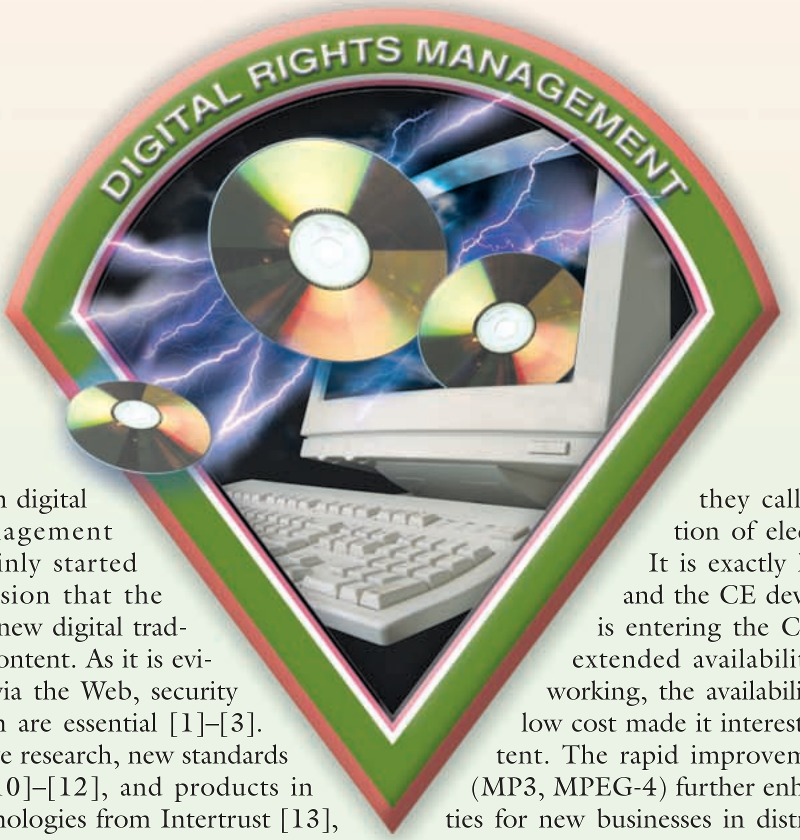
Digital Rights Management in Consumer Electronics Products

Willem Jonker and Jean-Paul Linnartz

Secure electronic content distribution is essential.



LOGO COMPOSITE: ©1995 PHOTODISC, INC., ©DIGTIAL STOCK, ©COREL

The interest in digital rights management (DRM) mainly started from the vision that the Web would become a new digital trading infrastructure for content. As it is evident from the piracy via the Web, security and content protection are essential [1]–[3]. This has triggered active research, new standards [4]–[9], legislation [10]–[12], and products in Web-based DRM technologies from Intertrust [13], IBM [14], Sony [15], and Real Networks [16]. Earlier on, content owners, the consumer electronics (CE) industry, and consumers were already in discussion about the protection of digital assets. This has resulted in media-related copy protection mechanisms for optical discs [18]–[22] as well as in conditional access systems that support current pay TV services [23], [26], [27]. The focus and priority changed with the advent of Web music exchange services like Napster [49]. Since important stakeholders see their business at risk, they call for secure distribution of electronic content [12]. It is exactly here, where the Web and the CE devices meet, that DRM is entering the CE world. Besides the extended availability of (Internet) networking, the availability of mass storage at low cost made it interesting to exchange content. The rapid improvements in compression (MP3, MPEG-4) further enhanced the opportunities for new businesses in distribution of entertainment content and at the same time accelerated the need for protection.

Technically speaking, DRM may be regarded as an extension of copy protection measures. However, DRM and copy protection fall under a different regime and different regulations. For the copy protection of mass-distributed content (broadcast, CD, etc.), the definition of user rights, e.g.,“fair use,” has become quite clear over the years and the scope of acceptable measures is reasonably well defined. For instance, copy-

1053-5888/04/$20.00©2004IEEE

protection states are time variant. On the other hand, DRM controls content for which the consumer and the rights owner set up an individual contract that can contain much more restrictive usage rights. DRM systems in general allow for usage rights that change over time (e.g., number of times or days left to play content). Another distinction is that DRM usually refers to closed systems.

DRM controls content for which the consumer and the rights owner set up an individual contract that can contain much more restrictive usage rights.

The Current CE Environment and Its Content Protection Technology

The current home CE environment consists of rather isolated devices that all have their own specific content formats. Although network-based distribution is emerging, the packaged media such as CDs and DVDs play a dominant role in the current distribution of audio and video content. Judging by the recent successful introduction of new disc formats such as the rewritable DVD+RW and Super-Audio CD (SA-CD), we do not expect this to change rapidly. As the protection of audio and video content on packaged media will remain important, future DRM solutions will have to take packaged media into account.

The encryption of content is an essential element of a strong secure storage system. Nonetheless, several approaches exist that are based on in-the-clear content. The prime motivation is the market dominance of legacy media and players, such as the CD, that generate almost all of the revenues in their segment. Although the standard for the CD is described unambiguously, some recently released titles intentionally divert from this standard, in the hope that CE players flawlessly play the content, while PC-oriented disc drives face problems reading the disc [3]. These technologies face legal and technical challenges: circumvention methods appear to be reasonably low-tech on PCs and some CE devices suffer from playback problems with legally obtained content as these products do not adhere to licensing conditions.

Most new solutions for content protection are based on a few core technologies, such as cryptography and watermarking, and in future presumably also on fingerprinting.

Cryptography-Based Content Protection

Cryptography-based content protection has two ingredients: encryption algorithms and key management. In a CE environment there are two major challenges: 1) the development of encryption, authentication and key management algorithms with low resource (power, CPU, storage) requirements and 2) the development of mechanisms for secure storage of keys, both in devices as well as on media. The economic model for CE products differs essentially from that of PCs. The relatively long life cycle, and the strong pressure on lowering the bill of material, typically leads to highly dedicated implementations with little flexibility. On one hand this facilitates secure and tamper-resistant implementation, while on the other hand it limits the upgradability of security measures.

Cryptographic algorithms are a mature area of research [40], [41]. However, copy management cannot easily be formalized into "Alice and Bob" protocols, as commonly studied in cryptography. In fact, Alice, in our case the content owner, intends to sell information to an unreliable customer Bob, without allowing Bob to further disseminate this information. Evidently there is no cryptographic or information theoretical solution to this problem. Nonetheless, international standardization efforts have recognized that a workable way to redefine the problem is as follows: Alice sells digital data to an unreliable Bob, who can only process this data on a trusted device. The protection relies on Bob's inability to access the data directly.

