Block-sliced DRM System for Secure Multi-Media Contents

Tae-Chul Jung[†], *and Moon-Seog Jun*[††]

[†]Samsung Advanced Institute of Technology, Postal Code 446-712, Seoul, Korea,
[††]Dept. of computer Science, Soongsil University, Postal Code 156-743, Seoul, Korea.

Summary
The improvement of computer communication and information processing technology brings the activation of multi-media content. The government tries to expand the development of cultural content into the national enterprise for promoting a growth foundation in an information-oriented society. This paper proposes an encryption method of multi-media data using a hash chain algorithm for secure multi-media contents and designs an authentication protocol using an authentication and key transmission algorithm for identifying an authorized user. Finally, this paper proposes the decryption method of multi-media content in real-time using a effective buffer scheduling method by constructing a duplicated buffer to minimize the delay time of playback at the decryption procedure.

Key words:
Hash Chain, DRM, DOI, OTP, Multimedia Contents.

1. Introduction

The improvement of computer and communication technology brings the information-oriented society with a rich set of digital contents being seamlessly available to end users. The demand of multi-media data as a digital media increases quickly. The security issues of digital copyright are very important against an illegal reproduction because digital works can be reproduced without a damage of quality. We need an information security method to guarantee the stability and security for protecting digital works, and DRM (DRM: Digital Rights Management) technology for governing the distribution of digital works.

There are various studies that protect a copyright against the violation of intellectual property rights, promote a counter plan for managing a distribution process, and provide a confident environment for the production, distribution, and usage of digital works. The main methods for protecting digital works securely are user authentication methods and data security.

User authentication means that authenticated user can use digital works without any restrictions. However, this method is not enough since the authenticated user can reproduce and distribute digital data. Data security is a method that encrypts digital data so that this problem can be solved. In encrypting data, there are two different types of algorithms. One is a private-key based algorithm and the other uses public keys. A private key algorithm is to encrypt data with one key and it provides fast operations. However, this algorithm has a problem that both the sender and the receiver must exchange the key in advance, and it requires long encryption times (e.g., encrypting large scale movies will be time consuming.) A public key algorithm uses different keys in encryption and decryption, so key exchange is more secure. However, the running time of algorithm is slower. Thus, in encrypting a large scale movie, the user typically encrypts a private key with a public key after encrypting digital data with the private key in advance. We need digital right management technologies that can apply to all types of digital work, manage them dynamically, and watch and track a digital work in real-time both on-line and off-line.

This paper proposes the method that provides an efficient user authentication and data security schemes based on public key system and a hash chain algorithm for protecting multi-media contents.

2 Related work

2.1 Conventional DRM system

We need the standardized classification and identification system for the distribution and payment of digital works through the mutual connection to commercial e-business systems to achieve a digital right management system. To protect the security and management of work, we need the automatic statistics and analysis function of digital work usage, and the function that watch and track automatically the usage breakdown to check the illegal and legal usage of digital work in the context of both on-line and off-line. Especially, copyright protection and management system can support the storage and maintenance of an objective data that proves illegal activities when a legal dispute has broken out. DRM systems must protect the movie data using not simple restrict of authorization or conventional password method but user authentication and data encryption method based on Public Key Infrastructure (PKI) for data protection and authentication.

Manuscript received October 5, 2007
Manuscript revised October 20, 2007

Figure 1 shows the DRM system that consists of publishing company, content provider, user and Clearing House. Digital contents is written by an author, and passed to a publishing company. This company describes a price, period of circulation, and directions, and sends it to distributor. Distributor encrypts the content and provides it to a user. Finally, user can use the content after paying a charge and accepting a license.

