A Group-oriented Digital Right Management Scheme with Reliable and Flexible Access Policies

Chin-Chen Chang[1] and Jen-Ho Yang[2]
(Corresponding author: Jen-Ho Yang)

Department of Information Engineering and Computer Science, Feng Chia University[1]
100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan, R.O.C.
Department of Information and Electronic Commerce, Kainan University [2]
No. 1, Kannan Rd., Luzhu, Taoyuan County, 33857, Taiwan, R.O.C.
(Email: jenhoyang@mail.knu.edu.tw)

(Received Apr. 20, 2012; revised and accepted July 5, 2012)

Abstract

In recent years, the information protection for digital contents becomes an important issue for enterprise applications. To protect digital contents, various enterprise digital right management (E-DRM) schemes have been proposed to prevent the digital contents from illegal accesses. However, the previously related schemes did not support the digital right management for multi-user environments. In addition, these schemes are insecure in some applications. To overcome the above problems, we propose a new group-oriented E-DRM scheme with reliable and flexible access policies in this paper. The proposed scheme allows multiple users to acquire the access right, which can be dynamically determined according to the enterprise policy. In addition, no one can access the digital contents except authorized users. Compared with the related works, the proposed scheme is more reliable and flexible for enterprise applications.

Keywords: Access policy, digital content, digital right management, enterprise application

1 Introduction

With the development of computer technologies, the digital files have replaced the traditional prints. Compared with the traditional print format, the digital file format is more convenient and efficient because it can be widely spread via the Internet. Therefore, people can easily download and distribute various digital contents (e.g., electronic books, on-line music, and product specifications) anytime and anywhere.

To protect the digital contents, various digital right management (DRM) schemes [1, 7, 10] are proposed in recent years. The DRM scheme is an information protection technique that manages the access right of a digital content and prevents the confidential information from unauthorized uses. Also, the DRM scheme supports the author with the capability to specify the access rights for his/her digital content, such as reading, copying, and editing rights. For example, the author can specify whether his/her digital content can be copied, edited, or viewed by an authorized user. Once the right of the digital content has been specified, the authorized user can access the protected content anytime and anywhere until the author changes its access rights.

Furthermore, the DRM mechanism is especially important for the information protection in government institutions or private enterprises. This is because the digital contents used in government institutions or private enterprises may contain some confidential information, such as marketing plans, customer lists, and financial reports. Assume that a company employee purposely sends a sensitive document that describes the new product design to a competitive company. The above information theft may cause a large amount of financial losses for the enterprise. Thus, how to prevent the sensitive data from illegal accesses becomes an important issue for enterprise applications. To solve the above-mentioned problems, various enterprise digital right management (E-DRM) schemes [3, 8, 11] have been proposed. The E-DRM schemes prevent the confidential data from the information theft by a malicious insider of the enterprise. In addition, it also provides the management of access rights for the sensitive information.

In 2009, Chen et al. proposed a group-based E-DRM scheme for business applications [4]. To access the digital contents, an authorized user must pass the authentication by any t out of n authorization authorities in their scheme. Thus, their scheme provides the dynamic authorization which allows authorized users to access the confidential information in an enterprise. However, we find that Chen et al.'s scheme is not flexible and secure for some applications. Let us suppose a common case: company employees in the same department often cooperatively discuss, plan, and develop a team project. And, the participants in such team project need to access the same confidential documents under the protection of the E-DRM

scheme. However, Chen et al.'s scheme only allows one user to access the digital content after passing the authorization. That is, their scheme does not support the multiple users to access the digital content dynamically.

On the other hand, Chen et al.'s scheme allows that one user in a group has the ability to pass the authorization and accesses the digital content. However, the access privileges need to be restricted for the security consideration in some enterprise applications. For example, a financial report only can be allowed to read when some managers appear in a financial department at the same time. If one financial manager wants to read this report, then the access right for reading needs to be suspended for the security consideration. Therefore, it is necessary to design an E-DRM scheme with the reliable access policy in such applications.

To solve the above-mentioned problems, we propose a group-oriented E-DRM scheme with reliable and flexible access policies in this paper. In the proposed scheme, only k out of l or more users in the user group can cooperatively obtain the access right of a digital content. To get the access right, these k users need to pass the authentications by any t out of n authorization authorities. That is, the proposed E-DRM scheme provides the dynamic access and authorization policies so it can be applied to many enterprise applications. In addition, the access privileges can be restricted because only k out of l or more users can pass the authorization to access the confidential data. Compared with Chen et al.'s scheme, the proposed scheme is more practical because it can support the multi-user environments for enterprise applications. According to the above reasons, the proposed scheme is more flexible and reliable than the previously proposed works.

