

Scalable DRM System for Media Portability

Hyounghick Kim

Samsung Electronics, Software Laboratory, Home S/W Platform Team
416, Maetan-3Dong, Yeongtong-Gu,
Suwon, Gyeonggi-Do, Korea 443-742
hyungsik.kim@samsung.com

Abstract. We present a new digital rights management (DRM) system for media portability using dynamic multimedia adaptation. For a user to share multimedia resources over home network, several DRM technologies based on the domain have been introduced. Domain-based approaches enable users to access contents on multiple devices within the same domain. However, most of current DRM systems were only designed for a homogeneous environment where common AV profiles are supported. It is a challenge to share the domain contents between domain members with diverse capabilities while ensuring the protection of the intellectual property rights for the legally obtained contents. In this paper, we propose an architecture that enables DRM contents to be securely shared between various home devices in a seamless manner.

Keywords: DRM, Home Network, Media Portability, Transcoding, Scalability.

1 Introduction

In order to take advantage of the online distribution while at the same time preventing illegal redistribution of the content, digital rights management (DRM) technologies are recently employed for restricting the use of the contents within usages granted by the content holder. Consumers, however, want to enjoy contents on any of their devices without limitation. In particular, the emerging standards and technologies for home entertainment networking are developed to enable all kinds of home devices to access the multimedia resources between the devices [3].

In order to satisfy both of the contents holders and the users over home network, the notion of authorized domain is introduced by identifying a set of devices which a home user owns [4][22]. In a DRM system supporting the domain concept, a user freely enjoys contents among devices within the authorized domain. Most commercial DRM technologies have already defined the authorized domain [7][8][11] which aims to meet the requirements for sharing between networked devices.

In order to share DRM contents effectively, however, the only domain management is not enough. In practice, transcoding for media portability is necessarily required to enable sharing contents among a multitude of playback devices with different device capabilities and dynamic channel capacities [1]. For example, a high-definition (HD) video content for home set-top box must be adapted to target displays of other devices such as a mobile phone that may not even support

standard-definition (SD) resolution because of its limited processing capability or small display. However, such content adaptation may introduce security implications. First of all, translation of DRM protected contents may pose serious threats to the security of the DRM system since the decrypted plaintext content is clearly revealed to the transcoder. In addition, the creation of the associated license should be also required when new DRM content has been created from the result of the translation.

For solving these problems, general DRM interoperability solutions may be considered. Several approaches are previously introduced in this challenging area [12][13][16][17][19]. In general, however, DRM interoperability solutions seem too heavy and complex. Conventional interoperability approaches require common trusted frameworks such as certificates management and keys management for secure communication between participating entities. The common trusted frameworks incur not only the cost of new mechanisms but also many business negotiations among participants in DRM value chains [8]. Furthermore, in the connected interoperability approach, the translation processes are handled by an online mediator on the outside of the home network through re-acquisition methods [12][19]. In general, it is difficult to guarantee continuous network connectivity to Internet.

In this paper, we focus on the challenges involved in scalability issues of both the DRM contents and the associated licenses. In order to enhance scalability of the DRM protected contents, we apply the scalable coding methods [20][21] directly to the generation of the scalable DRM protected contents. Also, we propose a method for compression of digital signatures which are appended to the license.

2 Problems

Our proposed system is intended for satisfying security requirements derived from both DRM protected contents and the associated license within an authorized domain. Both objects must be securely translated for one of supported AV profiles in a playback client device. Before addressing the detailed description of our system, we briefly review two main problems identified by previous approaches.

2.1 Secrecy of Protected Content

During a delivery of a DRM protected content from a media server to a playback client through AV operations such as copy, move or streaming, intermediary devices over home network may perform some transcoding operations such as bit rate reduction, changing resolution, spatial down sampling, or frame rate reduction to adapt to application capabilities. Transcoding often refers to the process of transforming audio and video from the original format in which the multimedia was encoded into a possibly different format or quality.

