair that used to encrypt DRM license. Then, after mutual authentication between the source and target conversion program, there are four conversion steps. First, the conversion program removes the original DRM protection in source device, and encrypts the clear resource audio file into a neutral DRM content format with program's CEK (Content Encryption Key). Second, it encrypts the CEK with public key of target device's program. Third, it sends the neutral DRM format file and encrypted CEK to target device through USB cable. After that, the target device's program can easily decrypt and get the CEK, as well as obtain the clear resource. Finally, it encapsulates the content in target DRM format and completes the conversion operation.

In their proposal, the neutral DRM format file and the encrypted CEK key are sent together through unsafe USB cable in the delivering step. If a user intentionally duplicates both data, then he can decrypt the CEK and get clear content.

2.4. Identity-based Encryption (IBE)

The concept of identity-based cryptosystem was proposed by Shamir [11] [12] in 1979 and 1984, but the first practical identity-based encryption (IBE) scheme was proposed by Boneh and Franklin [13] until 2001. There are two major characters of IBE. Firstly, IBE simplifies certificate management by using secret data receiver's unique and well-known information as public key. Secondly, the security of IBE is based on elliptic curve discrete log problem, and makes use of the property of bilinear pairing. By these two characters, IBE not only makes the key management easier, but also lower the computational cost compared to conventional public key cryptosystem. We briefly describe the IBE scheme as follows, and inherit some notations in later section.

Let *G1* be an additive cyclic group generated by *P*, whose order is a prime *q*, and *G2* be a cyclic multiplicative group of the same order *q*. We assume that the discrete logarithm problems in both *G1* and *G2* are hard, and a trusted Private Key Generator (PKG) is responsible for setting up IBE parameters and generating private key for each user. PKG defines two hash function $H_1 : \{0,1\}^* \rightarrow G1$ and $H_1' : \{0,1\}^* \rightarrow Z_q$. PKG choose a random number $s \in Z_q^*$ as the master key, and compute the master public key is $P_{pub} = sp \in G1$. Finally, PKG keeps *s* secretly and publishes $\{G1, G2, q, e, P, P_{pub}, H_1, H_1'\}$.

Assume sender *A* has to deliver a secret message to receiver *B*. Before delivering, *B* will get his private key $sH_1(ID_B)$, where ID_B is the identity of *B*, from PKG, and *A* generate a random number r, as well as calculate rp. After that, *A* computes $e(H_1(ID_B), sP)^r$ used to encrypt secret message, and delivers encrypted message with rp directly to *B*. When *B* receives this encrypted message, *B* will compute $e(sH_1(ID_B), rp)$ and decrypt the message. Based on the bilinear pairing:

$$e(H_1(ID_B), sP)^r = e(sH_1(ID_B), rp).$$

Therefore, *B* can decrypt message successfully without key agreement processing with *A* in advance.

3. PROPOSED ROBUST DRM

As we mentioned above, the technology of DRM format may be different and every content provider may keep some secret values to process his encrypted audio files. In following sections, we describe our overall framework and conversing scheme.

3.1. Notations

Portal: A multi-functional online site. Its works as a digital music store, PKG (Private Key Generator), and payment authority.

PK_i : Public key of *i*.

SK_i : Private key of *i*.

$H_x()$: Portal*'s* public hash function in IBE.

s_x : A random secret number of Portal.

P_x : A point on elliptic curve of Portal.

$h_x()$: Public hash function of Portal.

$Device_i$: The *i* th device of user.

ID_i : Unique information of $Device_i$.

N_{IDi} : A random number corresponds to ID_i. N_{IDi} is generated from Portal after user's registration, and is kept secretly by the Portal.

R : An unprotected resource (such as music files or movie files).

3.2. System Architecture

It is assumed that there are two online music stores, *Portal A* and *Portal B*, who use different DRM content format on their merchandise respectively. Someone (e.g. Tom) has three devices used to play file: $Device_1$ (ID_1) and $Device_2$ (ID_2) belong to *Portal A*'s DRM format, and $Device_3$ (ID_3) adopts *Portal B*'s DRM format. In our paper, *Portal A* and *Portal B* not only

sell music to consumers, but also need to assign private key to each consumer's devices. In order to get commercial profit and strike illegal music distribution cooperatively, we make a further assumption that both *Portal A* and *B* introduce identity-based encryption (IBE) and employ the property of bilinear pairing to facilitate consumer's converting request.