Cryptographic Algorithms for Media Protection

Encryption of content was first used at large scale in the DVD video standard [20], [18], [21], using the content scrambling system (CSS) for encryption and key management. The encryption operates over 40 b, but the effective key length of the cipher is in the order of 8–16 b. The effect of its protection primarily comes from the enforcement of licensing rules rather than from a technical hurdle in its own right. CE products largely adhere to the copy protection methods. According to the U.S. Digital Millennium Copyright Act (DMCA) [10], the use and dissemination of the DeCSS code to circumvent CSS is illegal. Since PC software packages to "back up" a DVD are commercially available, increasingly many countries adopt similar legislation. Presumably, new generations of standards will rely on stronger encryption of content. For instance, SA-CD, the successor of the popular audio CD, encrypts its digital music signal that is placed on an optical disc with DVD-like physical properties. For recordable discs, two systems are available, namely the copy protection for recordable media (CPRM), often referred to as 4C reflecting the four companies IBM, Intel, Toshiba, and Matsushita [19], and the protected data storage system (PDSS) by Philips and Sony [22]. Both systems are generic in the sense that the solution also works for other media, such as hard discs or flash memory cards. For instance, secure digital (SD) flash cards uses CPRM. Meanwhile Sony promotes Magic Gate [12] to protect content on

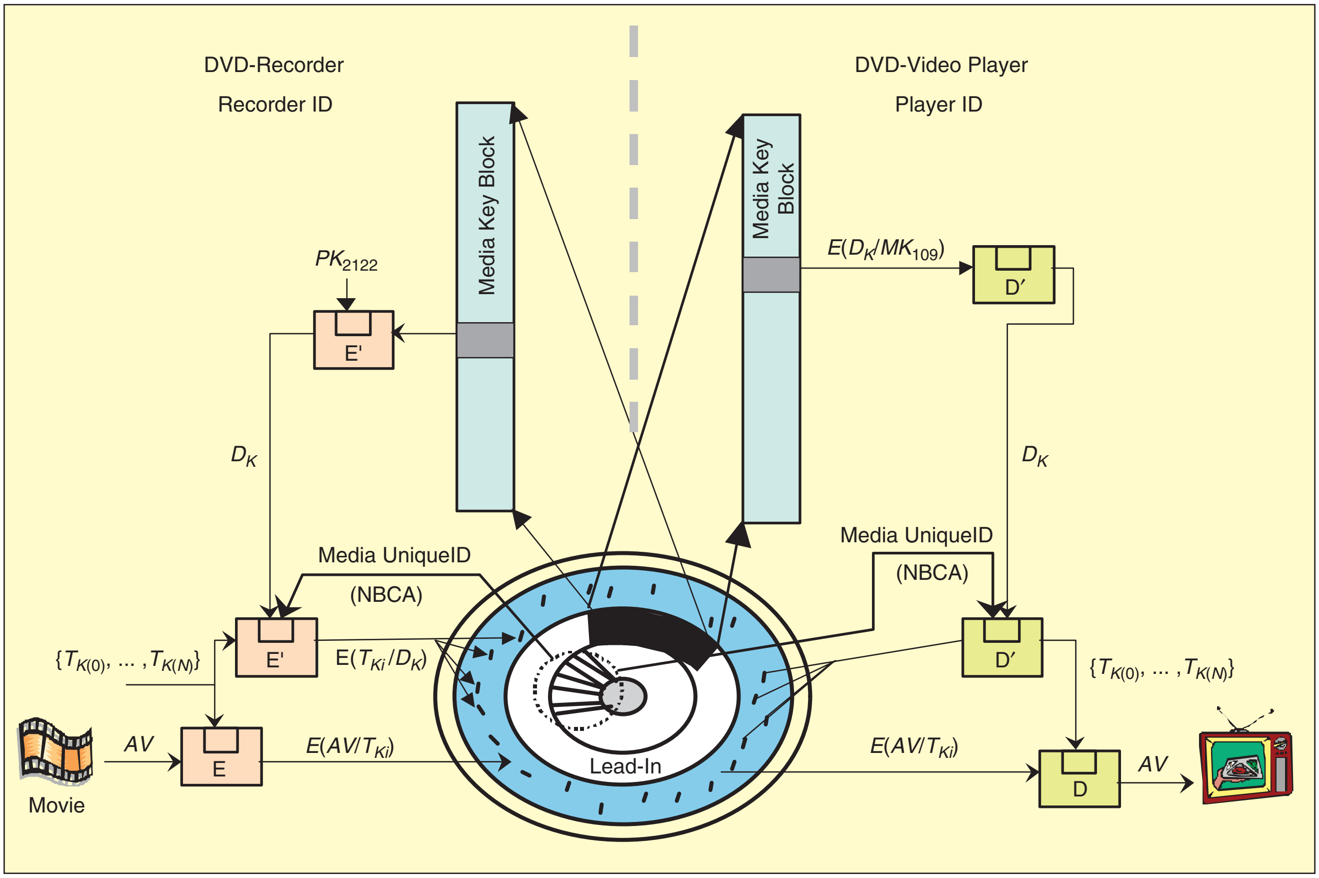
DRM originated from the Internet community where people understood that the Internet had the potential of becoming the digital marketplace of choice for the trading of digital items.

flash memory cards, and Microsoft bases content protection on their Window Media Player.

Key Management on Media

Whenever content is encrypted, preferably the decryption keys partly come from a secure environment inside the player (otherwise any hacker could create a noncompliant player that contains the same secrets as a compliant one, thereby being able to misuse the content) and partly from a secure segment of the disc (otherwise a bit-by-bit clone of the encrypted content would play on any player that plays an original). Technologies for embedding unique identifiers on optical disc, such that consumer writers cannot mimic these, have been introduced. CSS relies on the inability of the firmware to access the lead-in areas of video DVDs. SA-CD uses a pit signal processing physical disc mark (PSP-PDM). Another example is the wobble key, which is a radial modulation of the location of the data track on the disc [38]. Such techniques essentially improve existing standards for prepressed discs as the storage of disc keys is better resistant to attacks. A further step is the embedding of a contact-less smart-card chip into a disc [39].

Figure 1 presents an early, publicly released version of CPRM. When CPRM device records incoming video, it generates title keys $T_{k(n)}$ and uses these to encrypt the video, before formatting it into sectors and writing these to the disc. The title tey itself is also encrypted and stored in the disc sector headers. The key to encrypt the T_K consists of a disc-unique ID, obtained from the burst cutting area (BCA) on the disc and by a disc key D_k. The disc key (DK) is specific for each disc and can be obtained from the media key block (MKB), using a player-specific key. The MKB is structured to allow reconstruction of D_k by any compliant nonrevoked device, even though all devices have different keys. The player derives D_k from the same MKB and its own player key, and then it derives title keys using the BCA code and the disc key D_k to decrypt the appropriate fields in the sector headers. Revocation appears to become a relevant feature for new systems. Compromised devices can be excluded (i.e., revoked) by distributing a new electronic key



▲ *1. Schematic diagram of CPRM content protection on a recordable optical disc.*

block (EKB) that gives the required keys to all devices except the compromised ones. Updated EKBs can be distributed via pre-pressed discs or via EMD services.