In the process of translation, the plaintext media stream of the protected content may be insecure in the view of end-to-end security from the media server to the client since decryption of the protected content is generally required at the transcoders. The transcoders decrypt the DRM protected content before transcoding it. For doing this, the transcoders must manage the content encryption key (*CEK*). In most DRM systems, *CEK* can be extracted from a DRM license by the only authorized entities

(e.g. domain members). Consequently, we need to assume that the transcoder is also an authorized participant and the transcoding operation is allowed under the terms stated by the DRM system. It is shown in Figure 1.

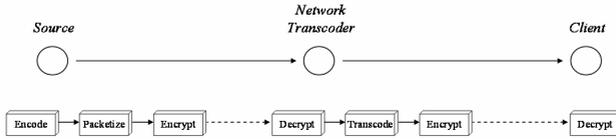


Fig. 1. Conventional system for transferring of a DRM content between a media server and a client

These approaches not only increase processing overhead for decryption and re-encryption but also require a strong security assumption on the transcoder. Transcoding method that requires the decryption of the protected content is not desirable in environment that transcoders may be not trust since it violates the end-to-end security guarantee of privacy [14].

2.2 Verifying License

Another important issue is to generate a valid license for a newly translated DRM content. Before installing a DRM license to render the associated DRM protected content, most DRM clients must check the validity of the license object for preventing against the modification of a DRM license or rogue content holder attack. For this purpose, the content holder's own secret information is required since a valid license can be generated by the only honest contents holder. The most intuitive solution is to use the content holder's signature or MAC (Message Authentication Code) [7].

Unlike conventional DRM systems, we cannot assume that the identical licenses are shared between domain members. As a result of the transcoding of DRM protected content, the creation of a new DRM license may be also required since hash value or content identifier of the associated DRM protected content are modified. By these modifications, new hash value or the changed content identifier must be included into the DRM license object. Therefore, the transcoder must also hold the content holder's unique secret information such as his sign key for generating the DRM license.

To exercise the localized licensing, the delegation of content holder's authority to transcoder using some advanced cryptographic primitives [15][18] such as proxy signature are previously introduced [2][13][24]. However, previous approaches have some limitations. First of all, assuming an authorized proxy of contents holder is not acceptable in conventional DRM world yet. To accept these as industrial technologies, contents holders need time to verify the security of the technologies since many cryptographers are still skeptical about the proof of the security for proxy signature or proxy re-encryption. Also, the existence of the delegated device may cause the single server failure problem. To access an interoperable service, the home devices must always contact the designated transcoder who holds the role of proxy. In

CE environment, it is difficult to assume that there is the specific device without cease since a device may be commonly turned off or broken down.

3 DRM System for Multiple AV Profiles

In this section, we focus on the distribution of the DRM protected content and the associated license. Our proposed system translates both objects in local home network without breaking end-to-end security between a content holder and a media player. In a practical environment, the content holder can be a combination of contents providers and service providers.

The multimedia adaptation problem for DRM contents deals with a media server, S and a media player, P . In general, given a DRM content c_n and a license l_n for an AV profile p_n , our goal is to translate them into the new DRM content c_m and the associated license l_m for the specific AV profile p_m in a secure and seamless manner. In general DRM systems, c_n consists the metadata of the content and the encrypted plaintext media stream s_n with a CEK , denoted as $E_{CEK}\{s_n\}$. At this time, we assume that the plaintext media stream s_n is encoded using a scalable video coding and a media stream s_i can be transcoded from s_n using dropping some enhancement layers if i is less than n . A scalable video coding provides a unique representation of one video signal allowing simultaneous access to the scene at different scales: spatial, temporal and quality.

Not all video coding technologies are suitable for scalability. AVC is expected to be basis of interoperability for home network. To guarantee interoperability and take advantage of these devices in home network technologies, scalable video coding shall support base layer compatibility with AVC standard. Recently, the Joint Video Team (JVT) is finalizing the standardization of MPEG-4 SVC: the scalable video coding extension of MPEG-4 AVC [6][9]. In this paper, we assume that home network and the related DRM standard technologies support AV profile which can be encoded by scalable coding such as MPEG-4 SVC.

