Copy Protection System for Digital Home Networks

Jean-Pierre Andreaux, Alain Durand, Teddy Furon, and Eric Diehl

SmartRight introduces renewability and a personal private network to copy protection systems.

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

This article describes the rationale supporting the design of a copy protection system called SmartRight. While carefully presenting our motivations, some light is shed on the very peculiar problems raised by the enforcement of copy protection. Hence, this article also explores less technical but highly important issues such as the legal and commercial aspects.

Context and Birth of the SmartRight Copy Protection System

This section presents the context of copy protection dealing with legal and socioeconomic aspects. This comprehensive picture shows the main actors and their relationships, the rules, and some basic definitions. A brief history of copy protection for DVD emphasizes the lessons from the past initiatives and highlights the pitfalls to avoid.

The Socioeconomic Aspects

In 2001, the creative industries (industries that create products such as theatrical films, TV programs, home video, DVDs, business software, entertainment software, books, and music and sound recordings) contributed more to the U.S. economy and employed more workers than any single manufacturing sector. It represented 5.24% of the U.S. gross domestic product, or US$535 billion and 3.5% of the total U.S. employment, or 4.7 million workers [6]. With the digital age, the artists' creations, in the form of multimedia content, are stored and transmitted with a very high fidelity. This generates new business models. Unfortunately, it also raises an unexpected level of piracy spoiling the creative industries. According to the Recording Industry Association of America (RIAA), the volume of sold audio CDs dropped by 5% in 2001 [7] and by 11% in the first half of 2002 [1]. The Motion Picture Association of America

1053-5888/04/$20.00©2004IEEE

(MPAA) estimates that the movie industry annually looses US$3 billion through physical good piracy [23]. This figure does not include Internet piracy.

This decrease stems from three main threats. The first and greatest danger is the optical disc piracy made on factory production lines and in smaller scale "CD-R labs." The International Federation of the Phonographic Industry (IFPI) estimates that in 2001, 28% of all audio CDs sold were pirated [5]. The creative industry fights against this organized piracy thanks to collaborations with local enforcement bodies and Interpol. In 2001, over 20 million pirate optical discs were seized and 42 manufacturing lines were closed. This is equivalent to the annual U.K. CD audio market. The second threat is the online piracy in the forms of downloadable media, hard goods piracy, streaming media, and online offerings of illegal circumvention devices. By some estimates, more than 350,000 movies are illegally downloaded every day and 99% of online music files are unauthorized. Here again, the creative industry is not weaponless against Internet piracy. For instance, IFPI closed over 1,000 peer-to-peer (P2P) servers and wiped out 700 million unauthorized music files [5].

This article focuses on the third threat: private copy. Copyright laws allow personal backup copies. Unfortunately, people sometimes abuse these legal provisions. Although content providers and consumer electronics (CE) manufacturers launched hand in hand the CD audio in the 1980s and the DVD video in the 1990s, the record button gave birth to a rampant dissension among the creative industries and consumers. Consumers easily duplicate pristine quality content thanks to the digital technology. This was tolerated in the analog age because of the quality loss, but unrestricted duplication becomes an act of piracy in the digital age. While anticopy CD systems proliferate, many consumers resort to the so-called "right to space shifting" (e.g., copying CDs on a portable MP3 reader) or would-be "right to backup" that they intend to exercise in an unlimited and unconditional manner. A recent German survey disclosed that 18% of the consumers admitted that burning CDs resulted in buying less music [5]. However, the way these practices affect the music industry is not clear. Some analysts explain that they ease the spread of the music culture that benefits to the society and finally the creation industries [24].