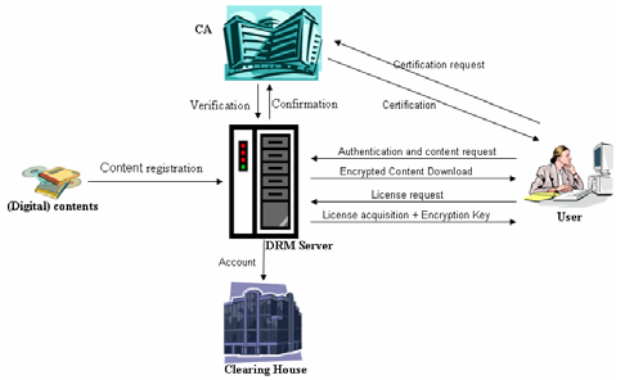

Figure 1. DRM system architecture

Digital content may be passed with the process from the production to the usage as content generation and encryption, distribution, and usage. Publisher sends a digital content to distributor with the security condition such as a copyright, usage, authentication information, charge, and audit. Distributor generates an encrypted content after constructing digital content according to the condition provided by a publisher. Encrypted content is registered on content server and user can download it via both on-line and off-line. Also, distributor decides and stores the information such as price and payment method to database, and sends it to Clearing House for handling the user payment information. User can use the content after downloading it via on-line or off-line and purchasing the execution authority through a license agent. When user receives the content license and provides a payment information after identifying the license through a Clearing House, a license agent achieves the process for user to use the content. Publisher, distributor, and user register on DRM CA (Certificate Authority) for public certification, receive a certificate, and perform the cross certification.

2.1.1 InterTrust's DRM system

This system can support the encryption and decryption for secure content, the directions of content, usage breakdown record and collection, and payment system. This system also realizes super-distribution (i.e., legal reselling of content to other users.) User can contract a business at the usage of content on his computer, and use a credit card or e-money as a payment method. .

1) InterTrust's DRM technology

InterRight Point is a core component of InterTrust's DRM, and is active between user computer and server Meta Utility. DigiBox Container loads the encrypted content and directions transmission . Direction includes a price, a payment method, playback, print, reproduction, store, and super-distribution information. Transaction Authority framework achieves the breakdown of content usage and payment.

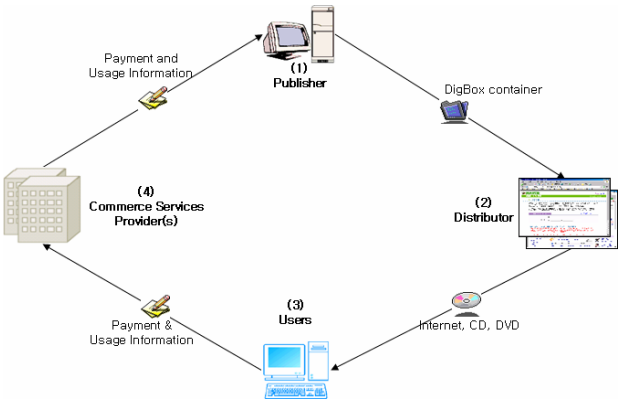

Figure 2. InterTrust DRM system

2) Receiving a license

User can receive a license from a license manager installed in computer. , An off-line payment mechanism must exist for supporting this method. Real-time playback is not supported, and user must wait long time (e.g., tens of seconds.) Secure DigiBox encrypts content with a key, so the content is not secure when a key is exposed.

Figure 3. Decryption method of InterTrust

2.1.2 Microsoft's WMRM (Windows Media Rights Manager)

In WMRM, there are a content provider and a DRM system that distributes digital contents to an end user. Rights Manager provides a media such as music and video in encrypted file format to content provider via Internet.

In WMRM, each server or client instance receive a pair of key by an individualization process, and remove cracked or unsecured instances form service list using CRL (Certificate Revocation List). CRL of Microsoft's

WMRM is distributed on Microsoft's web page, key is included in license, and license and content are distributed separately. License acquisition steps are that player requests a license to license server when client executes packaging content, server verifies user authentication and payment condition, server generates a license, and server transmits a license to the player of client. Player checks the licenses transmitted by a server, and plays the content according to the directions. Figure 4 shows these steps.