2 Review of Chen et al.'s Scheme

In this section, we introduce Chen et al.'s E-DRM scheme [3] as follows. There are four roles in their scheme: the author of the digital content, the package server, a group of authorization authorities with *n* members, and the user who wants to access the digital content. Here, the package server is responsible for encrypting the digital content which is packed into E-DRM format file as shown in Figure 1. In addition, the group of the authorization authorities is responsible for authenticating the user's access right for the digital content.

To manage the access right of the digital content, Chen et al.'s scheme uses the E-DRM file structure which is shown in Figure 1. The DRM file structure is divided into two parts: the content header and the encrypted digital content. The content header contains the following information. The content identity (*CID*) which is the identity of the digital content; and the type of the DRM-enable application ($DRM\text{-}AP_{type}$) is constructed for integrating the existing applications and indicating the correct DRM application (e.g., the reader or player to access the digital content). In addition, the group identity (ID_G) is the identity of the user group, and the signature (S_P) which is generated by the package server for encrypting the digital content. Moreover, the threshold value (t) is the security level of the digital content, and (*URL*) is the authorization authority's uniform resource locator.

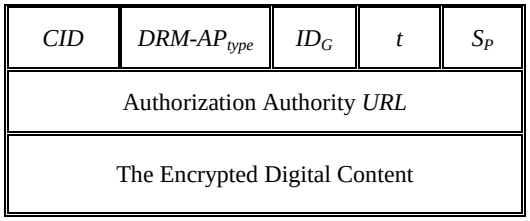

Figure 1: The DRM file structure

The notations of Chen et al.'s scheme are shown in Table 1 as follows.

Table 1: The notations of Chen et al.'s scheme

U	The user
PS	The package server
A_i	The i-th entity of the authorization authorities
ID_X	The identity of the entity X
$SymE_K(\cdot) / SymD_K(\cdot)$	The symmetric encryption/decryption function using the symmetric key K such as AES [2]
SK_X / PK_X	The secret/public key of the entity X
$Sig_{SK_x}(\cdot) / Ver_{PK_x}(\cdot)$	The signing/verifying function using any digital signature scheme such as RSA [9]
$E_{PK_x}(\cdot) / D_{SK_x}(\cdot)$	The encryption/decryption function using any public-key cryptosystem such as RSA [9]
CID	The digital content's identity
$h(\cdot)$	A secure one-way hash function

2.1 Content Package Phase

In this phase, the author sends the digital content to the package server. Then, the package server encrypts the digital content and packs it into the E-DEM formatted file. Finally, the package server generates the shadow of the encryption key using a secret polynomial and sends it to each authorization authority. The steps of this phase are shown as follows.

Step 1. The author creates the digital content M and sends it to the package server.

Step 2. The package server generates a symmetric key K_{CID} to encrypt M as $C_M = SymE_{K_{CID}}(M)$. Then, the package server generates a digital signature by computing $S_{PS} = Sig_{SK_{PS}}(h(C_M))$.

Step 3. The package server generates a secret polynomial function in the form of $f(x) = K_{CID} + a_0 + a_1 x + \ldots + a_{t-1}x^{t-1} \bmod P$, where P is a large prime and $a_0, a_1, \ldots, a_{t-1} \in [1, P-1]$ are integers.

Step 4. The package server generates the secret shadow SD_i for each authorization authority A_i, where

$SD_i = f(h(CID, ID_{A_i}, ID_G))$. Then, the package server sends SD_i to each A_i .

Step 5. The package server generates the content header including *CID*, *DRM-AP*$_{type}$, ID_G, t, S_{PS} , and the *URL* of authorization authority. Then, the package server combines the content header and C_M as the E-DRM formatted file which is shown in Figure 1. Finally, the package server publishes the E-DRM formatted file in a public directory.

2.2 License Acquiring Phase

In this phase, the user downloads the E-DRM formatted file from the package server and sends an authorization request to the group of authorization authorities. If *t* out of *n* or more authorities send their shadows to the user, then the user has the ability to get the symmetric key to decrypt the encrypted digital content. The steps of this phase are shown as follows.