Figure 2 illustrates how the PDSS uses a hierarchical key management solution to supports right management for each individual asset, i.e., for every content file. PDSS generates a key locker key from a number of hidden identifiers in the optical disc, namely a disc-specific secure identifier, and a key from a hidden-channel for the asset file, that also verifies the compliance.

Each device contains a device key, which is used to calculate a common secret from the key locker. The key locker key, together with the key locker, generates a 128-b DK and digital asset rights. A DK is used to decrypt the asset data sector. Protected assets are reencrypted in the drive. This allows the use of different security solutions tailored to the specific treats of the (hardware) interface between disc and drive and those of the (software) interface between drive and PC. Not only assets can be delivered to a PC application but also the digital rights for a DRM application. For CE applications, where the electronics implementation inherently is more robust, the reencryption is omitted.

Watermarking-Based Content Protection

Content eventually needs to be presented in the clear to the human consumer. While the link protection of digital content can be extended all the way to digital monitors and speakers, eventually an analog signal (that inherently is vulnerable to copying) must be created. Additional protection is needed to prevent that this analog signal can successfully be offered to a (compliant) recorder, as if it were the user's personal creation.

Watermarking technology allows the embedding of hidden data, e.g., copyright information, in the digital content [32]–[39]. While cryptography is applicable only in the digital domain, in the analog domain watermarking is the more effective content protection technology. Cryptography behaves as a protective envelope that prevents unauthorized access, but once the content is decrypted the protection is completely removed. In contrast to this, detectable remnants of watermarks are more likely to remain after an attack. That is, even though an attacker manages to "remove" a watermark in the sense that a particular detector during a particular test does not see the watermark, that does not mean that other detectors (particularly future ones) do not recognize the watermark. It is now well recognized that cryptography and watermarking complement each other and these technologies are both essential to prevent major leaks.

Watermarking for DVD: Play Control

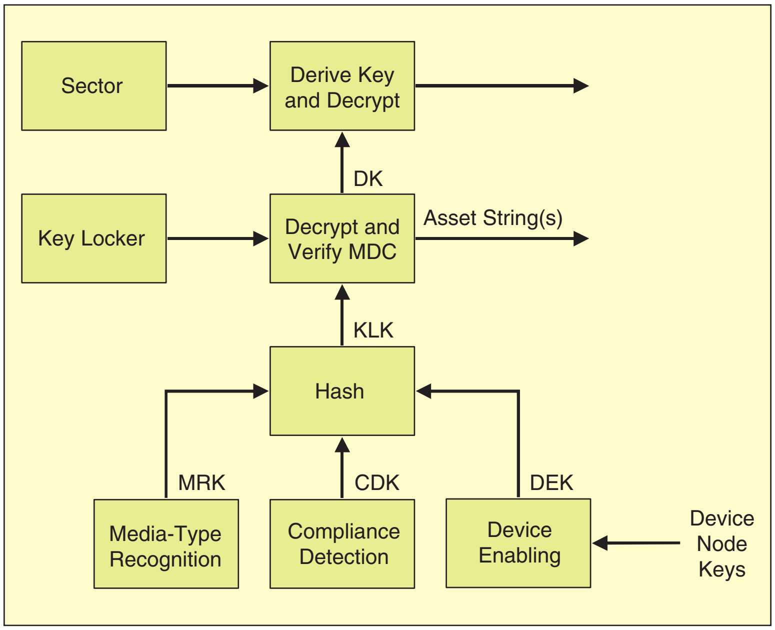
In 1997, the DVD Copy Protection Technical Working Group (CPTWG) started to discuss the use of watermarking [18], [20], [21]. Its DataHiding SubGroup (DHSG) defined requirements for a system that should execute "play control" of DVD discs. Rather than only checking the copyright status during the recording of video, the idea was to verify the status also during the playback. Watermarked content is released on prepressed (ROM) discs, but its appearance on recordable (R, RW) media indicates that an illegal copy was made. The watermarking system under discussion is at the same time designed to be simple and to satisfy all requirements with respect to perceptual quality and robustness.

Watermarking for SDMI Audio: Content Screening

The use of watermarks for audio was discussed in the Secure Digital Music Initiative (SDMI). The intention was to define a system that prevents redistribution of content over the Internet. Original released music contains both a fragile and a robust watermark. During the (MP3) compression of the music the fragile watermark vanishes. An SDMI-compliant device would always combine the compression with an encryption that binds the content to the compliant domain of the legitimate user. PC and consumer devices accept to import music with both watermarks but refuse to handle in-the-clear music that contains a robust watermark but no fragile watermark, as this was deemed a copy that was illegally distributed over the Internet. After scientific attacks [35], negative publicity about the user friendliness of the solutions and a lack of business interest, SDMI became dormant.

Fingerprinting

An important drawback of watermarking is that the embedding process needs to change the content, which makes it useless in the case of already released content.



▲ 2. Schematic diagram of PDSS content protection on a recordable optical disc.

> **The large-scale availability of Internet-connected consumer electronic devices will certainly accelerate the growing importance of the electronic content delivery channel.**

Fingerprinting (see, for example, [42]–[45]) is a new technology that can be used for content identification. The prime objective of multimedia fingerprinting is to establish the perceptual equality of two multimedia objects: not by comparing the (typically large) objects themselves, but by comparing the associated fingerprints. The fingerprints of a large number of multimedia objects, along with their associated meta-data (e.g., name of artist, title, and album) are stored in a database.

Broadcast monitoring is probably the most well-known application for audio fingerprinting [47]. It refers to the automatic playlist generation of radio, television, or Web broadcasts for purposes such as royalty collection, program verification, advertisement verification, and people metering. Another application is filtering, i.e., active intervention in content distribution for instance in a file sharing service. Starting in June 1999, users who downloaded the Napster client [49] could share and download a large collection of music for free. Later, due to a court case by the music industry, Napster users were forbidden to download copyrighted songs. In May 2001 Napster introduced a fingerprinting system [46], which filtered out copyrighted material. Owing to Napster's closure only two months later, its effectiveness is not publicly known.