The related bilinear parameters in our proposal have been presented in section 3.1. Furthermore, we separate our conversion process into following four phases. The parameters used by *Portal A* and *B* respectively in overall system architecture and four phases are showed on Fig.1.

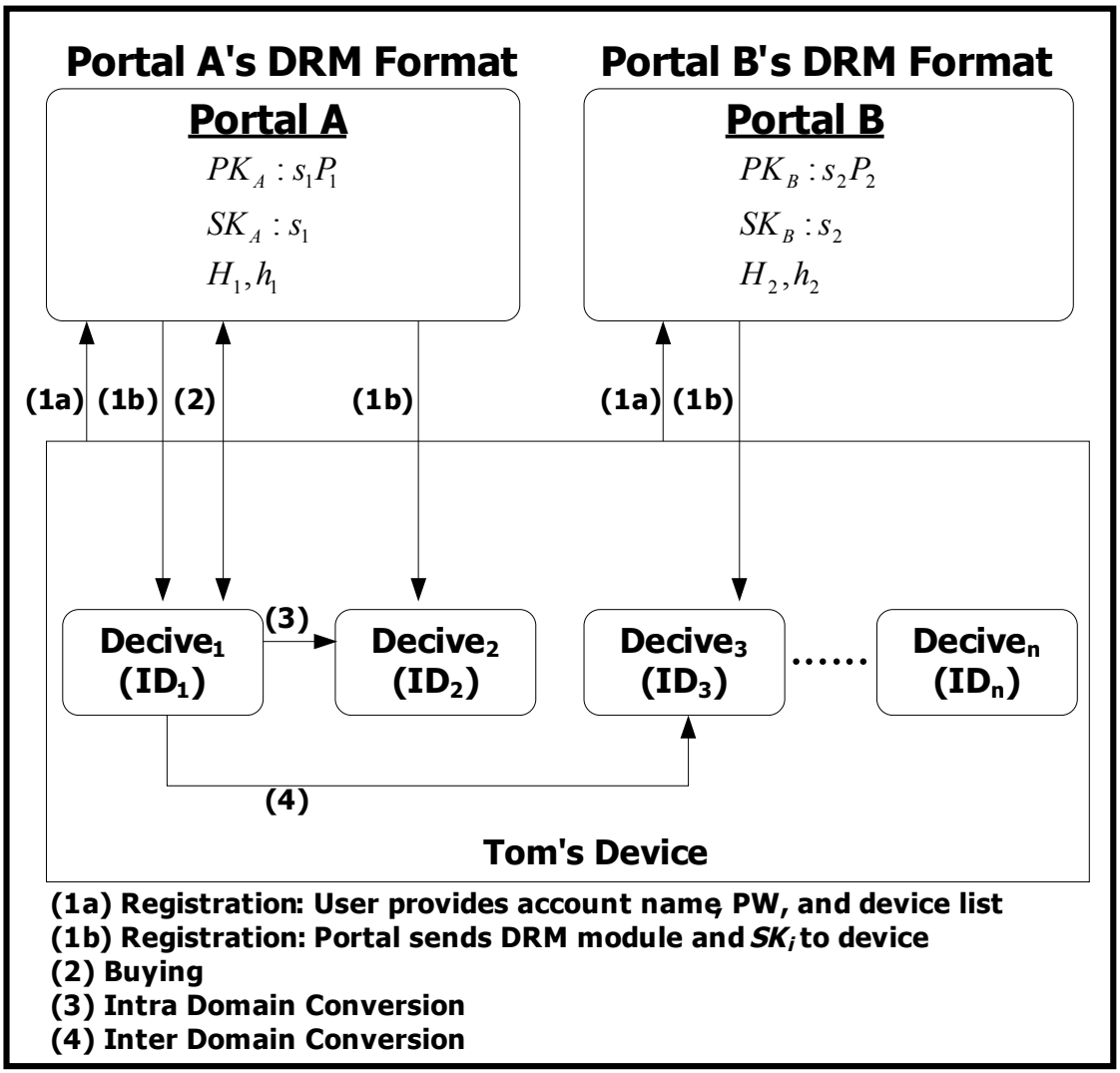

Fig.1 The overview system architecture and four phases

3.3. Registration Phase

Before user buying audio files from online music store, user has to select an account name and password *PW*, and provides some related payment information securely by reliable channel. As shown in Fig.2, the user registers to Portal with his device unique ID, such as ID_1 and ID_2. After the successful registration, the Portal sends registration reply and the processed DRM module, which is embedded with a random number N_{IDi}, respectively to user's device.