Step1. The user downloads the E-DRM formatted file from the public directory in the package server. Then, the user verifies the signature S_{PS} by checking if the equation $Ver_{PK_{PS}}(S_{PS}) = h(C_M)$ holds. If the equation holds, then the user generates the signature by computing $S_U = Sig_{SK_U}(CID, ID_U, REQ, TS)$, where *REQ* is the authorization request message and *TS* is a timestamp.

Step 2. The user sends $(CID, ID_U, REQ, TS, S_U)$ to the group of authorization authorities. Then, the authorization authorities check if the equation $Ver_{PK_U}(S_U) = (CID, ID_U, REQ, TS)$ holds. If the equation holds, then each A_i uses his/her shadow SD_i to compute $C_{SD_i} = E_{PK_U}(SD_i)$. In addition, each A_i uses his/her secret key to generate the signature $S_{A_i} = Sig_{SK_{A_i}}(CID, ID_G, ID_{A_i}, Right, C_{SD_i})$, where *Right* denotes the user's access right.

Step 3. If A_i accepts the user to access the digital content, and he/she sends $(CID, ID_G, ID_{A_i}, Right, C_{SD_i}, S_{A_i})$ to the user. Afterward, the user can verify the correctness of each shadow by checking if the equation $Ver_{PK_{A_i}}(S_{A_i}) = Sig_{SK_{A_i}}(CID, ID_G, ID_{A_i}, Right, C_{SD_i})$ holds. If the equation holds, then the user computes $SD_i = D_{SK_U}(C_{SD_i})$ to get each shadow for reconstructing the symmetric key.

Step 4. If *t* out of *n* or more authorities provide their shadows, then the user can reconstruct $f(x)$ by using the Lagrange interpolation formula [6]:

$$f(x) = \sum_{i=1}^{t} SD_i \prod_{j=1, j\neq i}^{t} \frac{x - h(CID, ID_{A_i}, ID_G)}{h(CID, ID_{A_i}, ID_G) - h(CID, ID_{A_i}, ID_G)} \bmod P .$$

Therefore, K_{CID} can be reconstructed by computing $K_{CID} = f(0) \bmod P$.

Step 5. If the user obtains K_{CID} from *t* secret shadows, then he/she can compute $M = SymD_{K_{CID}}(C_M)$ to get the digital content.

According to the above descriptions, Chen et al.'s scheme has two disadvantages. First, their scheme allows that one user has the ability to pass the authorization and get the digital content. In some applications, the user's access privilege cannot be restricted using their scheme. Second, *t* out of *n* authorization authorities also have the ability to reconstruct the symmetric key K_{CID} to obtain *M*. If the digital content only can be accessed by the user, then their scheme is insecure in this assumption.

3 The Proposed Scheme

To overcome the disadvantages of Chen et al.'s scheme, we propose a group-oriented E-DRM scheme with reliable and flexible access policies in this section. The proposed scheme is divided into two phases: the package phase and the license acquiring phase. There are four roles in the proposed scheme: the author, the package server, a group of *n* authorization authorities, and a group of *l* users. Note that the notations used in the proposed scheme are shown in Table 2. Now, we introduce the proposed scheme as follows.

Table 1: The notations of the proposed scheme

G_A	A group of *n* authorization authorities
G_U	A group of *l* users
PS	The package server
A_i	The *i*-th authority of G_A
U_i	The *i*-th user of G_U
ID_X	The identity of the entity *X*
P	A large prime
$SymE_K(\cdot)/SymD_K(\cdot)$	The symmetric encryption/decryption function using the key *K* such as AES [2]
SK_X / PK_X	The secret/public key of the entity *X*
$Sig_{SK_X}(\cdot)/Ver_{PK_X}(\cdot)$	The signing/verifying function using any digital signature scheme such as RSA [9]
CID	The digital content's identity
$h(\cdot)$	A secure one-way hash function

3.1 The Content Package Phase

In this phase, the author sends the digital content to the package server. And, the package server chooses a symmetric key to encrypt the digital content. In addition, the package server packs the cipher into the E-DEM format. Then, the package server embeds the symmetric key in two secret polynomials for the user group and the authority group. Moreover, the package server generates the shadow for each user and each authorization authority according to the above polynomials. Finally, the package server sends

each shadow to each user and each authorization authority. The steps of this phase are shown as follows.

Step 1. The author generates the digital content M and sends it to the package server.