Content Protection in the Future Networked CE Environment

The content protection technologies discussed so far focus on disc copy protection. Although discs will remain an important content distribution channel in the future, the arrival of the Internet has introduced a widely accessible new content distribution channel: electronic content distribution via the network. While electronic audio and video distribution is currently mainly targeted to the PC, CE manufacturers are starting to deliver Internet connectivity directly into their products, such as Internet radios, home cinema-sets with Internet connections, and high-end TVs with Internet connections. The large-scale availability of Internet-connected CE devices will certainly accelerate the growing importance of the electronic content delivery channel. In addition, growing storage capacity and more efficient coding techniques like MP3 and MPEG4 enable the exchange of large amounts of digital content. However, content providers are reluctant to make their premium content available if no adequate content protection mechanisms are in place. This explains the growing interest in DRM in the CE industry as a way to guarantee the flow of premium quality content to their devices.

Digital Rights Management

DRM originated from the Internet community where people understood that the Internet had the potential of becoming the digital marketplace of choice for the trading of digital items. Just like any marketplace, the digital marketplace needs rules for trading and use of digital items. So DRM can be seen as the whole collection of commercial, legal, and technical measures to enable trading of digital items on electronic infrastructures. As the digital marketplace appeared to be ideal for automating most of the DRM, DRM systems emerged. Although DRM systems are still in their infancy, a number of common elements can be identified.

▲ Digital item description formalism—the description formalism is used to describe the digital item. MPEG-21, particularly, has an elaborated description formalism that supports description of complex and composite digital items. In the CE domain the focus is mainly on audio and video content and as a result simple item identification suffices.

▲ Rights language—rights languages like XrML [9], ODRL [51], and LicenseScript [52] are used to express how (and by whom) digital items may be used. DRM rights languages are often expressed in XML. Since for digital items in general there are many possible situations, DRM rights languages tend to be complex. There is a continuous discussion about this complexity in the CE domain. First of all, in the case of content protection, the focus is mainly on a limited set of manipulations that need to be addressed, such as playing, copying, etc. In addition, CE devices often distinguish themselves from computers in their ease of use. And thus, complex DRM rights are not what consumers expect of CE devices.

▲ Licenses—licenses are used as a mechanism to distribute rights (that are expressed in the rights language). By bringing a license and a digital item together in a device, the device can inspect the right to see what it may do with the digital item. In some cases licenses also contain keys needed to access the digital item.

▲ Content protection scheme—most DRM systems rely on cryptography to protect the content. In this case there is a need for an additional key distribution scheme, for example, by means of licenses. Some DRM systems rely on watermarking; in this case content is in the clear and the system completely relies on compliant devices.

▲ Device compliancy—DRM systems rely on device compliancy to function properly. Device compliancy requires that devices that implement (part of) the DRM functionality function according to the "rule" imposed by the DRM system. This means that devices do not access digital items in case of absence of a license and also that they do not carry out operations on digital items that are not allowed by the associated rights (e.g., copying or sending content in the clear over nonprotected links).

▲ Device robustness requirements—since devices manipulate licenses, rights, and keys, the manipulation and storage of these items needs to take place in a secure environment. As a result DRM systems impose hardware and software tamper resistance requirements on devices.

Cryptography-based content protection has two ingredients: encryption algorithms and key management.

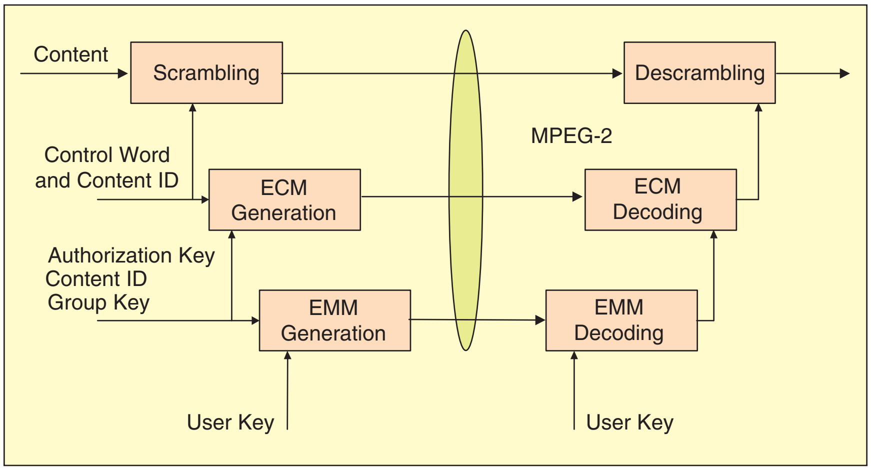
DRM in the Networked CE Environment

For CE devices, the (free to air) broadcast system is the dominant network. Currently, DRM hardly plays a role, except for conditional access systems used in pay-TV. However, with the advance of digital TV, the discussion on content protection of broadcast content is taking off as can be seen in the adoption of the broadcast flag in the United States [29]. Next to the broadcast network, the broadband network (the Internet) is becoming an important content delivery channel in the future as has been described above. Currently most of the DRM work in the CE domain is concentrated here. Finally, there is the mobile network. Although currently mostly used for telephony and short messaging, we see emerging content delivery in the form of ring tones and images, which has raised the interest in DRM also in this domain.

DRM in the Broadcast Domain

The only widespread form of content protection in broadcast is that of conditional access (CA) systems. CA systems rely on cryptography as a basis. The systems use SetTopBoxes and smart cards as secure devices. Content is encrypted at the source and decrypted in the STB using the secret keys stored in the smart card. Most of the work has been carried out in MPEG-2 and MPEG-4 and is centered on encryption of MPEG-2 transport streams and the MPEG-4 IPMP system [27].

Figure 3 gives a high level overview of the MPEG-2 TS encryption and decryption in a typical CA system. The system is hierarchical; at the highest level there is the content that is encrypted using a control word contained in the so-called entitlement control message (ECM). This ECM also contains the content ID to be used at descrambling time to associate the right control word with the right content. The ECM is encrypted using an authorization key that is contained in the entitlement management message (EMM). As well as the ECM the EMM contains a content identification. The EMM is encrypted by means of the user key. At the decoding side, this key is stored in the smart card.