The Legal Aspect

All copyright systems aim at striking a proper balance between the interests of the authors and the investors and the public interest to promote learning, culture, and development. International treaties and conventions rule this balance through a complex framework invoking copyrights, neighboring rights, and exceptions [2], [3], [8], [9]. Exceptions are situations exempting certain uses from authorization. Each national law defines its range of exception, but most copyright systems recognize the same types either in a restrictive list or through a general provision like fair use in the United States. Some exceptions express fundamental rights like the exception of quotations for criticism or review. Other exceptions cover public interest needs like public libraries. Private reproduction belongs to a third class of exceptions. When introduced, these tolerated acts were insignificantly prejudicial. These tolerances are not rights. For instance, article 6.4 of the European Union Copyright Directive (EUCD) states that private reproduction may be granted "in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the right holders receive fair compensation" [10]. Thus, a copy protection system may enforce the exception of private reproduction for the sake of user friendliness but under the agreement of content provider and with respect of legal provisions.

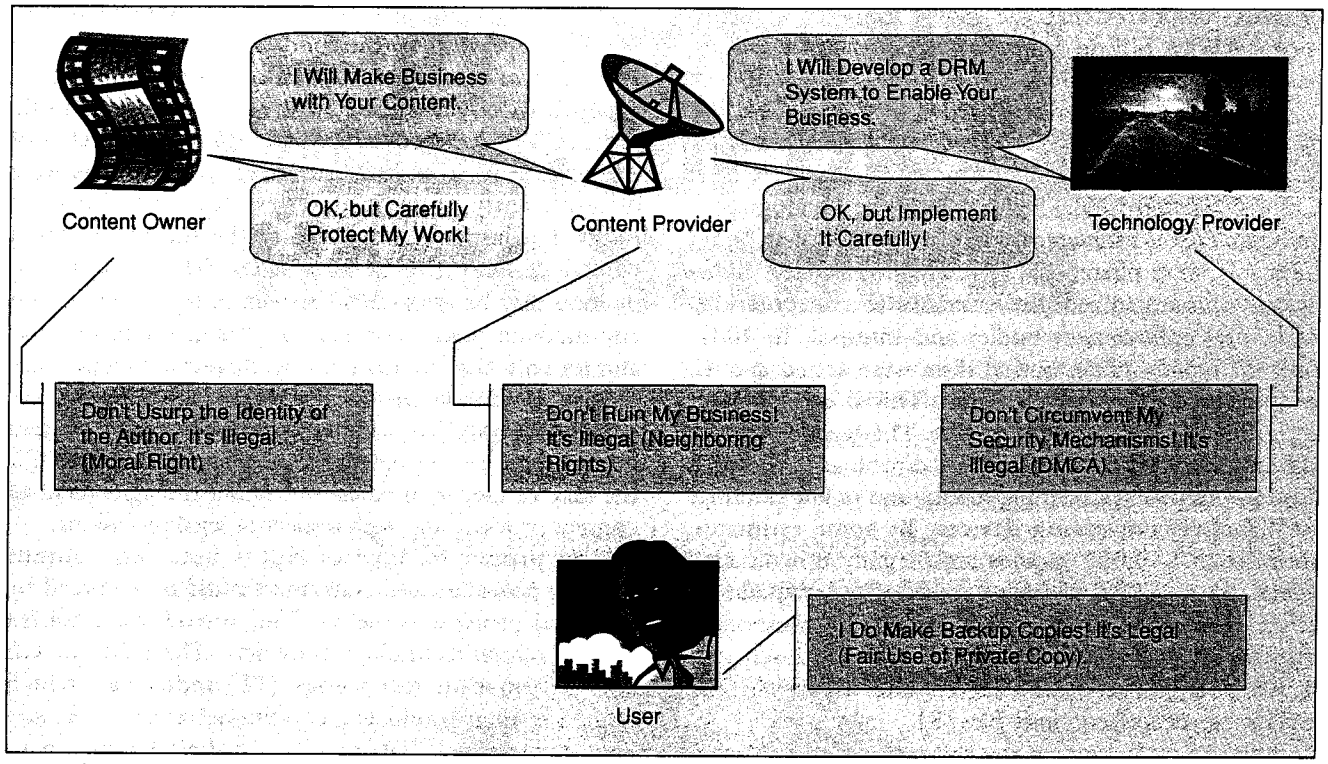
The proper balance of rights between content owners, providers and consumers must be enforced by technical protection means. This introduces a fourth type of actors: technology providers. These are the CE and information technology (IT) industries, which embed in their products a conditional access (CA) system (for instance [19] or [20]), a digital rights management (DRM) system (for instance [21] or [22]) or a copy protection (CP) system. CA or DRM systems enforce various business models defined by content providers. In particular, they implement technical means to guarantee that dishonest users will not tamper the consumption defined by these business models. CP systems only guarantee, if necessary, that no copy (copy never/copy no more) or only one copy (copy once) can be made from protected content. Thus, a CP system does not enforce any business model other than illegal duplication prevention. Figure 1 sketches the actors of the content distribution chain.