Step 2. The package server generates a symmetric key K_{CID} and compute $C_M = SymE_{K_{CID}}(M)$ to encrypt M. Then, the package server signs $h(C_M)$ by computing $S_{PS} = Sig_{SK_{PS}}(h(C_M))$.

Step 3. The package server chooses a large prime P and two integers $a \in [1, P-1]$ and $b \in [1, P-1]$ satisfying $GCD(a, b) = 1$, where $GCD(a, b)$ is the greatest common divisor of a and b. Then, the package server computes another two integers c and h satisfying $a \cdot c + b \cdot h = 1$. Note that c and h can be computed by Euclidean algorithm [5].

Step 4. The package server chooses a symmetric key $K_{CID} \in [1, P-1]$ and constructs a secret polynomial $f_A(x) = (K_{CID})^{a \cdot c} + a_0 + a_1 x + , \ldots, a_{t-1} x^{t-1} \bmod P$ for the group of authorization authorities, where $a_0, a_1, \ldots, a_{t-1} \in [1, P-1]$. In addition, the package server constructs another secret polynomial function $f_U(x) = (K_{CID})^{b \cdot h} + b_0 + b_1 x + , \ldots, b_{k-1} x^{k-1} \bmod P$ for the group of users, where $b_0, b_1, \ldots, b_{k-1} \in [1, P-1]$.

Step 5. To generate the secret shadows of the above polynomials, the package server computes $SD_{A_i} = f(h(CID, ID_{A_i}, ID_{G_A}))$ and $SD_{Ui} = f(h(CID, ID_{Ui}, ID_{GU}))$ for each U_i and A_i, respectively. Then, the package server sends SD_{A_i} and SD_{U_i} to each U_i and A_i, respectively.

Step 6. The package server constructs the E-DRM formatted file by combining the content header and the cipher C_M, where the content header contains the information: CID, $DRM\text{-}AP_{type}$, ID_G, t, k, S_{PS}, and the URL of authorization authority. Finally, the package server publishes the E-DRM formatted file in its public directory.

Note that all the communications of the above steps are performed via a secure channel.

3.2 The License Acquiring Phase

If k users want to access the digital content, then these k users choose a clerk on behalf of them to communicate with the group of authorization authorities. Then, the clerk sends a request to the group of authorization authorities for acquiring the access right. If any t out of n or more authorities accept the request and provide their shadows, then the t authorities compute one part of the symmetric key $(K_{CID})^{a \cdot c}$ and send it to the user group. To get the other part of the symmetric key $(K_{CID})^{b \cdot h}$, k out of l users need to provide their shadows. After combining two parts of the symmetric keys $(K_{CID})^{a \cdot c}$ and $(K_{CID})^{b \cdot h}$, these k users can obtain the symmetric key K_{CID} to decrypt the encrypted digital content. The detailed steps of this phase are shown as follows.

Step1. If k out of l users want to access the digital content, then these k users download the E-DRM formatted file from the public directory of the package server. Afterward, the k users can verify the signature S_{PS} by checking if the equation $Ver_{PK_{PS}}(S_{PS}) = h(C_M)$ holds. If the equation holds, then the k users choose a clerk (user clerk) on behalf of them to generate $S_{G_U} = Sig_{SK_{G_U}}(CID, ID_{G_U}, REQ, TS_{G_U})$, where REQ is a request message and TS_{G_U} is a timestamp.

Step 2. The user clerk sends the message $(CID, ID_{G_U}, REQ, TS_{G_U}, S_{G_U})$ to the group of authorization authorities. Then, each A_i can verify the signature S_{G_U} by checking if the equation $Ver_{PK_{G_U}}(S_{G_U}) = (CID, ID_{G_U}, REQ, TS_{G_U})$ holds. If the equation holds, then each A_i can ensure that the user request is valid.

Step 3. If any t out of n authorities accept the above request, then these t authorities cooperatively reconstruct $f_A(x)$ by using the Lagrange interpolation formula [5] which is shown as follows:

$$f_A(x) = \sum_{i=1}^{t} SD_{A_i} \prod_{j=1,\, j \neq i}^{t} \frac{x - h(CID, ID_{A_j}, ID_{G_A})}{h(CID, ID_{A_i}, ID_{G_A}) - h(CID, ID_{A_j}, ID_{G_A})} \bmod P$$

Then, the t authorities can obtain one part of the symmetric key $f_A(0) = (K_{CID})^{a \cdot c} \bmod P$.