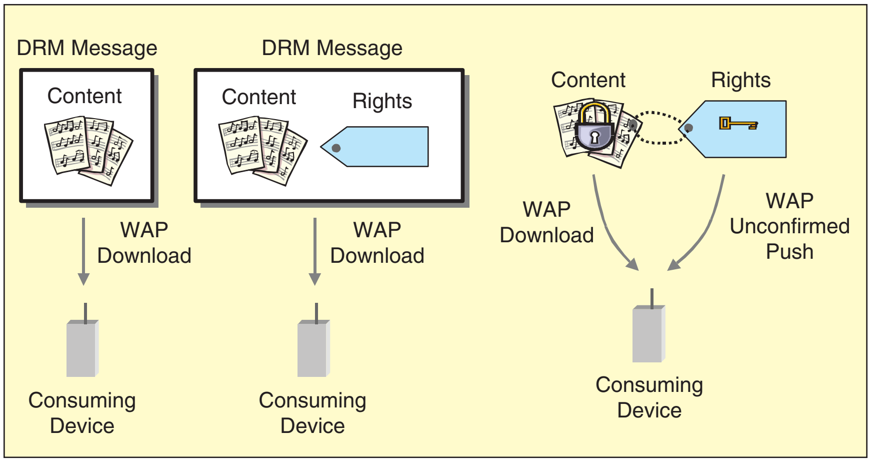
▲ *3. Content encryption in MPEG-2 CA.*

As stated above the advance of digital TV leads to a renewed interest in content protection and DRM in the broadcast world. Most activities take place in DVB-CPT [26] and TV-ANYTIME [23]. The discussion there is focused on two major themes: how to evolve from copy protection to DRM and how to extend the protection beyond the STB into the home network (see below).

DRM in the Broadband Domain

DRM in the broadband domain is currently mainly PC dominated with players such as RealNetworks, Microsoft, Apple, and IBM. In the audio domain, we see that after an initial period of legal fights against peer-to-peer networks, electronic music distribution services are emerging that also can become very relevant for CE devices. Figure 4 shows the architecture of a typical PC-centered electronic music distribution EMD service, namely that of RealNetworks.

More recent PC centered systems such as, for example, Apple iTunes [17] or Sony Open Magic Gate [15] extend the system in Figure 5 towards download of content from the PC to portable CE devices such as MP3 players or to discs. For the time being these are proprietary solutions (iPod, Magic Gate memory sticks). However, any full CE DRM solution will require a uniform DRM architecture, independent of the specific distribution channel, content type, and medium format. Such a solution will have to be end-to-end, in the sense that it will have to guarantee protection of the digital content all the way from the production source, over the distribution channels up till its destination in a CE device: being it either storage on fixed or removable media, or rendering. The CE