CP systems attempt to "keep honest people honest" securing a fair and limited exercise of the "private reproduction" exception tolerated by content owners and providers. It prevents the "ant pirates," i.e., individuals with very limited resources making few illegal copies for friends, relatives, or for themselves. Copy protection does not target organized piracy that will always have the means (money, skills) to circumvent technical barriers. However, security level of CP systems increases to defeat the average skilled hacker class, the so-called garage piracy. Meanwhile, new regulations implementing the WIPO treaty [9] forbid tampering these technical barriers and severely punish violators [10], [4].

Lessons Learnt from the Past: The Example of the DVD

The Beginning of Digital Copy Protection

The launch of DVD video in 1996 raised the need of copy protection. Despite many already existing proprietary solutions, the motion picture (MP), IT, and CE industries created the first large dedicated forum, the so-called Copy Protection Technical Working Group



▲ *1. Balance of rights between the four actors of the content-distribution chain.*

(CPTWG). Its initial target was the security of DVD video. They agreed in November 1996 on the first CP system called the content scrambling system (CSS). Only CSS-compliant devices can play protected content. These devices have to comply with strict implementation rules, so-called compliance rules. The content is encrypted with CSS. The master key, needed to decrypt CSS-encrypted DVD videos, is only delivered to compliant devices. In 1999, a class attack broke the DVD protection system. This attack was possible due to a weak software implementation of CSS. It was then possible to descramble any DVD content. This is still true since the system is not renewable. Three lessons can be drawn from that experience:

▲ security should not only rely on software implementation
▲ breaking one implementation of a CP system should not endanger the other implementations
▲ security system should be renewable.

Toward a Global Copy Protection System

In October 1996, CPTWG decided to study the protection of digital buses (e.g., IEEE 1394 [17], DVI) between two compliant devices. Many link encryption systems were proposed. Two commercial solutions were adapted. Digital transmission content protection (DTCP) secures digital compressed content (February 1998) across the IEEE 1394 interface; high-bandwidth digital content protection (HDCP) secures digital uncompressed content across the DVI (October 1999). An exhaustive list of the CP systems presented during the CPTWG meetings is given in [15].

In 1998, a web of local CP systems ensured copy protection. Each system was specialized in a domain (transmission, storage, etc.). Thomson considered this piecemeal solution inadequate. The inner interoperability induces a huge complexity and is thus expensive. Furthermore, each bridge between CP systems was a potential security hole. Figure 2 illustrates this approach. Thomson proposed a global CP system as sketched in Figure 3. The main idea was to extend the security already brought by the conditional access systems to the home network. This system was called XCA (eXtended Conditional Access). It is the ancestor of SmartRight.

SmartRight Overview

This section describes the architecture of SmartRight. (SmartRight is designed by Thomson, with the help of world-class technology partners: Axalto, Canal+ Technologies, Gemplus, Micronas, Nagravision, Panasonic, Pioneer, SCM Microsystems, ST Microelectronics.) First, it provides the main requirements and features. Then, it describes the architecture and the technical solutions. Some use cases and business models illustrate the operation of the SmartRight system.

Main Features

End-to-End Protection

SmartRight's philosophy prevents any break in the chain of content protection. To that end, digital content is kept scrambled as required throughout the home network during storage or transmission from one

device to another. Digital content is only descrambled by a rendering device such as a TV set.