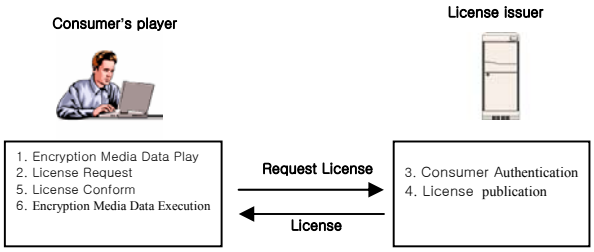

Figure 4. Certification process of WMRM license

Microsoft's WMRM generates encrypted content key after combining Key ID and Key seed, and Key ID included in content header is packaged and distributed with content. Key seed is kept in Clearing House. Both key ID included in content and key seed managed by a server are needed to generate decryption key. WMRM is loaded in window media player and used widely, but real-time decryption technology is only applied to Microsoft's streaming file format such as WMV and WMA and cannot be applied to the movie such as MPEG and MPEG 4.

2.2.3 I-Frame encryption method

The key used in partial encryption system that uses I-Frame of movie GOP (Group Of Picture) as a asymmetric key is stored in database, and key used in encryption is encrypted with a user public key and transmitted to a client at the playback. Only I-Frame is decrypted, stored with B and P Frame in a buffer, and played.

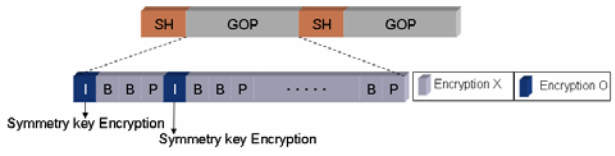

Figure 5. GOP structure

Decryption method of I-Frame is to play the file when only one part is decrypted before entire movie has been decrypted using duplicated buffer algorithm.

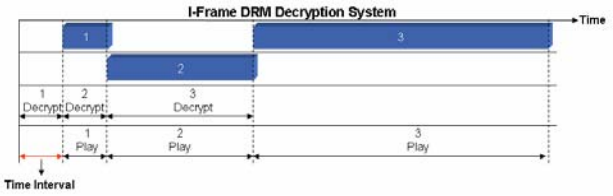

Figure 6. Decryption method of I-Frame DRM system

Disadvantage of I-Frame is that user can get I-Frame size after reading all headers in GOP group to extract I-Frame, and delay until first block has been decrypted at the playback due to overhead to read all GOP headers. This system uses one key for an encryption similar to the conventional system, so the movie cannot be protected when the key is exposed.

2.2 Conventional DRM system

Encryption methods of multi-media are two types; public key and symmetric encryption algorithm. User cannot download a digital data in real-time because each user must encrypts a large scale data if the system selects public key encryption method, and system must cope with an overhead. Also, client must perform many operations at the decryption. If a system selects symmetric algorithm as a encryption method, key management is a very difficult problem. Because only I-Frame is encrypted in a movie, we need to use a extraction algorithm of I-Frame and this method cannot support various multi-media formats. Because it is difficult to watch and track the digital content, conventional DRM system may not collect the data to prove illegal activities when there are some disputes of intellectual property rights. Also, the existing system has the overhead to construct BH (Block Header) at the partial encryption.

This paper proposes an encryption algorithm to guarantee the stability of content and the method to generate several keys using hash chain method by one symmetric key at the encryption of a movie. Attacker cannot generate the key if he does not know a hash function although a key may be exposed. Also, this paper proposes the collaborative protocol of user authentication, so only registered user can use the content. We propose the algorithm without delay time at the decryption of content. Proposed DRM system is more secure and stable.

Proposed system uses a security agent and provides an integrated DRM system to check an illegal execution and modification by user authentication and encryption of raw data via on-line and off-line. Figure 7 shows the system to manage the integrated process that consists of required identification, copyright information, watch for content usage, and breakdown of copyright usage.

Figure 7. Content processing step

3 Proposed Data Encryption Method

3.1 ,Block-sliced Method of Multi-media Data

Proposed method performs the pre-processing step to encrypt each block that the raw data is divided into. At the pre-processing phase, the first encryption block has the size based on the time interval before the original data. The size of second block is 100~200% of the size of the pre-block. Several blocks are bound to a group, and one group is bound to a group again within the 15 times of first block. The same method is applied from the second group to the final group. We use the method that a block is bound to several groups because this method can provide stable DRM system by improving the processing speed using a double buffer at the encryption and decryption steps. Figure 8 shows division processing of multi-media data block.

