IMPLEMENTATION AND EVALUATION OF NEW ILLEGAL COPY PROTECTION

Protection Against Making a Illegal Copy of a Copy

Masaki Inamura and Toshiaki Tanaka
KDDI R&D Laboratories Inc., 2-1-15 Ohara, Fujimino-shi, Saitama, Japan

Keywords: Digital Rights Management, Private Copy, Illegal Copy Protection, Terminal ID, Group Key Agreement.

Abstract: We propose a new method of illegal copy protection, which is adapted to digital contents delivery service, allows for legitimate users to make private copies on arbitrary terminals within the limited times, and requires no secure hardware. Using the method, we can realize two types of services; one is a client-server model over peer-to-peer network, and the other is a broadcast model over multicast network which is similar to existing broadcast. In this paper, we implement the proposed method and evaluate whether our method is feasible from the viewpoint of security and performance.

1 INTRODUCTION

Recently we can easily obtain broadband network because of improvement on network infrastructure. Thus delivery services of digital contents over the Internet are penetrating. Furthermore various kinds of technologies for communicating digital contents within home network are standardized. For example, Digital Living Network Alliance (DLNA) is promising standard technologies for this purpose. Using these technologies, a user can move the digital contents to the other digital home appliance everywhere in his home.

On the other hand copy operation should be strictly restricted because digital data can be easily duplicated with no loss of information. Accordingly delivery of digital contents may cause copyrights violation, making illegal copies or illegal distribution. Digital Rights Management (DRM) is a technical solution for copyrights protection and secure contents distribution.

Currently many DRM systems have been proposed. A major purpose in these systems is to protect that users with no copyrights make a copy of digital contents freely. Therefore, most copy control methods such as Digital Video Disc Recordable (DVD-R)/ReWritable (RW) media and Secure Digital (SD) card, which are widely used in real-world systems, prohibit copy operation. Namely users cannot modify the contents even for his own purpose or cannot copy valuable contents for back-up. This means that digital contents are in danger of lost if the system applying these methods fails to move to other degital devices. Thus, strict copy control is not suitable for user friendly DRM systems.

A strong point of newly proposed DRM systems is loosely control copy operation. FairPlay for iPod and OpenMG are welknown examples. In these systems, the user can copy contents for his player while leaving the original contents in his computer. Thus the user can easily make back-up contents in his computer. As another methods, the copy operation is controled by the license administrator. For the purpose to control copy operation, two methods are identified. One method is binding copy operation to a designated terminal, e.g. the system proposed Fujii et al. The other is usage control by limited time, e.g. the system proposed Cheng et al. However these systems have imperfect usability because of the following:

1. it is difficult to use these systems into open plathome,
2. these systems need to register user's terminal information,
3. user cannot use content in a long term by limited time.

In this paper, we propose a DRM system with new illegal copy protection. We pay attention that a problem of making personal copies from an original content (we call it "First Generation Copy") is less

Inamura M. and Tanaka T. (2007).
IMPLEMENTATION AND EVALUATION OF NEW ILLEGAL COPY PROTECTION - Protection Against Making a Illegal Copy of a Copy.
In *Proceedings of the Second International Conference on Security and Cryptography*, pages 427-432
DOI: 10.5220/0002124204270432

serious than that of making copies from other copies without an original content (we call it "Second Generation Copy"). We summaize main features of our proposed DRM system as follows:

- Permission to make First Generation Copy and prohibition to make Second Generation Copy;
- Permission to copy on only Set-Top Box;
- No hardware equipment;
- Privacy protection that a user does not need to communicate terminal ID;
- Enabling offline use of contents/copies;

Futhermore we made two types of software based on proposed method; one is a client-server model over peer-to-peer network, and another is a broadcast model over multicast network which is similar to existing broadcast. We also evaluated perfomance of two systems and confiermed that we could realize proposed method in real computers.

2 SERVICE MODEL

We show service model in Figure 1.

License Administration Server administers user license and make content key for the purpose of encrypting/decrypting contents. Content key is generated from Set-Top Box (STB) ID.

Content Provider or Broadcasting Station encrypts contents using content key and distributes encrypted contents to users.

After receiving encrypted contents, users at home record these contents into STB and decrypt them using content key generating from STB. Decrypted contents are able to use watching on memory and are not recorded on recording media.

If users want to copy contents for their private player, STB gets ID of this player and generates re-encryption key from this ID. STB re-encrypts contents using re-encryption key and this player record them. Because re-encryption key is bound to player's ID, users can use re-encrypted contents on only this player binding this key.