Universality

SmartRight makes no assumption on the format of the content to protect. It accepts content from any kind of digital source, including free-to-air broadcast and prerecorded content.

Interoperability

SmartRight is complementary to current CA and DRM systems. It defines an API with them. Moreover, to ensure interoperability, it defines a common syntax for SmartRight content. SmartRight supports any current and future bidirectional digital bus, such as IEEE 1394 [17] or IEEE 802.11 [18]. SmartRight's end-to-end protection may coexist and interoperate with all currently existing CP systems. To that end, importation and exportation rules have been defined between the SmartRight system and other coexisting content protection systems on the same digital home network, to translate the rules associated with the content.

Renewability

History shows that any security system is breakable. Perfect security does not exist [16]. Renewal of the security is therefore mandatory for any serious design. Thus, SmartRight uses renewable security modules. CE devices will be equipped with removable modules such as smart cards.

Personal Private Network

SmartRight introduces the innovative concept of personal private network (PPN). A PPN is the set of devices owned by a given person or household. A PPN encompasses multiple homes and mobile devices. Consequently, a user can access his contents from any device belonging to his PPN. Nevertheless, to ensure the protection of rights associated with the content, a SmartRight device belongs to only one PPN at a given time, and two different PPNs cannot interoperate. The number of rendering devices within a same PPN is limited. The absence of such limitation would actually allow a unique, global PPN within a building block, a small town, or even the Internet.

Business Model Enabler

SmartRight facilitates the creation of a wide range of innovative business models, including any time- or event-related business model that may be supported by the digital devices connected to a PPN. SmartRight provides a secure environment for the consumption of content in accordance with such business models. All content usage rules are determined and managed by the CA and DRM systems that deliver content to the home network.

Architecture

Environment

Figure 3 shows the environment of the SmartRight system. There are two domains of protection:

▲ in the first domain (on the left side), prerecorded content encryption, CA systems, or DRM systems protect content during delivery to the home

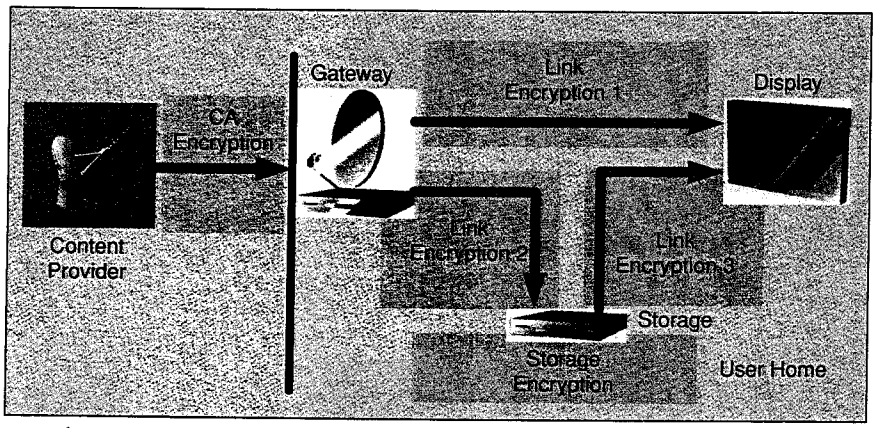
▲ in the second domain (on the right side), the SmartRight system protects content after it enters the home and until it is rendered or exported.