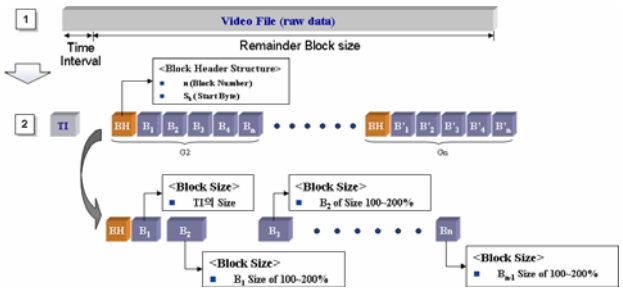

Figure 8. Division processing of multi-media data block

```
Procedure Block_Slice_Split(binary RawData)
{
      long int RawDataSplitSize[ ][ ];

      // acquire the size of movie
      RawDataSize = GetSize(RawData);
      RawDataRemain = RawDataSize

      // initiate array
      array Initialize of RawDataSplitSize

      // acquire Time Interval Size
      RawDataSplitSize[1][1] = Compute(Time_Interval_Size);

      // acquire the size of lasted movie
      RawDataRemain = RawDataRemain - RawDataSplitSize[1][1];

      // make a division group of movie
      for (int i = 2; ; i++) {
         j = 0;
         for (Total_Percent = 0; Total_Percent < 1500; ) {
         j++;
         N = Random_Number_Generator();        // acquire 100 ~ 200%
         Total_Percent += N;

         if RawDataRemain > Compute(RawDataSplitSize[1][1] * N)
            RawDataSplitSize[i][j] = Compute(RawDataSplitSize[1][1] * N);
         else {
            RawDataSplitSize[i][j] = RawDataRemain
            Exit Procedure;
         }

         // acquire the size of lasted movie
         RawDataRemain = RawDataRemain - RawDataSplitSize[i][j];
      }   // Exit for Total_Percent
   }   // Exit for i
} //Exit Procedure
```

Figure 9. Division algorithm of multi-media data block

3.2 Generation of encryption key using hash chain

Proposed system generates a key from the first hash function (H1) using a user authentication number and encrypts the first block with the generated key. The second key is generated from the second hash function (H2) after receiving the first generated key, and the second block is encrypted using the second key. The third key is generated after the key generated from H2 is transmitted to H1 function, and the third block is encrypted. Proposed system repeats this process until all blocks are encrypted. Proposed system generates the key using double hash function and encrypts the data. Because proposed system encrypts multi-media data using two hash functions, the encryption is more secure and attacker cannot decrypt other blocks, although one key is exposed. Figure 10 shows double hash protocol.

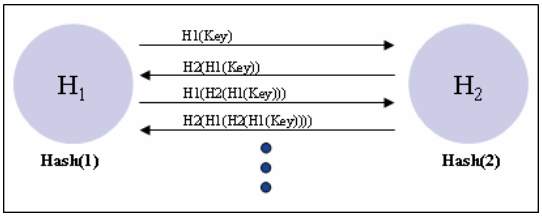

Figure 10. Double hash protocol

Proposed system generates a key using a division and hash algorithm, and encrypts each block using the generated key.

```
Procedure Block_Slice_Encryption(binary RawData)
{
      // acquire block slice
      Get RawDataSplitSize[ ][ ];

      // acquire a key
      Get Key;

      for (int i = 2; i < = X; i++) {                    // i → Group Number

         // encrypt block header
         BH[ i ] = Encryption(Key);

         // generate block slice key
         Temp_Key = Key || Start_Byte

         for ( int j = 1; j < = Y; j++) {                // j → Block Slice Number

            // use hash function for encryption block key
            Temp_key = hash_Chain(Temp_key);

            // encrypt block slice
            RawDataSplitSize[ i ][ j ] =
                        Encryption(RawDataSplitSize[ i ][ j ], Temp_Key);

         }  // Exit for j
      }  // Exit for ii

} //Exit Procedure
```

Figure 11. Block encryption algorithm using double hash

Block Header (BH) that includes the address and size of block and control information of entire group are constructed by Container Header (CH) that includes LAU (License Acquisition URL) and content ID at the encryption. Main Header (MH) includes group size and the hash value of Description ID (DID). Figure 12 shows container header and main header.