In this system, for the purpose of protecting contents distributed in this model against illegal use/copy, the following is required:

- **Terminal Legitimacy:** Users or third parties cannot use/copy the contents on not-permitted terminals.
- **Wiretapping Impossibility:** The contents, which are obtained through wiretapping, cannot be used on terminals without permitted terminal.
- **Illegal Copy Process Impossibility:** Even if users or third parties copy content without running legal process, they cannot use it.
- **Replay Attack Impossibility:** The contents cannot be copied by using other license information for other content.
- **Privacy Protection:** License administrator and third parties cannot get IDs of terminal using copied content.

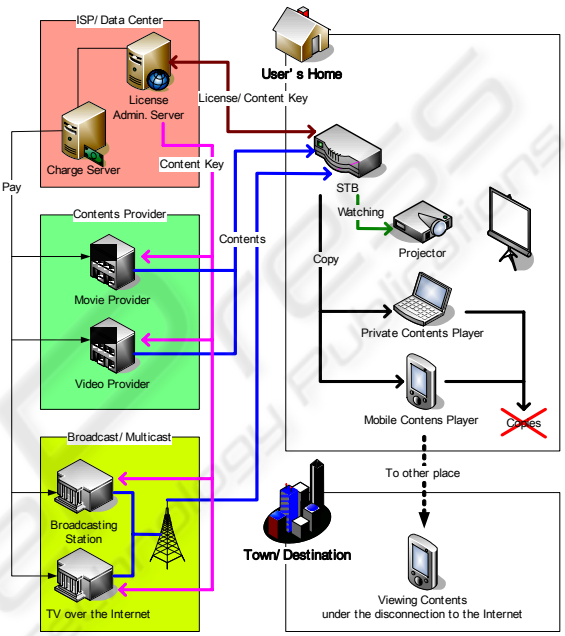

Figure 1: Service Model.

3 PROTOCOL

In this chapter, we propose a protocol which realizes this model in secure. We establish four types of entities; License Administration Server (LAS), Contents Delivery Server (CDS), STB and Private Player (PP). Proposed protocol is used to communicate among these entities.

We define assumptions of this protocol as follows:

Assumptions:

- LAS and CDS are honest and trustful; however STB and PP are not honest and trustful.
- Hardware improvements are not required, and anyone cannot disassemble programs running on these entities. For example, disassemble programs are realized with software obfuscation.
- Existing hardware ID, e.g. hard-disc drive ID or BIOS chip ID, is introduced as terminal ID.

- Terminal ID is bound to one terminal, and anyone cannot forge/modify it.
- Content key generated on STB, re-encryption key generated on PP and Decrypted content run on only memory and are not recorded in recordable media, for example HDD or DVD-R/RW.
- PKI has been prepared in advance, and asymmetric encryption scheme and digital signature scheme are used rightfully.

3.1 STB Registration

The following sequence describes STB registration procedure as depicted in figure 2.

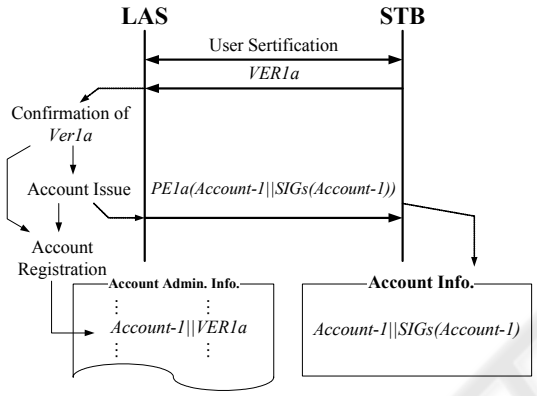

Figure 2: Service Model.

1. LAS certificates user communicating with STB.
2. STB sends verification key *VER1a* to LAS.
3. After confirmation of *VER1a*, LAS generates account name of user 1 *Account-1* and digital signature *SIGs(Account-1)*. Furthermore LAS concatenates 2 messages, encrypts concatenated data with STB's public key and sends it to STB. LAS records *Account-1* bound to *VER1a*.
4. STB records *Account-1||SIGs(Account-1)* as STB's account information of user 1.

3.2 Reception of Content Distribution

We show reception of content distribution procedure in figure 3.