Devices

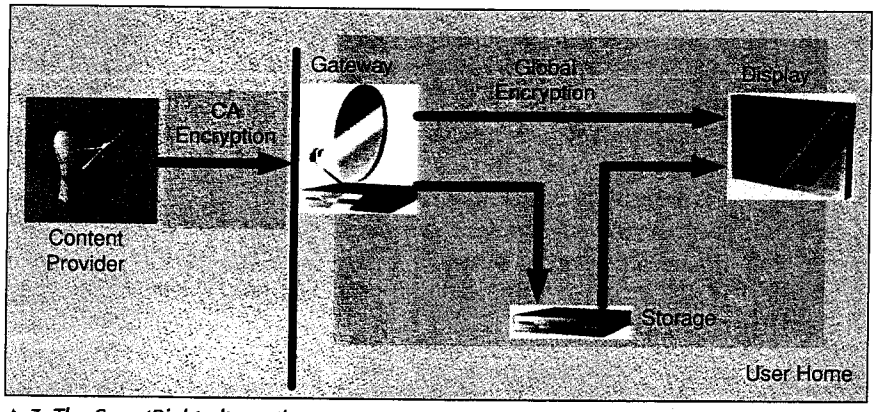
SmartRight-enabled devices may play three roles:

▲ *Acquisition role*—the device is a gateway for protected content coming from outside of the home network. Distribution means include broadcast, broadband, prerecorded media, or proprietary DRM systems. Set-Top Box may be such a device.

▲ *Presentation role*—the device renders SmartRight protected content or exports content to proprietary CP systems. Digital television may be such a device.



▲ 2. *The piecemeal approach.*



▲ 3. *The SmartRight alternative.*

▲ *Storage role*—the device records content carried over the home network. Since protected content is scrambled, it remains protected in storage. Any storage unit may be such a device.

SmartRight-enabled devices may combine several roles, such as acquisition and presentation roles (e.g., an integrated digital TV), or as storage and acquisition roles (e.g., a set top box with embedded personal video recorder).

Cards

To ensure high-level protection and renewable security, SmartRight uses removable hardware tamper-proof cards. Theses cards hold keys and perform secure cryptographic processing. The card associated with the access role is called the converter card. The card associated with the presentation role is called the terminal card.

SmartRight Use Cases

Every piece of content entering the SmartRight PPN is associated with one scenario. The three possibilities are view only, private copy, and copy free.

▲ Usage rules for view-only content
- –content can be rendered after it is delivered to the PPN
- –content cannot be rendered if it has been stored in the PPN or in a different PPN.

▲ Usage rules for private-copy content
- –content can be rendered after it is delivered to the PPN, or if it has been stored in the PPN
- –content cannot be rendered in a different PPN.

▲ Usage rules for copy-free content
- –content can be rendered after it is delivered to the PPN, or if it has been stored in the PPN, or in a different PPN.

Business Models Based on SmartRight

CA and DRM systems use view only and private copy to enforce their business rules. One example, the "Pay twice and keep it" model, will illustrate it.

Pay Twice Then Keep It

In this model, the broadcaster presents at least two offers:

▲ the "basic" offer: the customer pays for accessing content once without being able to record it

▲ the "premium" offer: the customer pays for accessing content program and will be able to record it after the second purchase.

If the customer buys content with the basic offer, then the content will be view only.

If the customer buys content with the premium offer, then the content will be view only for the first access, and private copy for the second access.

SmartRight in Detail

This section details the management of the PPN. The management complies with the following user-friendliness and CP requirements.

▲ User-friendliness requirements
- –*No master device:* the PPN management shall be distributed so that the user does not need to buy and maintain a dedicated device to run it.
- –*Support for untethered clusters:* untethered clusters belonging to one person or family (main household, summer home, . . .) shall belong to the same PPN.
- –*Install and play:* the installation of a device on a PPN shall be fully transparent to the user.
- –*No remote authority:* the PPN management shall not require the presence of a return channel to a remote authority.
- –*User privacy:* no personal information about the customer or content accessed shall leak.

Some features were given up because they raise conflicts with CP requirements. For instance, if lending a piece of content to a relative is still possible, the way to do it is not user friendly.

▲ CP requirements
- –*PPN control:* PPN management shall prevent devices from belonging to several PPNs or shall prevent PPN interconnections. Furthermore, it shall restrict the PPN size.
- –*Private-copy enforcement within a PPN:* private-content from a PPN shall not be consumable in any other PPN.
- –*View-only enforcement within a PPN:* recorded view-only content shall not be played back.
- –*End-to-end protection:* content shall be descrambled only when needed, i.e., in the presentation device.