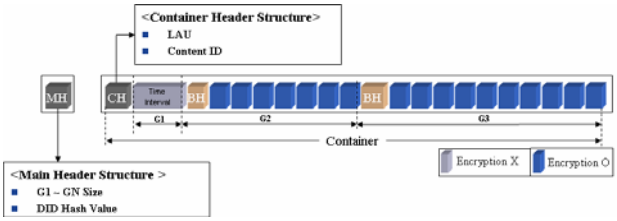

Figure 12. Container Header and Main Header

3.3 User authentication and key transmission

Figure 13 and 14 show the key transmission method and key transmission protocols, respectively. Sever provides an user authentication number via wireless network to verify the information disclosure and user identity, and the user requests a decryption key by inputting authentication number as a key value. Agent that verifies the value of user authentication generates a decryption key by OTP (One Time Password). The generated key is divided into two parts ("a" and "b") using a key partitioning algorithm, and the client agent transmits the key to user after performing the hash function of "a" with an increased session and user authentication value. Receiver performs the hash function of user authentication number and key "a" with a random value, and transmit the hash value to server. Sever recognizes the transmission of key "a", and performs the hash function of key "b" with the user authentication number and random value. Finally, server transmits the key value to user.

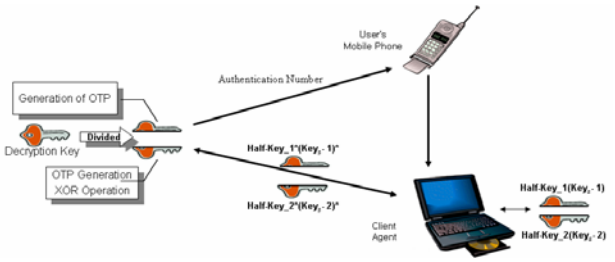

Figure 13. Key transmission method

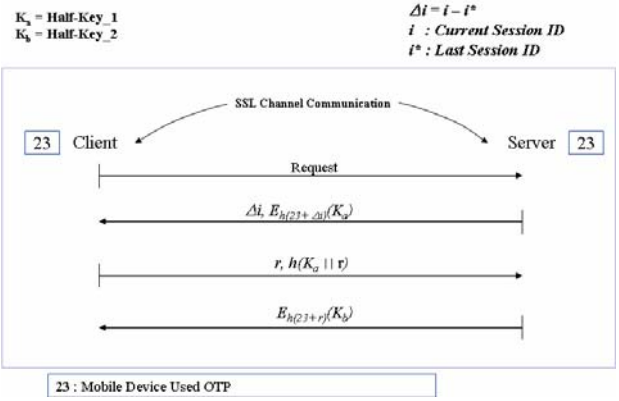

Figure 14. Key transmission protocol

3.4 Decryption method of multi-media data

Proposed system verifies whether the license that is the same to the content ID of container exists or not. If a

license does not exist, user can acquire a license through LAU of Container Header and store the hash value of DID (CPU Serial Number).

At the acquisition of a license, proposed system receives an encryption key for user authentication and decryption. User requests Main Header of movie using content ID, and transmits DID of user hash value and Main Header by user public key. User decrypts Main Header with his private key, and replays the content after verifying whether his hash value is same to the hash value of Main Header or not.

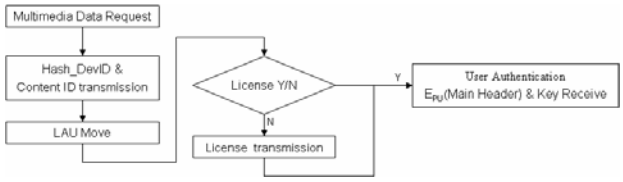

Figure 15. License certification method at the decryption

MH is transmitted using user public key, and decrypted by user private key. After getting the location of BH, proposed system can acquire a key through user authentication method and the content of Gk (B1~Bn)* is decrypted by this key. The decryption method uses a compensated double-buffer algorithm and replays a digital content. Movie is replayed after getting the buffer size through the operation of delayed frame during the playback of the movie. Figure 16 shows a compensated double-buffer system.