Except generating $\mathcal{N}_{IDi}$ and setting it into DRM module's internal parameter, Portal has to calculate private key $SK_i = s_i H_i(ID_i)$, then sends the private key secretly back to ID_i together with DRM module. After user installing DRM module tools on device$_1$, device$_2$, and device$_3$, the overall architecture environment is set completely. Fig.3 shows the result of successful registration process. Note that the key pair, public key and private key, is stored in device memory space outside DRM module tool. So for devices owner, he knows the exact value of every key pair, but $\mathcal{N}_{IDi}$ is embedded inside DRM module; no one knows it except Portal, even the device owner.

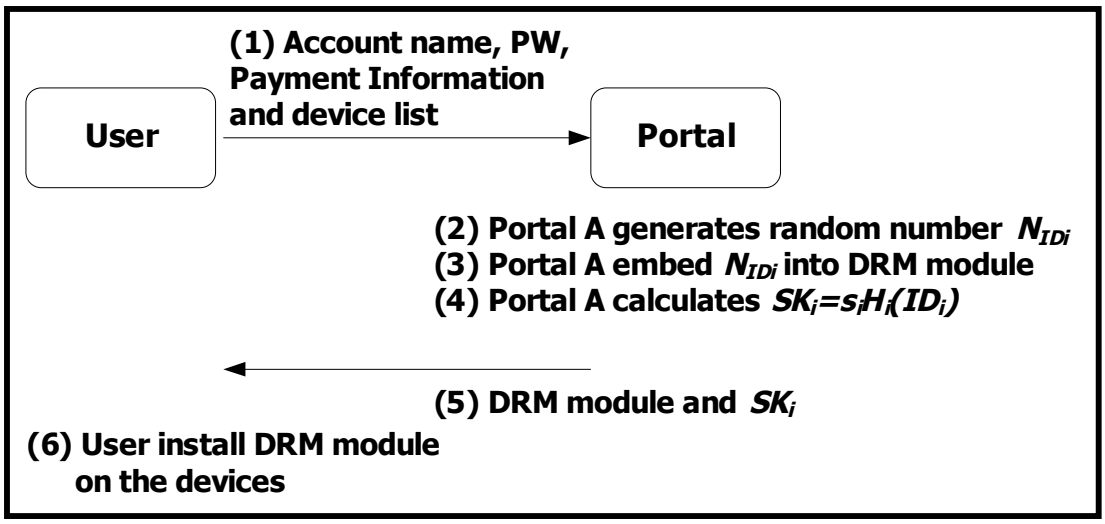

Fig.2 The steps and data flow of registration

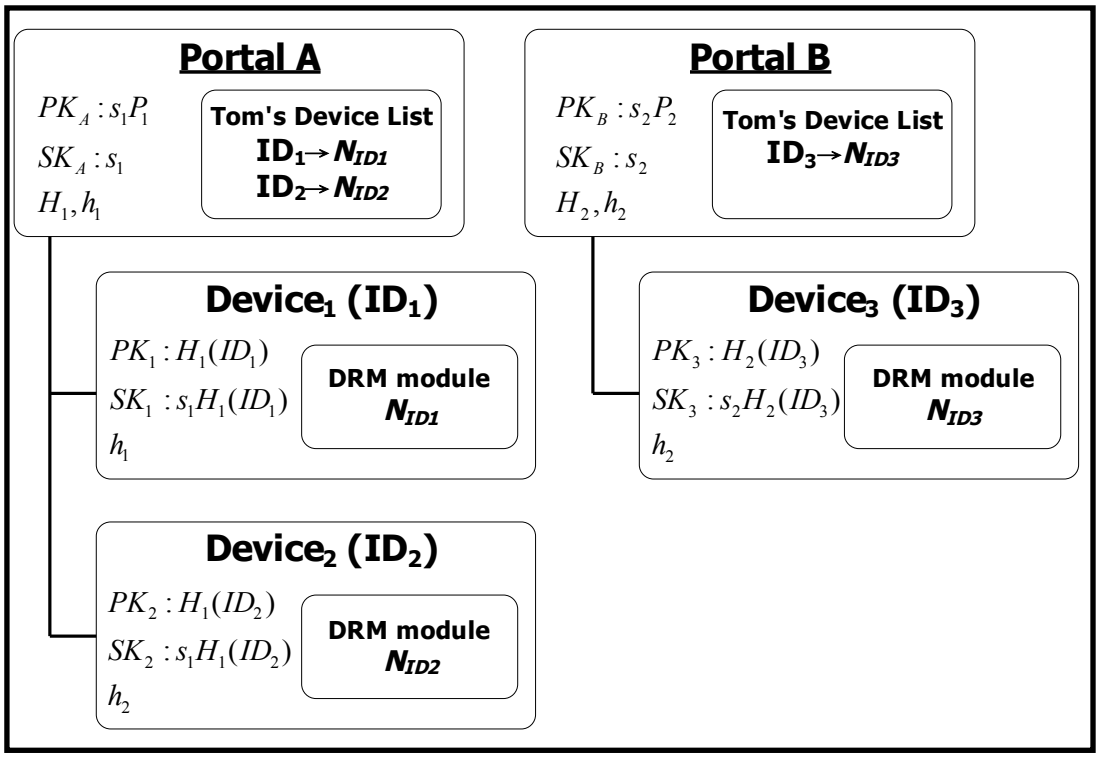

Fig.3 The architecture of successful registration process

3.4. Buying Phase

After a consumer picking a music file, he wants to buy (download) on portal, he needs to choose one device for purchase request. As shown in Fig.4, Tom sends ID_1 for buying request to *Portal A*. In order to generate symmetrical key to encrypt music file R, *Portal A* calculates $r_1 = h_1(PW_1 \| N_{ID1})$. PW_1 is Tom's account password in *Portal A*. Then, *Portal A* sets the symmetrical key $K_1 = e(H_1(ID_1), s_1P_1)^{r_1}$ coming from the identity-based encryption and bilinear pairing concept. Using K_1, *Portal A* encrypts R and sends $E_{k_1}[R]$ to ID_1.

When Tom wants to use ID_1 to play $E_{k_1}[R]$, it must be decrypted by DRM module first. DRM module tool will appear a message to ask user provide his password. Then, DRM module tool calculates $r_1 = h_1(PW_1 \| N_{ID1})$ and $e(s_1H_1(ID_1), r_1P_1) = e(H_1(ID_1), s_1P_1)^{r_1} = K_1$, thus ID_1 can play R successful.