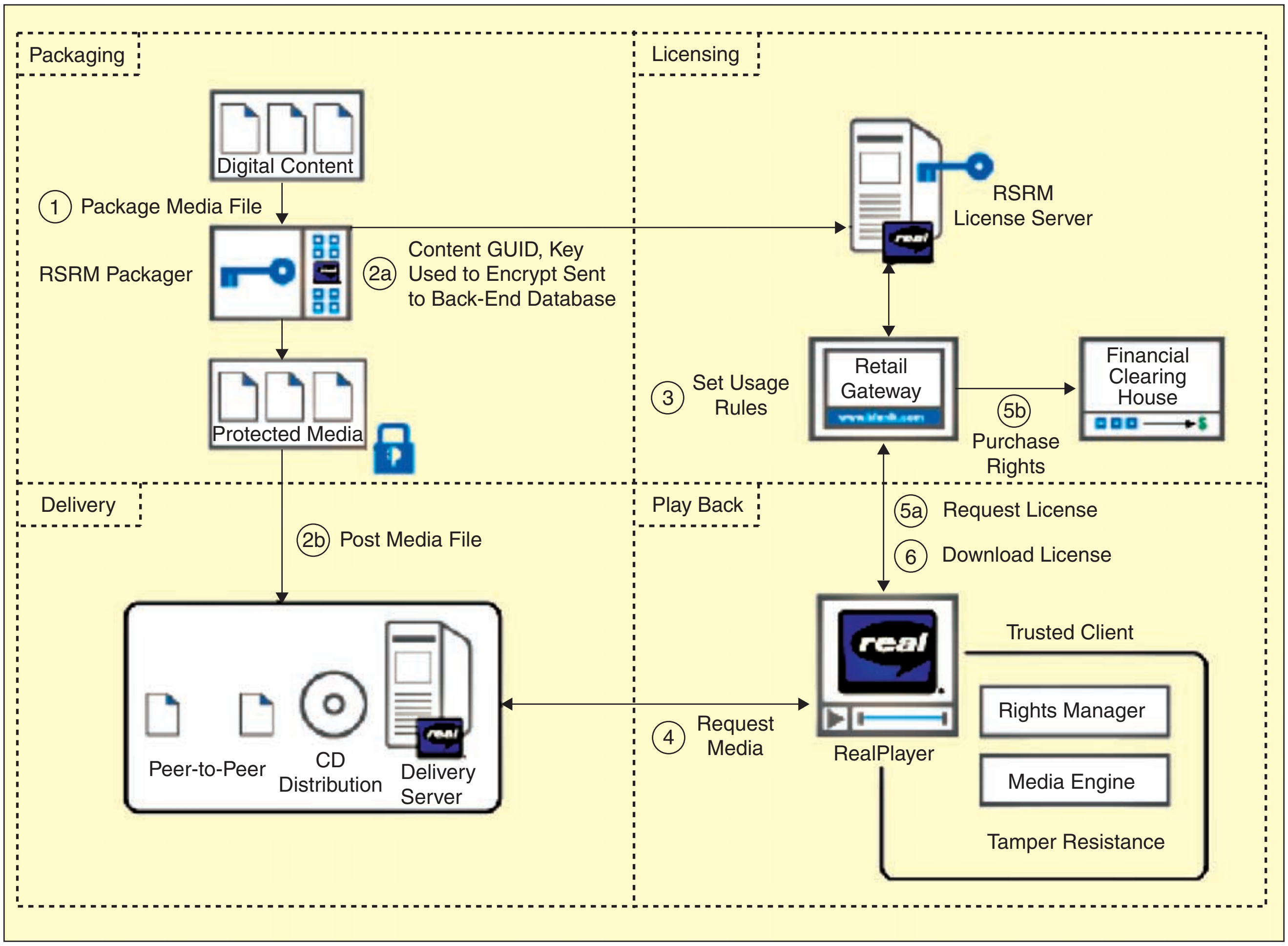


4. OMA version 1 download modes.

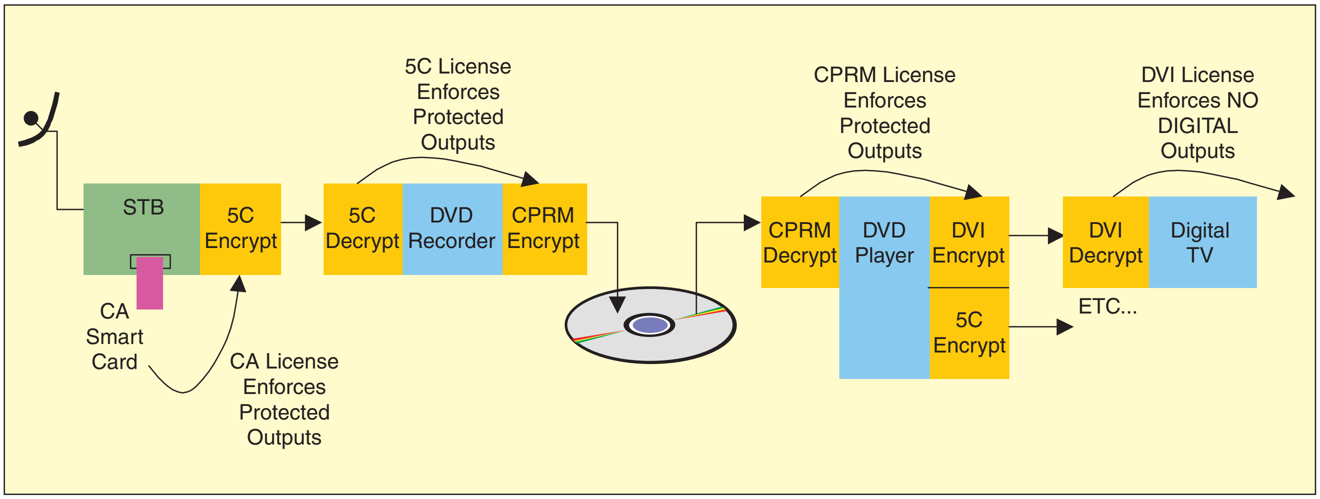
industry is slowly entering this domain. Issues that are high on the CE agenda are: reduction of the complexity of XML based rights languages, tamper-resistant hardware and software solutions both in the PC and CE domain (for example the activities in the Trusted Computing Group [30], [31]), lightweight DRM clients that can be deployed on resource constrained CE devices, and compatibility with disc formats.

DRM in the Mobile Domain

Content distribution in the mobile domain is still rather limited; however, with the growing bandwidth of mobile systems, DRM will become an issue here as well. For this reason the Open Mobile Alliance (OMA) [8] is developing DRM solutions. OMA DRM version 1 supports three content download modes as depicted in Figure 4. The simplest mode is the "forward lock" (left) where the content is just downloaded via WAP download without additional security measures but the compliance rule that this content may not be forwarded to other devices. The second mode (middle) is the "combined delivery" where in addition to the content some rights are WAP downloaded. The compliance rule to be obeyed is that the device respects the rights. Finally, there is the "separate delivery" mode in which there is content encryption and separate delivery of the rights including the key. It is clear that the security deployed here is very weak, so OMA is currently specifying a sec-



5. RealNetworks PC centered EMD system.



▲ *6. CPSA in a home network.*

ond version with public key cryptography to improve security of delivery.

Home Networks

The inclusion of (mainly wireless) network interfaces in CE devices leads to the establishment of home networks. Up till now content protection in home networks, e.g., the 5C scheme [28], has mainly focused on physical link and storage protection. However, there is a growing awareness that content protection and especially DRM should be addressed at the middleware of even at the application layer. This explains, for example, the growing interest in DRM support in Universal Plug and Play (UPnP) [24]. Most prominent however is the work on authorized domain (AD) as explored in DVB [26].

An AD is a protected home network environment where content can freely float around and be consumed; content import and export from such a domain, however, takes place under strict control of the DRM system. Although the original idea was to have no DRM control inside the AD, more recently some DRM control is introduced to support rental models where content will automatically be removed from the domain after a certain period of time.

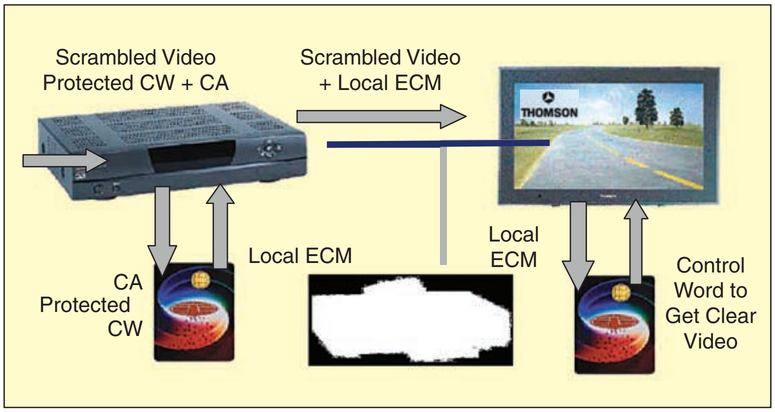
There are different ways of realizing an AD. An example is the copy protection system architecture (CPSA) [25] that combines 4C media protection [19] with 5C link protection [28] technologies to provide a protected home network. Figure 6 illustrates a protected home network.

Another way of realizing an AD is Thomson's SmartRight [53] system. Rather than exploiting media and link protection, SmartRight builds upon the conditional access approach. Each device in the home network is equipped with a smart card that contains the key to decrypt the encrypted content stream. Upon entrance in the home the SetTopBox replaces the ECM of the CA stream with a local ECM (LECM). This LECM is unique to the home network and in such a way the content is "bound" to this specific home network. Currently SmartRight is mainly broadcast oriented. The system setup is depicted in Figure 7.

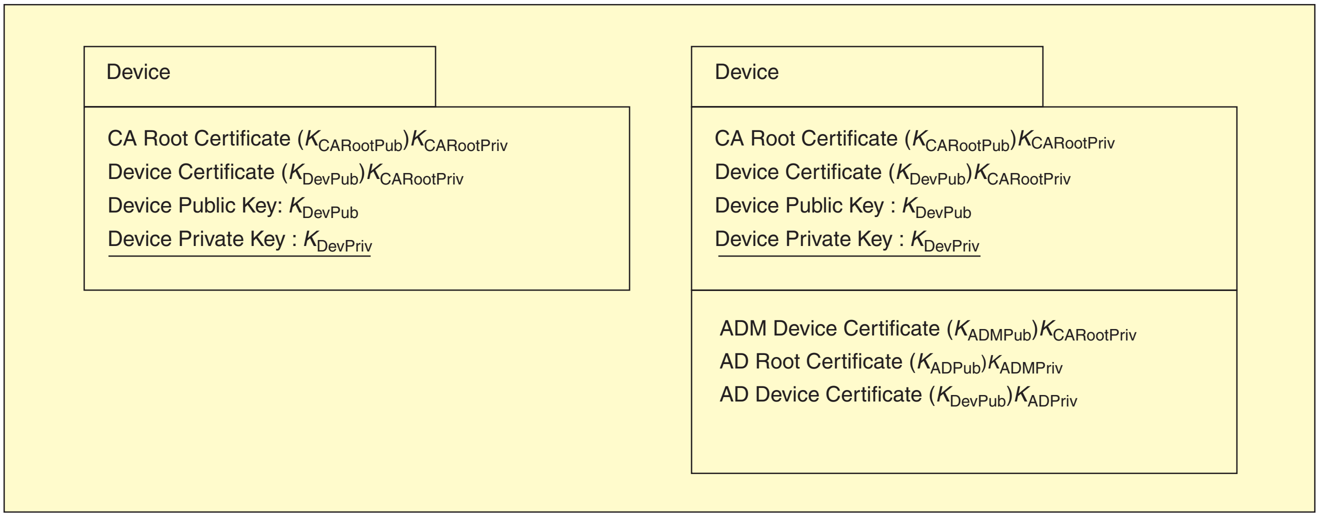
At Philips Research, the authors explore various solutions for an AD implementation. One of these is the device-based AD, which defines an AD as a collection of devices belonging to a specific household [50]. The system is neither targeted to a specific content delivery channel nor to a specific content type. The system uses certificates and a public key cryptography as its underlying content protection mechanism.