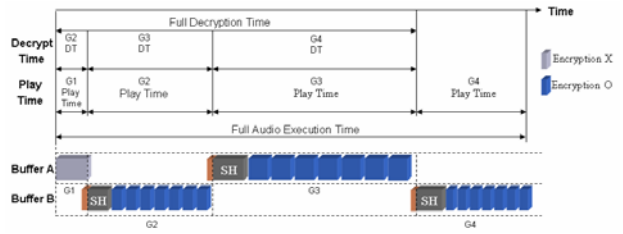

Figure 16. Compensate double-buffer system for movie playback

Proposed system stores digital content to replay the G1 frame for 10 seconds in buffer A and replay it. During 10 seconds, slice layer G2 mounts of data are decrypted and stored in buffer B. If the playback of data in buffer a data is terminated, agent stores the memory reference value of buffer B to replay the data of buffer B sequentially. The phenomenon of breaking screen may happen when changing from buffer A to buffer B because G2 frame is incomplete. Accordingly, the system needs to make a complete frame by adding the last frame of G1 to buffer B. The rest of data is decrypted in buffer A during movie player replays the data of buffer B, and an incomplete frame of buffer B is transmitted to buffer A again. Consequently, the phenomenon of breaking screen does not happen, and the movie can be replayed without interruption.

4 Performance Analysis

4.1 Proposed System Architecture

Proposed DRM system architecture is shown in Figure 17.

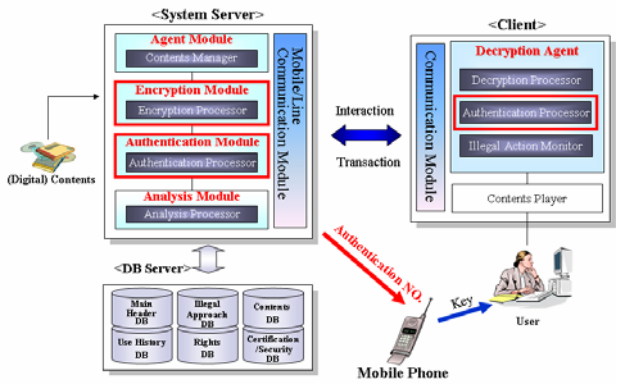

Figure 17. Proposed DRM system architecture

Figure 18 shows the comparison between conventional and proposed DRM system. Conventional DRM system stores an encrypted file in user computer that introduces a considerable delay. A encrypted file prevents a user from illegal reproduction and disclosure of content. Accordingly, content is decrypted by DRM agent when user replays a digital content. However, the user must wait and spend long time to decrypt a large scale file. Conventional method decrypts a file at the playback of content. When user replays a digital content, agent decrypts and replays the content if the user is valid after verifying the validity of content license via server. However, conventional decryption methods replay the content after the decryption of an entire movie is terminated, and the user must wait until the decryption is complete. Accordingly, conventional methods cannot support the time-constraint real-time service. A public key-based decryption system uses also a double buffer algorithm, but this system cannot replay content seamlessly because all frames of movie must be encrypted.

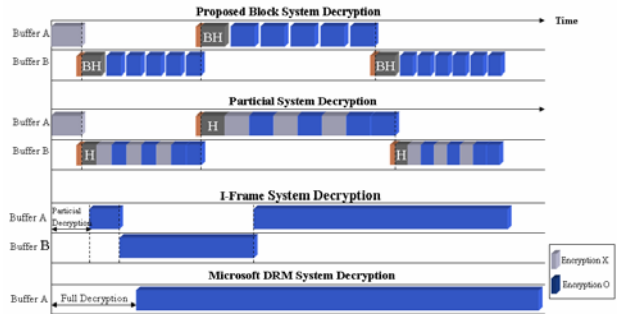

Figure 18. Comparison of delay time in proposed and existing system

4.2 Comparison with the existing system

Conventional systems use only one key as an encryption key to protect the movie content, but the proposed system uses "n "keys and is more secure because the entire movie can not be decrypted, although the key is exposed. Figure 19 summarizes the comparison results.