1. STB obtains *CID*, generates Content Distribution Request Data *Account-1||SIGs(Account-1)||CID ||SIG1a(Account-1||CID)* using Account info. and STB sends this data to LAS.
2. After verification of Content Distribution Request Data, LAS generates *g, p* and *t* using in DH and sends $g||p||g^t \bmod p||SIGs(g||p||g^t \bmod p)$ to STB.
3. STB generates public key for content key $g^{f(ID1a)} \bmod p$ and sends $g^{f(ID1a)} \bmod p \ ||SIG1a(g^{f(ID1a)} \bmod p)$ to LAS.
4. After reception, LAS generates STB Certification Code *E(Account-1, Ks-1a)* and sends it to STB. If the line on which the content distributes is multicast, LAS generates Content Key Seed $g^{t\{f(ID2a)+ \ldots + f(IDma)\}} \bmod p$ using all reception users' ID and sends it concatenated STB Certification Code to STB. Furthermore STB records public key of user 1 bound to Account Admin. Info. of user 1.
5. STB records *g*, *p*, $g^{f(ID1a)} \bmod p$ and *E(Account-1, Ks-1a)* (in case of multicast, and $g^{t\{f(ID2a)+ \ldots + f(IDma)\}}$) as content using info..

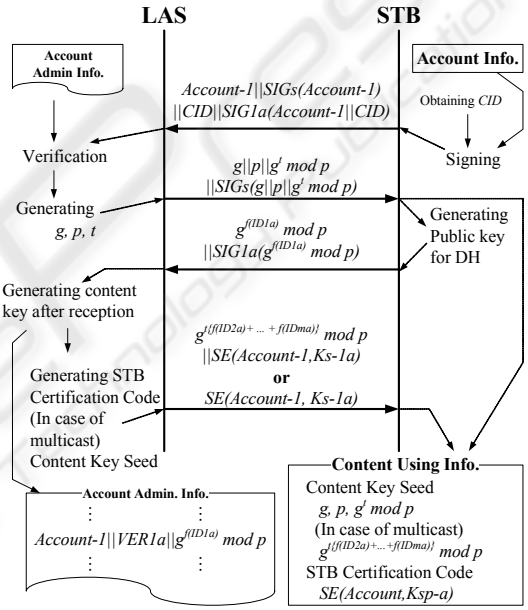

Figure 3: Reception of Content Distribution.

3.3 Content Distribution

We show content distribution procedure in figure 4.

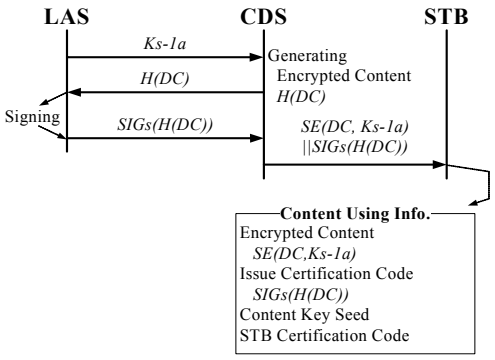

Figure 4: Content Distribution.

1. LAS sends content key *Ks-1* generated in section 3.2 to CDS.
2. CDS encrypts content with *Ks-1*. Furthermore CDS generates *H(DC)* and sends it to LAS.
3. LAS generates digital signature within *H(DC) H(DC)* and sends *SIGs(H(DC))* to CDS.
4. CDS sends encrypted content *SE(DC, Ks-1)* and Issue Certification Code *SIGs(H(DC))* to STB.
5. STB adds *SE(DC, Ks-1)* and *SIGs(H(DC))* to Content Using Info..

If the line on which the content distributes is multicast, all *Ks-x* ($0<x<m$) are the same.

3.4 Content Viewing

At content viewing, legitimacy of content use is checked by content viewing program. We show procedure of this program as follows:

1. *SE(DC, Ks-1a)*, *SIGs(H(DC))*, *g*, *p* and g^t *mod p* (in case of multicast, $g^{t\{f(ID2a)+ \ldots + f(IDma)\}}$ *mod p* too) are inputted into client program. Furthermore *ID1a* is automatically inputted into this program.
2. Client program generates *f(ID1a)* from *ID1a* through transforming function. This program generates *Ks-1a* = $g^{tf(ID1a)}$ *mod p* (in case of multicast, $g^{t\{f(ID1a)+f(ID2a)+ \ldots + f(IDma)\}}$ *mod p*) from *f(ID1a)* and Content Key Seed.
3. Client program decrypts *SE(DC, Ks-1a)* with *Ks-1a* and obtain *DC*.
4. Client program verifies Issue Certification Code *SIGs(H(DC))* with *DC* and verifying key of LAS.
5. If verification of Issue Certification Code is succeeded, STB can let user view content. However *DC* without encryption does not remained in recordable file.