Step 4. The t authorities also choose a clerk (authority clerk) on behalf of them, and the authority clerk generates a group signature by computing $S_{G_A} = Sig_{SK_{G_A}}(CID, ID_{G_A}, Right, f_A(0), TS_{G_A})$, where $Right$ is the user's access right and TS_{G_A} is a timestamp. Then, the authority clerk sends the message $(CID, ID_{G_A}, Right, f_A(0), TS_{G_A}, S_{G_A})$ to the user clerk.

Step 5. After receiving each user's shadow message $(CID, ID_{G_A}, Right, f_A(0), S_{G_A}, TS_{G_A})$, the user clerk sends it to the other (k-1) users. Then, each user can verify the authorization message by checking if $Ver_{PK_{GA}}(S_{G_A}) = (CID, ID_{G_A}, Right, f_A(0), TS_{G_A})$ holds. If the above verification holds, then each user provides his/her shadow to the other (k-1) users. If k

users provide their shadows, then each user of them can reconstruct $f_U(x)$ by the equation:

$$f_U(x) = \sum_{i=1}^{k} SD_{U_i} \prod_{j=1, j\neq i}^{k} \frac{x - h(CID, ID_{U_j}, ID_{G_U})}{h(CID, ID_{U_i}, ID_{G_U}) - h(CID, ID_{U_j}, ID_{G_U})} \bmod P .$$

Step 6. Finally, each user can obtain K_{CID} by computing $f_A(0) \cdot f_U(0)$. Then, the k users can access the digital content by computing $M = SymD_{K_{CID}}(C_M)$.

The package phase and the license acquiring phase are shown in Figure 2 and Figure 3, respectively.

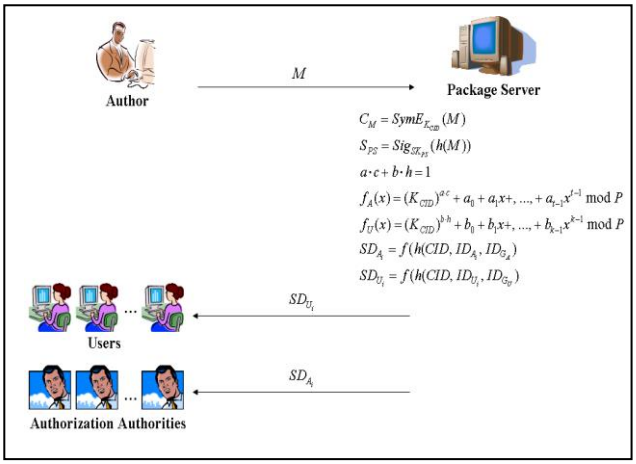

Figure 2: The package phase

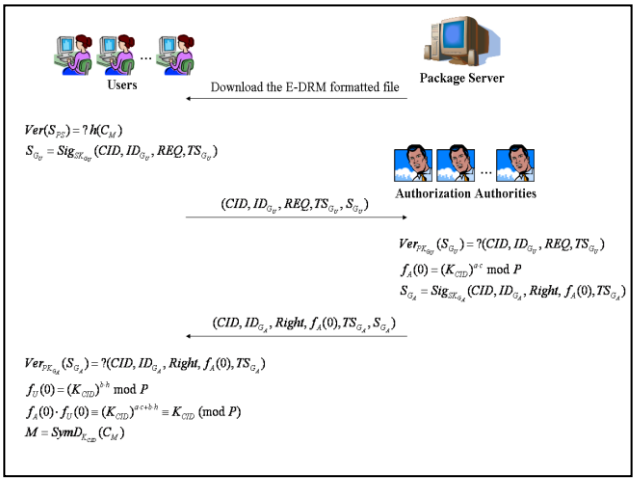

Figure 3: The license acquiring phase

According to the steps of the proposed scheme, each authorization authority does not need to encrypt his/her shadow using the public-key cryptosystem (PKC). That is, each user does not need to perform the PKC decryption to get each shadow of authorization authority. Compared with Chen et al.'s scheme, the proposed scheme eliminates the computation cost of the PKC encryption/decryption operation so the proposed scheme is more efficient.

In addition, at least k users have the ability to cooperatively reconstruct the symmetric key K_{CID}. Therefore, the user's access privilege can be restricted. Since the threshold values t and k can be changed, the security level of the digital content can be dynamically determined according to the company policy. Therefore, the proposed scheme provides the flexibility to many enterprise applications.