	InterTrust DRM	Microsoft DRM	I-Frame DRM	Particial DRM	Proposal System
File	All File	WMA/WMV File	All File	All File	**All File**
Encryption	Full file	Full file	Full file	Partially file	**All file(TI Exption)**
Encryption Speed	Normal	Slow	Normal	Fast	**Normal**
Decryption Speed	Normal	Normal	Normal	Fast	**Slow**
Transmission Key	Safe	Weak	Safe	Safe	**Best Safe**
Encryption Key	1	1	1	N	**N**
Exposure Key	Weak	Weak	Weak	Normal	**Safe**

Figure 19. Comparison of conventional and proposed DRM system

5 Conclusion

This paper proposes a double hash chain method to improve the security of multi-media content through a block-sliced DRM system. Proposed DRM system uses PKI technology as a key management engine for encrypting and decrypting the digital content. In the proposed solution, each block is encrypted with a separate key. Thus, the attacker cannot decrypt the whole content illegally, even when the encryption key is exposed. Server stores each key for each block of data, and a security agent generates "n" pieces of symmetric keys through the key management process. Security agent encrypts content with each key by block unit. Proposed system gets the key and certifies a user using an efficient user authentication protocol. Also, the proposed system is strong against external attacks because this system can perform an operation to prevent a replay attack with both old session ID and present session ID value. A block key that is computed only once and does not need to be recomputed, can be used repeatedly after certifying a user.

References

[1] J. Park, K. Lee, J. Kim, and Moon S. Jun, "Design of security and watch system of digital copyright using a license agent," Korea Industrial Information Security Society paper, Vol. 4, NO. 1, pp. 15~24, 2004.

[2] J. Kim, J. Park, and Moon S. Jun, "DRM system based on public key pool for the security of multi-media data," Korea Information Processing Society paper, Vol. 12-C, NO. 2, 2005.

[3] Alexandre Silva and Michael stanton, Pequi: "A PKIX Implementation for Secure Communication," Proceedings of the 1999 International Networking Conference(INET'99), 1999.

[4] Andre Arnes, Mike Just, Svein Knapskog, Steve Lloyd, and Henk Meijer, "Selecting Revocation Solutions for PKI," Proceedings of The Fifth Nordic Workshop on Secure IT Systems (NORDSEC), 2000. .

[5] Barbara L. Fox Brian A. LaMacchia, "Encouraging Recognition of Fair uses in DRM Systems," Communications of The ACM, VOL. 46, NO. 04, pp. 61 ~ 63, April, 2003.

[6] Intertrust : http://www.intertrust.com/main/overview/drm.html

[7] John S. Erickson, "Fair use, DRM, and trusted computing," Communications of the ACM, VOL.46, NO.04, pp. 34 ~ 39, April, 2003.

[8] Russ Housley and Tim Polk, "Planning for PKI," John Wiley & Sons, 2002.

[9] Gildas Avoine and Philippe Oechslin, "RFID Traceability: A Multilayer Problem" EPFL Lausanne, Switzerland, 2005.

T.C Edward Jung received the Ph.D. and B.S (with honors) in computer science from the University of Minnesota, Minneapolis, in 1994 and 1987, respectively. He is the founding and technical director of information system security research group at Samsung's Advanced Institute of Technology (SAIT), the central research lab at Samsung Group. From 1997 to 2002, he was a Member of the Technical Staff at Lucent Technologies - Bell Labs in Holmdel, New Jersey. From 1994 to 1997, he worked at Motorola Inc. and at Siemens in USA. His research activities are in information systems security with special emphasis on mobile and wireless security

Moon-Seog Jun received her Bachelors Degree in Computer Science from Soongsil University in 1981, M.S and Ph.D Degree in Computer Science from University of Maryland, MD, U.S.A. in 1985 and 1988 respectively. He joined the School of Computer Sciences at Soongsil University in 1991 as a full professor. He was the Dean of the School of Computer Sciences.He was a senior at Physical Science Laboratory, USA in 1989. He has an editor-in-chief in International Journal of Computer Science and Network Security from 2005 and also senior delegation in SC-17 and SC-27.His current research work is in the area of Network Security, Cryptography, Computer Algorithms, and Network Protocol. He has published a number of papers related to Network security, PKI, and Mobile security areas.