Our proposed system consists of two parallel steps, ‘content translation’, and ‘license translation’ which are processed on the media server S and the media player P . Upon completing protocols successfully for content purchase, the media server S stores the purchased content. The media server S translates the encrypted media stream s_n and the digitally signed l_n with the contents holder’s sign key then delivers them to the media player P when the player P requests to share the content. Upon successful receiving the translated DRM content and the associated license, the player P passes them to the DRM agent.

3.1 Content Translation

The contents holder H passes raw audio and video input through the specific encoder to produce scalable encoded streams. The content is encoded into multiple layers consisting of one base layer and multiple enhancement layers using layered coding. The base layer is encoded at the minimum rate necessary to decode the content stream, and its decoding results in the lowest quality version of the content. Each enhancement layer provides progressive refinement of the encoded content [10].

For protecting the secrecy of the plaintext media stream, the encoded streams must be encrypted with the *CEK*. The encrypted streams can be generated from scalable compressed bitstreams. The server *S* parses the scalable bitstreams, and groups the data into n layers g_1, g_2, \dots, g_n . After grouping the scalable coded data into layers, the contents holder *H* sequentially encrypts them using *CEK*. After completing the purchase, the encrypted group data $E_{CEK}\{g_i\}$ for $1 \leq j \leq n$ and additional metadata *M* as the DRM Protected content are stored to a media server *S*. Not only general DRM information such as content identifier but also the location information for transcoding must be included into metadata *M*. In general, these data can be directly represented common DRM file formats in Conventional DRM systems.

In the step of playback, a media player *P* can download only a difference between quality levels rather than downloading the entire multimedia stream for minimizing communication cost. When the media player *P* requests the media server *S* to download a DRM content c_m for a AV profile p_m where $1 \leq m \leq n$, the media server *S* transfers the data $E_{CEK}\{g_i\}$ for $1 \leq i \leq m$ and the metadata *M* to the player *P*. The server *S* achieves secure transcoding without operations such as decryption and re-encryption. The server *S* simply reads the metadata of the DRM protected content and then truncates a set of group data at the appropriate locations. It is not required that the specific compression, decoding, or encryption algorithms are implemented in the media server *S*. Therefore, we do not assume that the server *S* should implement DRM clients or be one of the authorized domain members.

For access the content, the media player *P* starts to decrypt the encrypted group data $E_{CEK}\{g_i\}$ for $1 \leq i \leq m$ using the content encryption key *CEK* if the player *P* already holds the key *CEK*. In general, the *CEK* is included to the associated license as encrypted form with the domain key. Therefore, the *CEK* can be obtained if the media player *P* is a member of the authorized domain. After successfully decrypting data, the resulting plain multimedia stream is passed to the DRM client.

3.2 License Translation

When the media server *S* translates the protected DRM content and then distributes on the fly them to the media player *P*, the associated DRM license may be also delivered to the player *P*. The associated DRM license must be newly generated due to the changed values such as the hash value of the translated DRM protected content or the associated content identifier.

The simplest solution is to download all associated licenses l_1, l_2, \dots, l_n from the content holder *H* and to deliver one of them according to the requested AV profile p_m . However, downloading all associated license is not efficient solution since the associated licenses l_1, l_2, \dots, l_n generally include redundant information.

Clearly, the most efficient method is to aggregate possible licenses into one which consists of common factors and uncommon factors.

In uncommon parts, the main overhead is to append the content holder *H*'s signature and MAC value of the DRM license itself for all profiles. The number of the appended signatures and MAC values are linear in the number of AV profiles in home.

For minimizing the size of these data, one solution is to generate the associated license l_m in local network without regard to the contents holder *H*. In our system, we

propose the following technique using a variant of aggregate signature schemes [5]. An aggregate signature scheme is useful for compressing the list of signatures on distinct messages. Our proposed scheme can be efficiently implemented compared with the general aggregate signature schemes since we only consider that the DRM licenses are issued by a unique content holder H .

Given a permutation description d , a permutation family is one-way if it is infeasible to invert the corresponding permutation. A permutation family is trapdoor if each description d has some corresponding trapdoor $t \in T$ such that it is easy to invert the permutation corresponding to s using t , but infeasible without t .