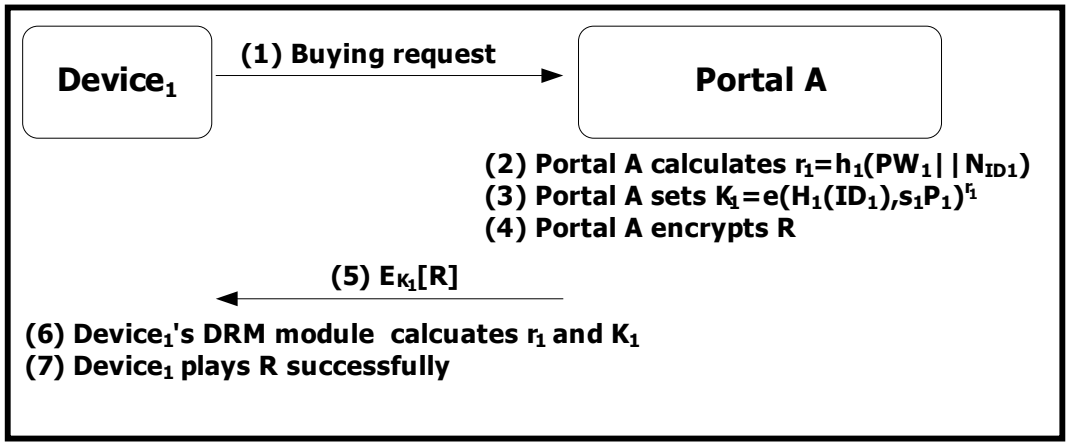

Fig.4 The steps and data flow of buying phase

3.5. Intra-Domain Conversion

If user wants to share the $E_{k_1}[R]$ from ID_1 to ID_2, first, ID_2 sends a sharing request to DRM module tool of ID_1 as shown in Fig.5. The DRM module of ID_1 will send a query message to *Portal A* to ask N_{ID2}. After *Portal A* checking Tom's device list, *Portal A* encrypts the N_{ID2} with K_1 and return back to ID_1. DRM module tool of ID_1 calculates $r_2 = h_1(PW_2 \| N_{ID2})$, $K_2 = e(H_1(ID_2), s_2P_2)^{r_2}$, and uses K_2 to encrypt R. Then, it sends $E_{k_2}[R]$ to ID_2. The DRM module tool of ID_2 can calculate r_2 and $e(s_1H_1(ID_2), r_2P_1) = e(H_1(ID_2), s_1P_1)^{r_2} = K_2$ Using K_2, ID_2 can decrypt $E_{k_2}[R]$ and play R successfully.

3.6. Inter-Domain Conversion

It is possible that user has devices of different DRM formats. In conventional DRM scheme, once a music file is encrypted in a specific DRM format, it can't be played on devices of other DRM formats; even user had bought the music legally and got rights (license). We apply the above method to solve this problem.

In our example, Tom has another device, ID_3 , which belongs to *Portal B*'s DRM format. If Tom wants ID_3 to play the music R , the DRM format conversion between ID_1 and ID_3 can be done as shown in Fig.6.

The DRM module tool of ID_3 sends a conversion request to DRM module of ID_1 . Same as section 3.5, ID_1 has to get N_{ID3} for calculating r_3 . Because ID_1 and ID_3 adopt different DRM formats, DRM module tool of ID_1 will ask *Portal A* to forward query message to *Portal B*. Portal B checks Tom's device list and returns a encrypted $E_{Pk_A}[N_{ID3}]$ to *Portal A*. After *Portal A* acquires N_{ID3} , it encrypts N_{ID3} with K_1 and returns back to ID_1 .

In the beginning of conversion process, the DRM module of ID_1 will appear a message to ask user provide his PW_2 , which is Tom's account password in *Portal B*. DRM module tool of ID_1 calculates $r_3 = h_2(PW_2 \| N_{ID3})$, $K_3 = e(H_2(ID_3), s_2 p_2)^{r_3}$, and encrypts R with K_3 , after that, delivers $E_{k_3}[R]$ to ID_3 . DRM module tool of ID_3 can calculate r_3 and $e(s_2 H_2(ID_3), r_3 P_2) = e(H_2(ID_3), s_2 P_2)^{r_3} = K_3$. Using K_3 , ID_3 an decrypt $E_{k_3}[R]$ and play R successfully.