Figure 8 shows the certificates and keys stored in a compliant and AD member device, respectively. A compliant device has a CA root certificate to "proof" compliance and a device certificate for authentication purposes. Once a compliant device becomes member of a specific AD it stores the specific certificate chain that allows it to proof its AD membership.

Free content exchange between devices is only allowed for devices in the same AD (e.g., home network); this is ensured through a symmetric domain membership verification protocol based on the domain certificates.



▲ *7. Example of SmartRight Network.*


Device
CA Root Certificate $(K_{\text{CARootPub}})K_{\text{CARootPriv}}$
Device Certificate $(K_{\text{DevPub}})K_{\text{CARootPriv}}$
Device Public Key: K_{DevPub}
Device Private Key : K_{DevPriv}
Device
CA Root Certificate $(K_{\text{CARootPub}})K_{\text{CARootPriv}}$
Device Certificate $(K_{\text{DevPub}})K_{\text{CARootPriv}}$
Device Public Key : K_{DevPub}
Device Private Key : K_{DevPriv}
ADM Device Certificate $(K_{\text{ADMPub}})K_{\text{CARootPriv}}$
AD Root Certificate $(K_{\text{ADPub}})K_{\text{ADMPriv}}$
AD Device Certificate $(K_{\text{DevPub}})K_{\text{ADPriv}}$

▲ *8. Security elements in devices.*

Content is always bound to a specific device in the domain. Encrypting the content with the public key of the specific device does this. In this way only the device can access the content by using its private key. By using a key hierarchy, laborious reencryption of the content itself can be avoided.

At Philips Research several prototypes of AD systems exist, and currently a demonstration implementation on the Philips Internet-connected Streamium devices is being developed.

Finally, we mention the IBM home network protection scheme xCP [55] based on broadcast encryption [54] as another alternative home network protection scheme.

Summary

In the current CE environment we see many activities in content protection and DRM, which could lead to a situation with many (conflicting) standards and unnecessary limitations on the flow of content over various devices. As a result, the main challenge in the CE environment is to develop DRM solutions that allow interacceptable exchange of content that is acquired via any of the main distribution channels to the customer, being discs media, broadband, broadcast, and wireless. To achieve this, a number of important architectural and research issues have to be resolved, including:

▲ development of an overall DRM architecture

▲ development of a standard DRM solution for home networks

▲ development and enhancement of existing copy protection techniques

- –enhance medium-based techniques to support personalization and rights management
- –enhance storage and link protection to support DRM
- –develop a solution to close the analog whole.

These solutions can only emerge through tight cooperation between the stakeholders and through the development of open standards.

Acknowledgment

We would like to thank Toine Staring, Joop Talstra, Ton Kalker, and other members of our research group for their help in putting together this article.

Willem Jonker studied mathematics and computer science at Groningen University. He then joined Delft University of Technology for his Ph.D. research on knowledge-based systems. After receiving his Ph.D. from the University of Utrecht he joined KPN Research. In 1992 he joined the European Computer Industry Research Center, Munich. In late 1994 he returned to KPN Research to head the database group focusing on applications of database technology in telecommunication. In 1999 he founded and headed the new research department of KPN Research at the campus of Twente University. In September 2001 he joined Philips Research. He is also a part-time full professor of computer science at Twente University. Among his research interests are database systems, multimedia databases, distributed applications, content management, and digital rights management.

Jean-Paul Linnartz received his Ir. (M.Sc. E.E.) degree in electrical engineering from Eindhoven University of Technology, The Netherlands, in 1986. During 1987–1988, he worked with the Netherlands Organization for Applied Scientific Research on UHF propagation. He received his Ph.D. from Delft University of Technology in 1991, where he was an assistant professor (1988–1991) and associate professor (1994). In 1992–1995, he was an assistant professor at the University of California at Berkeley. In 1995, he joined Royal Philips Electronics to set up a research activity on security, conditional access, and copy control for multimedia content at the Natuurkundig Laboratorium (Nat.Lab.), Eindhoven, The Netherlands, where he is currently department head. He has 20 patents and he authored more than 100 papers, various books, and an educational CD-ROM.

References

[1] "Special report: Copy protection," (special section), *IEEE Spectr.*, vol. 40, pp. 20–35, May 2003.

[2] B. Pence, "The impact of MP3 and the future of digital entertainment products," *IEEE Commun. Mag.*, vol. 37, no. 9, pp. 68–70, Sept. 1999.

[3] A. Goroch, "The business of digital copyright, content protection and management in the consumer digital era," *Digital Tech Consulting,* Dallas, TX, 2002.

[4] W3C [Online]. Available: www.w3.org/

[5] [Online]. Available: www.ietf.org/

[6] [Online]. Available: www.sdmi.org

[7] [Online]. Available: http://www.licensing.philips.com/copyright/

[8] [Online]. Available: www.openmobilealliance.org/

[9] XrML—The Technology Standard for Trusted Systems in the eContentMarketplace [Online]. Available: http://www.xrml.org/

[10] Digital Millennium Copyright Act (DMCA) [Online]. Available: http://www.loc.gov/copyright/legislation/dcma.pdf

[11] [Online]. Available: http://www.europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_167/l_16720010622en00100019.pdf

[12] D.S. Marks and B.H. Turnbull, "Technical protection measures: The intersection of technology, law and commercial licenses," *European Int. Prop. Rev.*, pp. 198–213, May 2000.