Our scheme generates the compressed signature using a trapdoor permutation $\pi: D \rightarrow D$ and a random oracle $h: \{0, 1\}^* \rightarrow D$ where D is a group with operation \cdot . The scheme comprises the following three algorithms:

- **Key Generation:** For the contents holder H , the trapdoor permutation π and the trapdoor information t are randomly selected. The selected values t and π are used as the signing key and verification key, respectively.
- **Signing:** Given the possible licenses l_1, l_2, \dots, l_n , the compressed signature is computed by the contents holder H as the follows:
The contents holder H then sequentially computes σ_i repeatedly applying the inverse of the permutation π^{-1} and the random oracle h where σ_0 is the unit element in the group D as the follows:

$$\sigma_i = \pi^{-1}(h(l_i) \cdot \sigma_{i-1}), \text{ for } 1 \leq i \leq n. \quad (1)$$

Each intermediate value σ_i means the signature of the DRM license l_i .

- **Verification:** For verifying the validity of the signature σ_k , the media player P computes the verification value v_k as follows:

$$v_k = h(l_k)^{-1} \cdot \pi(\sigma_k). \quad (2)$$

It is clearly true that there is a $h(l_k)^{-1}$ since D is a group. The media player P sequentially computes the verification values v_i repeatedly until computing v_1 as follows:

$$v_i = h(l_i)^{-1} \cdot \pi(v_{i+1}). \quad (3)$$

We can verify the validity of the signature by checking whether v_1 is the same as the unit element in the group D .

The advantage of the proposed scheme is to generate the valid signatures of the associated licenses without the key management or too heavy cryptographic operations. The media server S locally generates the signature σ_m of the license l_m from the stored σ_n without regard to the trust relationship with the contents holder H . In addition, for computing MAC value of the DRM license l_m , the media server needs to hold the MAC key of the DRM protected content. It can be solved by delivering the signed MAC key MK instead of MAC value of the DRM content. The media server S computes the MAC value of the license l_m using the signed MAC key. Figure 2 shows the protocol of the overall system.

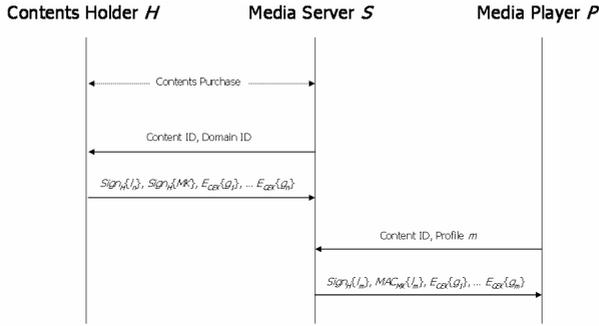


Fig. 2. The overview of the proposed system

In general, the delivered values can be easily adapted to the conventional file formats such as a license object or a DRM protected content without modifying them. Therefore, our approach does not require new standardized DRM file formats.

4 Conclusion

In this paper, we have presented a new DRM system for multiple AV profiles.

To share DRM contents between diverse home devices, the proposed system provides scalable DRM contents and the compression of the associated license. The proposed system which is based on a scalable coding and the aggregate signature scheme, encodes a content sequence such as audio/video frames into protected data that can be streamed or copied to heterogeneous clients.

It would be interesting to analysis the performance of the proposed system. In the future, we plan to investigate how our system can be efficiently implemented using a specific DRM technology such as OMA DRM. We will also investigate a formal security proof of the system.