When user views copied content on PP, viewing program installed in PP runs with same procedure.

3.5 Content Viewing

We show copying content procedure in figure 5.

1. STB send *g* and *p* to PP.
2. PP generates public key for DH $g^{f(ID1b)}$ *mod p* from *g*, *p* and automatic inputted *ID1b*. PP encrypts public key with digital signature *PE1b*($g^{f(ID1b)}$ *mod p*|| *SIG1b*($g^{f(ID1b)}$ *mod p*)) and sends it to STB.
3. STB generates Copying Request for PP *H*($g^{f(ID1b)}$ *mod p* ||*SIG1a[SIGs(H(DC))||H*($g^{f(ID1b)}$ *mod p)]* and sends it to LAS.
4. LAS checks Copying Request whether the number of copies is less than limited number or not. If Checking is succeeded, LAS generates Copy Permission *SIGs(H*($g^{f(ID1b)}$ *mod p))* and sends it to STB. Furthermore LAS records a part of Copying Request *SIG1a[SIGs(H(DC))||H*($g^{f(ID1b)}$ *mod p)]* into Copy Record and reduces the remained number of copies.
5. STB generates Re-encryption Key *K1a-1b*, Re-encryption Key Seed $g^{f(ID1a)}$ *mod p* and Re-encrypted Content *SE(DC, K1a-1b)* using Content Using Info., Account Info., *ID1a* and PP's public key. In this time, if STB does not obtain Copy Permission, STB cannot generate these data.
6. STB sends $g^{f(ID1a)}$ *mod p*, *SE(DC, K1a-1b)* and Issue Certification Code *SIGs(H(DC))* to PP.
7. PP can view content under the procedure which is same as section 3.4.

Only STB can copy content for PP. For verification of STB which can copy content, STB Certification Code is used. Copying program verifies STB with this code. We show procedure of this program as follows:

1. Copying program generates Content Key *Ks-1a* from *ID1a* and Content Key Seed.
2. Copying program verifies Account Info. *Account||SIGs(Account)*.
3. Copying program decrypts STB Certification Code with *Ks-1a*. This program verifies STB comparing decrypted data of STB Certification Code with Account Info.
4. Copying program decrypts *SE(DC, Ks-1a)* with *Ks-1a* and obtains *DC*.
5. Copying program verifies Issue Certification Code *SIGs(H(DC))* with decrypted *DC*.
6. Copying program generates Copy Request for PP *H*($g^{f(ID1b)}$ *mod p)* ||*SIG1a[SIGs(H(DC))||H*($g^{f(ID1b)}$ *mod p)]* from public key of PP for DH and sends it to LAS.
7. LAS checks Copying Request whether the number of copies is less than limited number or not. If Checking is succeeded, LAS generates Copy Permission *SIGs(H*($g^{f(ID1b)}$ *mod p))* and sends it to Copying Program in STB.
8. After verification of Copy Permission, copying program generates Re-encryption Key *K1a-1b* and Re-encryption Key Seed $g^{f(ID1a)}$ *mod p*.
9. Copy program re-encrypts *DC* with K1a-1b. Furthermore copy program generates Re-encrypted Content *SE(DC, K1a-1b)* and Re-encryption Key Seed $g^{f(ID1a)}$ *mod p* and sends it to PP with Issue Certification Code.

4 SIMULATION

In this chapter, we show the result of evaluation.

Environment of simulation is following:

- LAS, CDS: Pentium4 2.8GHz, Memory 1GB, Windows XP;
- STB: A) Pentium4 2.66GHz, Memory 1GB, Windows 2000;
- PP (in case of multi-connection, other STB):
  B) Pentium4 2.4GHz, Memory 1GB, Windows 2000
  C) Pentium4 2.2GHz, Memory 1GB, Windows 2000;
- Network; 100BASE-TX;
- Security Algorithm:
  Symmetric Encryption: AES-128
  Asymmetric Encryption: RSA-1024
  Digital Signature: RSA-1024
  One-way Function: SHA-1;

We show result of throughput of downloading and copying on Client-Server model in table 1.

Table 1: Throughput on Client-Server Model.