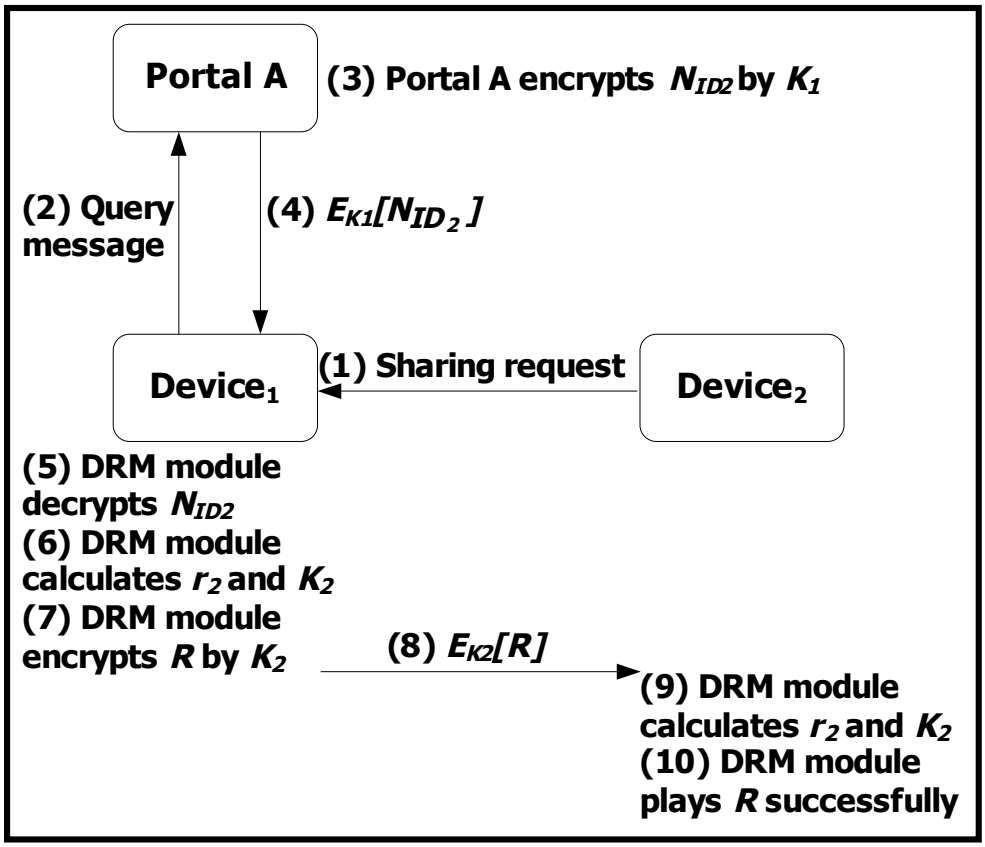

Fig.5 The steps and data flow of intra-domain conversion

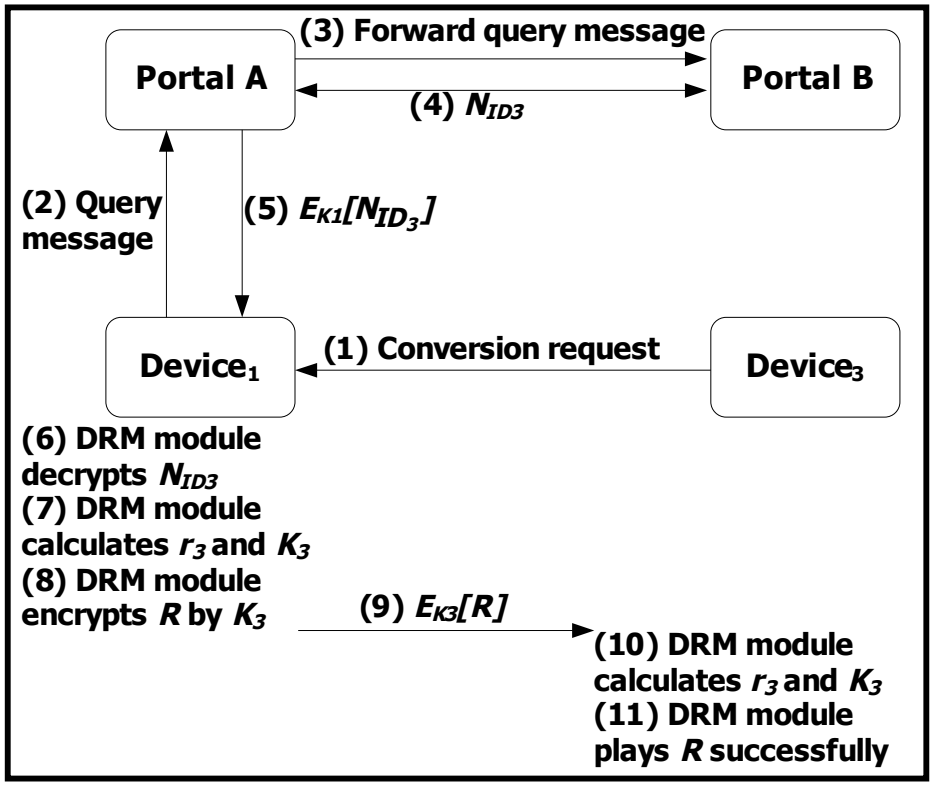

Fig.6 The steps and data flow of inter-domain conversion

4. Security Analysis

In this section, we explain three advantages in our proposed scheme that enhance the DRM system security.

Eavesdrop Attack:

In [5], if a malicious user can steal or copy the neutral DRM format file and encrypted CEK in the delivering phase, the clear content may be derived and loses the rights limitation. To avoid dishonest owner's behavior, we employ a secret value N_{IDi} that was embedded inside DRM module; therefore user can't calculate the key value even he copies the encrypted content.

Forgery DRM Module Attack:

The second security analysis is the device verification. By using the identity-based encryption and secret N_{IDi}, only the true identity DRM module can calculate the right key, thus the identity verification between any two devices is unnecessary.