References

1. Eskicioglu, A.M., Delp, E.J.: An integrated approach to encrypting scalable video. In: IEEE ICME, pp. 573–576. IEEE Computer Society Press, Los Alamitos (2002)
2. Taban, G., Cárdenas, A.A., Gligor, V.D.: Towards a secure and interoperable DRM architecture. In: Proceedings of the 6th ACM Workshop on Digital Rights Management, pp. 69–78 (2006)
3. DLNA. DLNA Overview and Vision, http://www.dlna.org/en/industry/about/dlna_white_paper_2006.pdf.
4. van den Heuval, S.A.F.A., Jonker, W., Kamperman, F.L.A.J., Lenoir, P.J.: Secure Content Management in Authorized Domains. In: Proceedings of IBC 2002, pp. 467–474 (2002)
5. Boneh, D., Gentry, C., Lynn, B., Shacham, H.: A survey of two signature aggregation techniques. RSA’s CryptoBytes 6(2) (2003)
6. Reichel, J., Schwarz, H., Wien, M.: Joint Scalable Video Model JSVM-6, Doc. JVT-S202 (2006)

7. Open Mobile Alliance. DRM Specification 2.0, <http://www.openmobilealliance.org/>
8. Popescu, B.C., Crispo, B., Tanenbaum, A., Kamperman, F.: A DRM Security Architecture for Home Networks. In: Proceedings of the 4th ACM Workshop on Digital Rights Management, pp. 1–10 (2004)
9. Wiegand, T., Sullivan, G., Reichel, J., Schwarz, H., Wien, M.: Scalable Video Coding-Joint Draft 6, Doc. JVT-S201 (2006)
10. McCanne, S., Jacobson, V., Vetterli, M.: Receiver-driven layered multicast. In: Proceedings of ACM SIGCOMM, pp. 117–130 (1996)
11. Kamperman, F., Szostek, L., Wouter, B.: Marlin common domain: authorized domains in marlin technology. In: 4th IEEE Consumer Communications and Networking Conference, pp. 935–939 (2007)
12. Koenen, R.H., Lacy, J., Mackey, M., Mitchell, S.: The long march to interoperable digital rights management. Proceedings of the IEEE 92(6) (2004)
13. Kravitz, D.W., Messerges, T.S.: Achieving media portability through local content translation and end-to-end rights management. In: Proceedings of the Fifth ACM Workshop on Digital Rights Management (2005)
14. Wee, S.J., Apostolopoulos, J.G.: Secure Scalable streaming and secure transcoding with JPEG-2000, IEEE ICIP (2003)
15. Ateniese, G., Hohenberger, S.: Proxy Re-Signatures: New Definitions, Algorithms, and Applications. In: Proceedings of the ACM Conference on Computer and Communication Security (CCS), pp. 310–319 (2005)
16. Safavi-Niani, R., Sheppard, N., Uehara, T.: Import/Export in digital rights management. In: Proceedings of the 4th ACM Workshop on Digital Rights Management, pp. 99–110 (2004)
17. Senoh, T., Ueno, T., Kogure, T.: DRM renewability & interoperability. In: 1st IEEE Consumer Communications and Networking Conference, pp. 424–429. IEEE Computer Society Press, Los Alamitos (2004)
18. Ateniese, G., Fu, K., Green, M., Hohenberger, S.: Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage. In: Proceedings of the 12th Annual Network and Distributed System Security Symposium. Internet Society, pp. 29–44 (2005)
19. Kalker, T., Carey, K., Lacy, J., Rosner, M.: The Coral DRM interoperability framework. In: 4th IEEE Consumer Communications and Networking Conference, pp. 930–934 (2007)
20. Radha, H., Chen, M.: A framework for efficient progressive fine granularity scalable video coding. IEEE Transactions on Circuits and Systems for Video Technology 2(3), 332–344 (2001)
21. Radha, H., Chen, M.: The MPEG-4 fine-grained scalable video coding method for multimediasstreaming over IP. IEEE Transactions on Multimedia 3(1), 53–68 (2001)
22. Sovio, S., Asokan, N., Nyberg, K.: Defining Authorization Domains Using Virtual Devices. In: SAINT Workshops 2003, pp. 331–336 (2003)
23. Kim, H., Lee, Y., Chung, B., Yoon, H., Lee, J., Jung, K.: Digital Rights Management with Right Delegation for Home Networks. In: Rhee, M.S., Lee, B. (eds.) ICISC 2006. LNCS, vol. 4296, pp. 233–245. Springer, Heidelberg (2006)