PPN Management

Removable secure cards manage the PPN. All terminal cards belonging to the same PPN share a secret key named network key (K_N). This section describes this key management scheme.

Transition Between Virgin, Progenitor, and Sterile Terminal Cards States (Figure 4)

A SmartRight terminal card may have three states. A terminal card that holds no network key (i.e., it is not yet installed on a PPN) is called a virgin. A terminal card that holds one network key (a terminal card knows at most one network key) is able to transmit its network key to a virgin terminal card (during its installation on the PPN), and it is called a progenitor. Finally, a terminal card that holds one network key is called a sterile. A sterile cannot transmit its network key. The user may reinitialize a progenitor or a sterile terminal card: the card becomes virgin, and its network key is erased.

Handling of the Current Network Size

A SmartRight PPN can have at most one progenitor terminal card. This terminal card determines the network size. Before transmitting the network key to a virgin terminal card, the progenitor decrements the current network size. When a terminal card leaves a PPN, the current network size is incremented.

Terminal Card Modes

Each terminal card "connected" to a same PPN cluster has three possible modes:

▲ operational mode: the device performs content management operations

▲ blocked mode: the device does not perform any content management operations

▲ key distribution mode: the device performs PPN management operations and may perform content management operations at the same time. Figure 5 depicts protocols and operations running during this mode.

Key Distribution Overview

For the sake of convenience, the terms virgin, progenitor, and sterile will refer, respectively, to virgin terminal cards, progenitor terminal cards, and sterile terminal cards.

Each time a device is connected to a PPN cluster or switched on, all the cards of that PPN cluster enter the key distribution mode. Each time a card is inserted in a connected device, all the cards of that PPN cluster enter the key distribution mode. The cards first exchange messages to identify the state of the other terminal cards as follows.

If there is at least one progenitor (scenario 1), each terminal card checks that there is only one present progenitor and that every sterile (if any) belongs to the same PPN as the progenitor. If not, they enter the blocked mode. Else, sterile cards enter the operational mode. The progenitor checks if there are some virgins present. If not, or if the maximal network size is reached, it enters operational mode (and virgins, if any, stop). If there is at least one virgin, the progenitor updates the current network size, becomes sterile and transmits the network key and the current network size to one of the virgin cards. This virgin card becomes progenitor and launches a new key distribution protocol. The eventual remaining virgin cards enter blocked mode. Network key transfer is secured using usual public key infrastructure techniques based on a root authority.

If there is no progenitor but at least one sterile (scenario 2), all virgins enter blocked mode. Their installation fails. Sterile cards check that they all belong to the same PPN. If so, they enter operational mode; else, they enter blocked mode.

If there are only virgins (scenario 3), a new PPN is created once the user is confirmed. A progenitor is chosen among the present virgin cards. The other virgin cards enter blocked mode. The progenitor picks, at random, the network key and sets the current network size to the maximum network size. A new key distribution protocol is then launched.

Some additional protocols are defined as well to reinitialize progenitor or sterile and to enable the mobility (among the PPN terminal cards) of the progenitor state.

Access devices and associated converter cards do not know the network key. SmartRight design actually respects the public key paradigm where the secret needs to be only in the decryption place. Access devices deliver content to the PPN. They only need to know encryption keys. Recording devices never know the network key. They are pure bit-buckets. Neither access devices nor recording devices are counted in the network size.