Besides, Chen et al.'s scheme allows that t authorization authorities have the ability to cooperatively reconstruct the symmetric key. Thus, their scheme is not secure for some applications. Unlike Chen et al.'s scheme, the proposed scheme only allows that t authorization authorities reconstruct one part of the symmetric key $(K_{CID})^{a \cdot c} \bmod P$. For these t authorities, it is impossible to obtain K_{CID} from $(K_{CID})^{a \cdot c} \bmod P$.

Therefore, the proposed scheme is suitable for the enterprise applications in which the symmetric key cannot be revealed to the authorization authorities. According to the above-mentioned advantages, the proposed scheme is more flexible and reliable than Chen et al.'s scheme.

4 Discussions

In this section, we discuss the security analyses of the proposed scheme. Besides, we give a performance comparison of the proposed scheme and Chen et al.'s scheme. Now, we show that the proposed scheme can prevent from the following attacks.

Outsider attack:

Assume that an attacker wants to get the encrypted digital content, and then he/she can download the cipher $C_M = SymE_{K_{CID}}(M)$ from the package server. To get the digital content M, the attacker needs to use the symmetric key K_{CID} to compute $M = SymD_{K_{CID}}(C_M)$. However, the attacker does not know the symmetric key K_{CID} so he/she cannot decrypt the cipher C_M.

Assume that an attacker wants to obtain the secret key K_{CID} from $(K_{CID})^{a \cdot c} \bmod P$. However, this attack is impossible because the attacker needs to face the difficulty of the discrete logarithm problem (DLP) [6].

According to the above descriptions, the outsider attack is infeasible for the proposed scheme.

Insider attack:

Assume that k malicious users want to cooperatively compute the symmetric key K_{CID} without passing the authentication, and then they can obtain $f_U(0) = (K_{CID})^{b \cdot h} \bmod P$ by using Lagrange interpolation formula. Without getting $(K_{CID})^{a \cdot c} \bmod P$ from the authorization authorities, these k users cannot obtain K_{CID} from $(K_{CID})^{b \cdot h} \bmod P$ because they need to face the difficulty of the DLP.

Similarly, t malicious authorities cannot cooperatively compute K_{CID} without getting $(K_{CID})^{b \cdot h} \bmod P$. This is because the t malicious authorities only have the ability to compute $(K_{CID})^{a \cdot c} \bmod P$ from $f_A(0) = (K_{CID})^{a-c} \bmod P$. To obtain K_{CID} from $(K_{CID})^{a-c} \bmod P$, these t malicious authorities need to face the difficulty of DLP. According to the above analysis, the proposed scheme can prevent the insider attack.

Impersonation attack:

Assume that an attacker wants to impersonate the group of users, and then he/she generates the signature $S'_{G_U} = Sig_{SK'_{G_U}}(CID, ID_{G_U}, REQ, TS)$ using a forged SK'_{G_U} and sends $(CID, ID_{G_U}, REQ, TS, S'_{G_U})$ to the authorization authorities. However, the authorization authorities can discover that $(CID, ID_{G_U}, REQ, TS, S'_{G_U})$ is sent by an attacker. This is because that $SK'_{G_U} \neq SK_{G_U}$ and $Ver_{PK_{G_U}}(S'_{G_U}) \neq (CID, ID_{G_U}, REQ, TS)$.

Assume that an attacker wants to impersonate the group of the authorization authorities, and then he/she generates $S'_{G_A} = Sig_{SK'_{G_A}}(CID, ID_{G_A}, Right, f_A(0), TS_{G_A})$. Then, the attacker sends $(CID, ID_{G_A}, Right, f_A(0), S'_{G_A}, TS_{G_A})$ to the group of users. However, the user can discover that $(CID, ID_{G_A}, Right, f_A(0), S'_{G_A}, TS_{G_A})$ is sent by an attacker because $Ver_{PK_{G_A}}(S'_{G_A}) \neq (CID, ID_{G_A}, Right, f_A(0), TS_{G_A})$. According to the above discussion, the impersonation attack is infeasible for the proposed scheme.