[13] [Online]. Available: http://www.intertrust.com

[14] [Online]. Available: www.ibm.com/software/data/emms

[15] [Online]. Available: http://www.sonysemiconductor.co.uk/pdfs/cxnews/CX20%20Techno%20World%20Memory%20Stick%20Copyright%20Protection.pdf; http://www.sony.net/Products/homeaudio/net_md/faq02.html

[16] [Online]. Available: http://www.realnetworks.com/

[17] [Online]. Available: www.apple.com/music/store/

[18] Copy Protection Technical Working Group [Online]. Available: www.cptwg.org

[19] [Online]. Available: http://www.4CEntity.com

[20] J.A. Bloom, I.J. Cox, T. Kalker, J.P. Linnartz, M. Miller, and C. Traw, "Copy Protection for DVD video," *Proc. IEEE*, vol. 87, no. 7, pp. 1267, July 1999

[21] A.E. Bell, "The dynamic digital disk," *IEEE Spectr.*, vol. 36. no. 10, pp. 28–35, Oct. 1999.

[22] A.A.M. Staring, F.L.A.J. Kamperman, S. Furukawa, Y. Sato, "Protected data storage system for optical discs," in *Proc. IEEE Int. Conf. Consumer Electronics*, Los Angeles, June 17–19, 2003, pp. 332–333.

[23] [Online]. Available: www.tv-anytime.org

[24] [Online]. Available: www.upnp.org

[25] [Online]. Available: http://www.4centity.com/data/tech/cpsa/cpsa081.pdf

[26] [Online]. Available: http://www.dvb.org/dvb_technology/pdf/cfp_cp_cm.pdf

[27] B.J. van Rijnsoever, P. Lenoir, and J.P.M.G. Linnartz, "Interoperable protection for digital multimedia content," *J. VLSI Signal Processing—Syst. Signal, Image, Video Technol.,* vol. 34 no. 1–2, pp. 167–179, 2003.

[28] 5C digital transmission content protection white paper. [Online]. Available: http://www.dtcp.com

[29] [Online]. Available: http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-231A1.pdf

[30] [Online]. Available: www.trustedcomputinggroup.org/

[31] [Online]. http://www.trustedpc.org, http://www.microsoft.com/resources/ ngscb/productinfo.mspx, http://www.intel.com/technology/security/ downloads/scms18-LT_arch.pdf

[32] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Syst. J.*, vol. 35. no. 3/4, p. 12, 1996.

[33] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "A secure, robust watermark for multimedia," in *Proc. Workshop Information Hiding*, Univ. of Cambridge, U.K., May 30–June 1, 1996, pp. 175–190.

[34] I. Cox, J. Bloom, and M. Miller, *Digital Watermarking: Principles & Practice.* San Mateo, CA: Morgan Kaufmann, 2001.

[35] S. A. Craver, M. Wu, B. Liu, A. Stubblefield, B. Swartzlander, D.W. Wallach, D. Dean, and E.W. Felten. "Reading between the lines: Lessons from the SDMI challenge," in *Proc. 10th USENIX Security Symp.*, Aug. 2001.

[36] M. Maes, T. Kalker, J.P. Linnartz, and J. Talstra, G.F.G. Depovere, and J. Haitsma, "Digital watermarking for DVD video copy protection," *IEEE Signal Processing Mag.*, vol. 17, no. 5, pp. 47–57, 2000.

[37] I.J. Cox and J.P.M.G. Linnartz, "Some general methods for tampering with watermarks," *IEEE J. Select. Areas Comm.*, vol. 16. no. 4, pp. 587–593, May 1998.

[38] J.P.M.G. Linnartz, "The ticket concept for copy control based on embedded signaling," in *Proc. ESORICS '98, 5th. European Symposium on Research in Computer Security,* Louvain-La-Neuve, Sept. 1998 (Lecture Notes in Computer Science, vol. 1485*)*, pp. 257–274.

[39] A.H.M. Akkermans and J.A.H. Kahlman, "Chip in disc for optical storage," in *Proc. Int Symp. Optical Memory and Optical Data Storage ISOM / ODS 2002,* Hawaii 7–11 July, MA-1, 2002, pp. 3–5.

[40] B. Schneier, *Applied Cryptography.* New York: Wiley, 1997

[41] A.J. Menez, P.C. van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography.* Baca Raton, FL: CRC Press, 1997.

[42] E. Allamanche, J. Herre, O. Hellmuth, B. Fröbach and M. Cremer, "AudioID: Towards content-based identification of audio material," in *Proc. 100th AES Conven.*, Amsterdam, The Netherlands, May 2001, pp. 1–11.

[43] P. Cano, E. Batlle, H. Mayer, and H. Neuschmied, "Robust sound modelling for song detection in broadcast audio," in *Proc. AES 112th Int. Conv.*, Munich, Germany, May 2002.

[44] J. Haitsma and T. Kalker, "A highly robust audio fingerprinting system," in *Proc. Int. Symp. Music Information Retrieval (ISMIR),* Paris, France, 2002, pp 107–115.

[45] J. Oostveen, T. Kalker, and J. Haitsma, "Feature extraction and a database strategy for video fingerprinting," in Recent Advances in Visual Information Systems (Lecture Notes in Computer Science*)*, vol. 2314, Berlin, Germany: Springer, pp. 117–128.

[46] Relatable [Online]. Available: http://www.relatable.com

[47] [Online]. Available: http://www.watercast.com

[48] [Online]. Available: http://www.shazamentertainment.com

[49] [Online]. Available: http://www.napster.com

[50] S.A.F.A. van den Heuvel, W. Jonker, F.L.A.J. Kamperman, and P.J. Lenoir, *Int. Broadcasting Conv., Secure Content Management in Authorised Domains (IBC2002),* Amsterdam, The Netherlands, 2002, pp. 467–474.

[51] R. Iannella, *Open Digital Rights Language (ODRL) Version 1.0.* IPR System Ptd Ltd. Nov. 2001 [Online]. Available: at http://odrl.net/1.0/ODRL-10-HTML/ODRL-10.html

[52] C.N. Chong, R. Corin, S. Etalle, P. Hartel, W. Jonker, and Y.W. Law, "LicenseScript: A novel digital rights language and its semantics," in *Proc. 3rd Int. Conf. Web Delivery of Music*, *WEDELMUSIC-03,* Sept. 2003, pp. 122–129.

[53] [Online]. Available: http://www.smartright.org

[54] J. Lotspiech, F. Pestoni, and S. Nusser, "Broadcast encryption's bright future," *IEEE Computer*, vol. 35, no. 8, p. 57–63, Aug. 2002.

[55] IBM response to DVB-CPT cfp for content protection and copy management: xCP cluster Protocol, DVB-CPT-716, Oct. 2001.