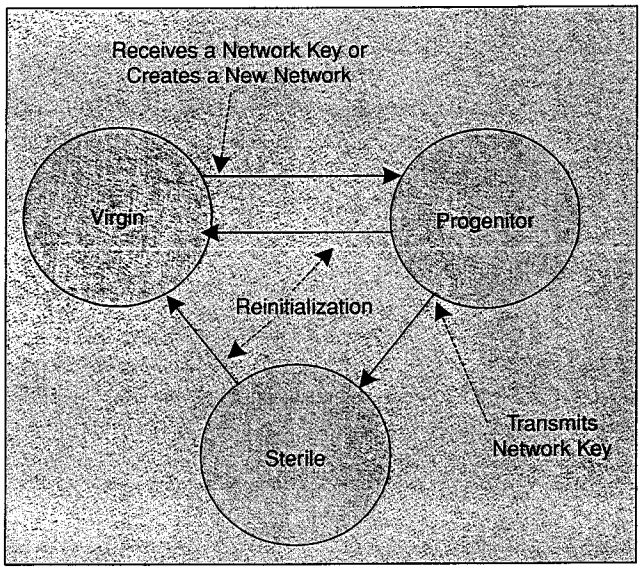
Content Management

Access devices convert proprietary-protected content into SmartRight-protected content. The access device replaces the licenses associated with the content, for instance a CA entitlement control message, with a SmartRight License called LECM (local enforcement copy management). If the content is not scrambled using a regular scrambling algorithm (triple DES in the United States and DVB-CSA in Europe), it is descrambled (if needed) and rescrambled using the control words generated by the converter card.

Handling of the LECM in the Converter Card

The converter card builds the LECM. It embeds information about the content protection (usage rules, authorization to export the content to another domain, etc., and the control words needed to descramble the content. LECM integrity is fully ensured for private-copy and view-only content. LECM confidentiality is partially guaranteed for private-copy and view-only content. In these cases, control words and other secret information are encrypted while usage rules remain in the clear.

The converter card randomly chooses a secret key called LECM key (K_L). This key encrypts the confidential part of the LECM. The clear part of the LECM includes the encryption of K_L by K_N [we will write $E\{K_N\}(K_L)$]. Hence, any terminal card belonging to the right PPN will be able to recover K_L since it knows K_N, as explained below. It will then be able to decrypt the confidential part of the LECM. To ensure integrity, a digest of the LECM computed before the encryption of the confidential part is appended. Alteration of LECM is thus not possible.