Replay attack:

If an attacker eavesdrops the communications between the user group and the authority group, then he/she can obtain $(CID, ID_{G_U}, REQ, TS_{G_U}, S_{G_U})$ and $(CID, ID_{G_A}, Right, f_A(0), S_{G_A}, TS_{G_A})$. Then, the attacker wants to reuse the signatures S_{G_A} and S_{G_U}. However, reusing the signatures S_{G_A} and S_{G_U} is impossible because S_{G_A} and S_{G_U} contain the timestamps TS_{G_A} and TS_{G_U}, respectively. Therefore, the proposed scheme can prevent the replay attack.

Comparisons:

Here, we analyze the computation costs of Chen et al.'s scheme and the proposed scheme. Table 3 shows the computation costs of the user side and the authority side in these two schemes. According to Table 3, we can find that the computation cost of the proposed scheme is much less than that of Chen et al.'s scheme.

Unlike Chen et al.'s scheme, the proposed scheme does not require that each authority computes his/her digital signature. In addition, the proposed scheme does not need to perform the encryption/decryption in the public key cryptosystem. That is, the user does not need to verify the individual signature generated by each authorization authority. Therefore, the proposed scheme is more efficient than Chen et al.'s scheme.

Table 2: The comparisons of computation costs

Schemes / Computations	Chen et al.'s scheme		The proposed scheme	
	User side	Authority side	User side	Authority side
PKC encryption/decryption	t	t	0	0
Signature Signing/verifying function	$t + 2$	$t + 1$	3	2
Symmetric key encryption/decryption	1	0	1	0

5 Conclusions

In this paper, we propose a group-oriented E-DRM scheme with reliable and flexible access policies. In the proposed scheme, the access right of the digital content can be dynamically determined according to the company policy. In addition, the proposed scheme has low computation cost because it does not need to perform the PKC encryption and decryption. Therefore, the proposed scheme is more flexible and efficient than the previously proposed works. Based upon the proposed scheme, we are going to investigate an efficient E-DRM scheme for mobile devices in the future.

References

[1] Adobe Lifecycle Document Security. http://www.adobe.com/products/server/Securityserver/pdfs/docsecurityserver_ds.pdf

[2] Advanced Encryption Standard. http://csrc.nist.gov/archieve/aes/

[3] Authentica Delivers Next-Generation Enterprise Rights Management Platform. http://www.authentica.com/news/pr2005/02-14-2005-ARM.aspx

[4] C. L. Chen, Y. Y. Chen, and Y. H. Chen, "Group-based authentication to protect digital content for business applications", *The International Journal of Innovative Computing, Information and Control*, Vol. 5, No. 5, pp. 1243-1251, 2009.

[5] J. Gathen and J. Gerhard, *Modern Computer Algebra*, Cambridge University Press, 2nd edition, 2003.

[6] A. J. Menezes, P. C. Orschot, and S. A. Vanstone, *Hand-book of Applied Cryptography*, CRC Press, 1996.

[7] Microsoft Windows Right Management Services System. http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx

[8] D. Mulligan, J. Han, and A. Burstein, "How DRM content delivery systems disrupt expectations of personal use, " in *Proceedings of 2003 ACM Workshop on Digital Rights Management*, pp. 77-89, 2003.

[9] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of ACM*, Vol. 21, No. 2, pp. 120-126, 1978.

[10] Windows Media Digital Rights Management. http://www.microsoft.com/windows/windowsmedia/forpros/drm/defualt.mspx

[11] Windows Rights Management Services: Protecting Electronic Content in Financial, Healthcare, Government, and Legal Organization. http://www.microsoft.com/windowsserver2003/techinfo/overview/

Chin-Chen Chang received his Ph.D. degree in computer engineering from National Chiao Tung University. His first degree is Bachelor of Science in Applied Mathematics and master degree is Master of Science in computer and decision sciences. Both were awarded in National Tsing Hua University. Dr. Chang served in National Chung Cheng University from 1989 to 2005. His current title is Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from Feb. 2005. He is currently a Fellow of IEEE and a Fellow of IEE, UK. His current research interests include database design, computer cryptography, image compression and data structures.

Jen-Ho Yang received the BS degree in Computer Science and Information Engineering from I-Shou University, Kaoshiung, Taiwan in 2002. He received his Ph.D. degree in Computer Science and Information Engineering from National Chung Cheng University, Chiayi County, Taiwan in 2009. Since 2009, he has been an assistant professor of Department of Multimedia and Mobile Commerce in Kainan University, Taoyuan County, Taiwan. His current research interests include electronic commerce, information security, cryptography, authentication mechanisms, digital right management, and fast modular multiplication algorithm.