Distribution Attack:

Finally, our scheme also provides access control by employing user's password in key calculation. A user bought a DRM file that can only be played on his devices. Because he is unwilling to reveal his password to others, based on the formula $r_i = h_i(PW_i \,||\, N_{IDi})$, even though he shared the encrypted content to his friends, others' DRM module can't compute the right key to decrypt it.

5. CONCLUSIONS

In this paper, we have presented a novel approach to improve the DRM system. In our proposal, each DRM module is embedded with a secret value, which is not obtainable by user, to prevent a dishonest user from revealing the protected content and distributing it on Internet. For music stores, our scheme provides a facilitated application cooperatively, it can encourage consumers to buy legal audio files; for consumers, our approach allows them play any DRM party's files on different devices.

ACKNOWLEDGEMENTS

This work was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC96-2628-E-005-009-MY3.

REFERENCES

[1] Apple – iTunes [Online]. Available: http://www.apple.com/itunes/download/

[2] Cheng Yang, Jianbo Liu, Yichun Zhang, and Aina Sui, "The Implementation Architecture of Content Protection in P2P Network," Proceedings of the International Conference on Computational Intelligence and Security Workshops, pp. 455-458, 2007.

[3] Jürgen Nützel and Rüdiger Grimm, "Potato System and Signed Media Format - an Alternative Approach to Online Music Business," Proceedings of the Third International Conference on Web Delivering of Music (WEDELMUSIC), pp. 23-26, 2003.

[4] Jae-Youn Sung, Jeong-Yeon Jeong, and Ki-Song Yoon, "DRM Enabled P2P Architecture," Proceedings of the The 8th International Conference on Advanced Communication Technology (ICACT), pp. 487-490, 2006.

[5] Yeonjeong Jeong, Junghyun Kim, and Kisong Yoon, "Audio DRM Conversion between Different DRM Content Formats," Proceedings of the International Conference on Consumer Electronics (ICCE), pp. 1-2, 2008.

[6] Jupiter Media Metrix: Press Release, "Subscriptions will account for almost two-thirds of US digital music sales in 2006," Jan. 15, 2004.

[7] Richard Stern, "Napster: a walking copyright infringement?" IEEE Micro, vol. 20 issue 6, pp.4-5, 95, Nov.-Dev. 2000.

[8] IFPI: Commercial Piracy Report 2004 http://www.ifpi.org/site-content/antipiracy/piracy-report-current.html

[9] Apple [Online]. Available: http://www.apple.com/

[10] Microsoft Windows Media–Digital Rights Management (DRM) [Online]. Available: http://www.microsoft.com/windows/windowsmedia/tw/drm/default.aspx

[11] Adi Shamir, "How to share a secret," Communications of the ACM, vol. 22, pp. 612-613, 1979.

[12] Adi Shamir, "Identity-based Cryptosystems and Signature Schemes," Proceedings of the CRYPTO 84 on Advances in cryptology, pp. 47-53, 1984.

[13] Dan Boneh and Matthew Franklin, "Identity-Based Encryption from the Weil Pairing," Proceedings of the CRYPTO 2001, pp. 213-229, 2001.

Authors

Chou-Chen Yang received his B.S. in Industrial Education from the National Kaohsiung Normal University in 1980. He received his M.S. in Electronic Technology from the Pittsburg State University in 1986, and his Ph.D. in Computer Science from the University of North Texas in 1994. He is an associate professor in the Department of Management Information System at National Chung Hsing University. His current research interests include network security, mobile computing, and distributed system.Short Biography

Ju-Chun Hsiao received the B.B.A. degree in Information Management from National Changhua University of Education in 2006. She is pursuing her M.S. in Department of Management Information Systems at National Chung Hsing University. Her current research interests include information security, digital rights management, peer-to-peer networks, and mobile communications.

Hung-Wen Yang received his B.S. in Information Management from Taichung Healthcare and Management University in 2003, and his M.S. in Information Management from Chaoyang University of Technology in 2005. He is pursuing his Ph.D in Department of Computer Science and Information Engineering, National Chung Hsing University, Taiwan. His current research interests include information security, digital rights management and mobile communications.

Jiang-Yi Jiang was born in Chiayi, Taiwan, Republic of China, on May 17, 1984. He received the B.S. in Information Management from Chang Jung Christian University, Taiwan, in 2006; the M.S. in the Department and Graduate Institute of Information Management from National Chung Hsing, Taichung, Taiwan, in 2009. His current research interests include cryptography, network security, P2P network, and digital rights management.