Download	A	B	C
For 1 STB	32Mbps	-	-
For 2 STBs	16Mbps	16Mbps	-
For 3 STBs	10Mbps	10Mbps	10Mbps
Copy (AtoB)	-	41Mbps	-

Next, we show result of throughput on multicast model in table 2.

Table 2: Throughput on Multicast Model.

Download	A	B	C
For 1 STB	21.7Mbps	-	-
For 2 STBs	21.8Mbps	21.8Mbps	-
For 3 STBs	21.7Mbps	21.7Mbps	21.7Mbps

Incidentally in our simulation, throughput of Client-Server model is not faster than that of Multicast model when LAS sends content to only one STB. Throughput of UDP is generally faster than that of TCP. However UDP does not have reliability about transmission of a message because UDP does not have function of flow control. So in our simulation, on the purpose of an increase in reliability about content distribution over UDP, we dared to reduce this throughput.

5 DISCUSSION

5.1 Security

We discuss security, defined in chapter 2, of the proposed system in this section.

- **Terminal Legitimacy:** If user views content, STB or PP needs to generate decryption key (Content Key or Re-encryption Key) bound to terminal ID, and thus even if malicious person vies content on other terminal, Encrypted Content is not able to run this terminal.
- **Wiretapping Impossibility:** Even if the contents are obtained through wiretapping, malicious person cannot generate decryption key, so illegal use of content is protected.
- **Illegal Copy Process Impossibility:** If user wants to use content, Issue Certification Code or STB Certification Code must be verified in section 3.4 and 3.5. Even though malicious person/STB obtains Content Using Info. with hardcopy, the malicious person/STB fails in both verification of code because of necessity of Content/Re-encryption Key.
- **Replay Attack Impossibility:** In case of obtaining legal account and STB Certification Code when STB received content, malicious person/STB can pass verification of STB Certification code. However this STB cannot decrypt Encrypted Content with key using verification of STB Certification Code, so Verification of Issue Certification Code is failed. Thus other terminal cannot copy content.
- **Privacy Protection:** PP's ID is used on Re-encryption Key, and LAS can know $g^{f(ID1b)} \bmod p$. However LAS cannot obtain original PP's ID, so user privacy about using terminal without STB is protected against LAS.

5.2 Performance

In Client-Server model, if one STB downloads content, downloading throughput is 32Mbps. And in Multicast model, downloading throughput is over 21.7Mbps. In Japan, throughput on Digital High-Vision is about 17Mbps (ground-wave) or 20Mbps (satellite). Considering this result, we can adopt our proposed system to any types of content file.

In case of copying, throughput is 41Mbps, so user can copy content without long waiting time.

6 CONCLUSIONS

We proposed new DRM system. In this system, usability of content use about copying improves by permission of First Generation Copy, and distribution/viewing of illegal copy is denied by prohibition of Second Generation Copy. Content is verified in three times checks, Generating Content key or Re-encryption Key bound to terminal ID, Issue Certification Code and STB Certification Code, so malicious person/STB cannot use/copy content illegally. Furthermore we made simulation system and evaluated performance. As a result, we could confirm that this system was realistic about current movie file.

In the future, we will apply this system to some types of multicast systems or broadcasting and confirm that the proposed system is of practical use. And on the purpose of simple implementation, we will revise our program module.

REFERENCES

The Association for Promotion of Satellite Broadcasting, http://www.bpa.or.jp/index.html

The Association for Promotion of Digital Broadcasting, http://www.d-pa.org/

Digital Living Network Alliance, http://www.dlna.org/en/industry/home/

4C Entity CPRM, http://www.4centity.com/

iTunes Overview, http://www.apple.com/itunes/overview/

OpenMG, http://www.sony.net/Products/OpenMG/

Association of Radio Industries and Businesses, 2003. Conditional Access System Specifications for Digital Broadcasting, In *ARIB STD-B25*. ARIB.

Fujii, H., Takei, H., Nakasato, K., Ihori, S., Miyake, N., 2001. A New Method of Copyright Protection Enabling Less Restricted Personal Copy. In *EIP2001*. IPSJ.

Spencer, C., Avni, R., 2003. DRM and Standardization – Can DRM Be Standardized?, In *Digital Rights Management*, Springer-Verlag.

Whitfield, D., Martin, E. H., 1976, New directions in cryptography, In *Trans. On Information Theory*, IEEE.

Carlos, S., Miguel, D., Jaime, D., 2006, Digital Object Rights Management –Interoperable Client-side DRM Middleware, In *SECRYPT2006*, INSTICC.