▲ *4. State transitions of terminal card.*

Handling of the LECM Key

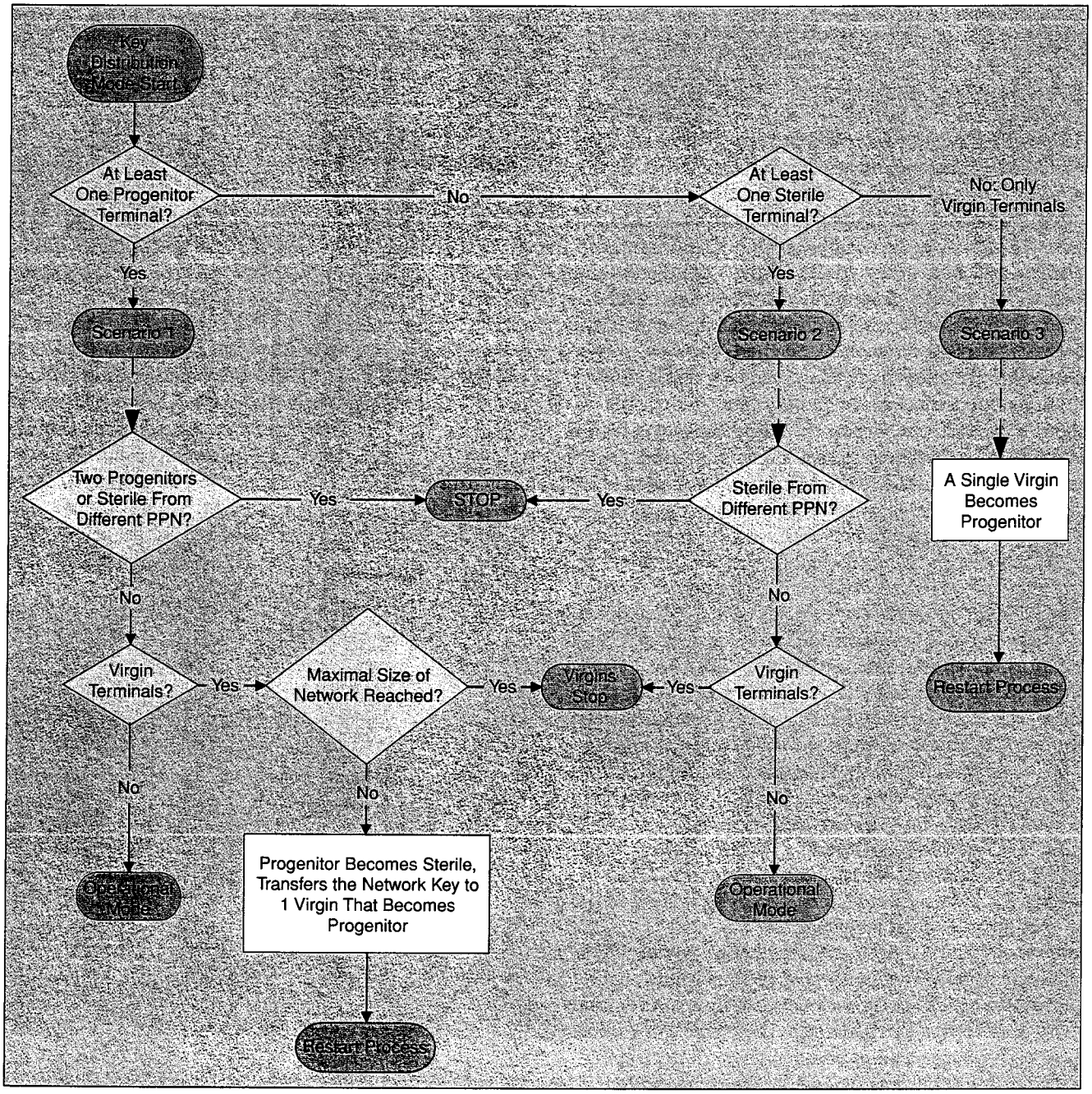
A converter card computes $E\{K_N\}(K_L)$ using public key cryptography techniques. During the key distribution mode, it obtains the certificate of one terminal card from the PPN. It then picks at random K_L, encrypts it using terminal card public key, and sends the result to the terminal card. The latter retrieves K_L using the terminal private key. It reencrypts K_L using K_N and sends back the result to the converter card. This allows the converter card knowing K_N and $E\{K_N\}(K_L)$ without having K_N.

Handling of the LECM in the Terminal Card

▲ *Copy free:* The control word is not encrypted. Thus, content can be descrambled in any PPN.

▲ *Private copy:* The confidential part of the LECM (encrypted by K_L) contains the control word while the clear part contains $E\{K_N\}(K_L)$. Thus, any terminal card from the relevant PPN will be able to recover the control word and then the content. Terminal cards from other PPN will not be able to access the control word. Stored content can be played at any time since LECM includes all information the terminal card needs to access the control word. This is how SmartRight enforces private-copy usage rule.

▲ *View only:* The converter card picks at random two additional specific keys. The first one, K_C, super encrypts the control word. The result of that super encryption together with the second key K_A constitutes the LECM



▲ *5. Key distribution protocol.*

confidential part. When the terminal card decrypts this confidential part, it recovers K_A and the super encrypted control word. It then picks at random a challenge and sends it to the converter card. The converter card computes a digest of that challenge using key K_A. It sends back the result together with key K_C. The terminal card checks the digest. If it is correct, the terminal card recovers the plain control word using key K_C. The converter card then erases K_A and K_C. If the user tries to store the content, when playing it back, the terminal card will choose and send a new challenge. Neither the converter card (that has already erased K_A) nor the storage unit (that never knew K_A) can compute the right digest. The terminal card will thus refuse to play the content even if it receives the correct K_C (recorded by the user). The knowledge of K_C without the network key is useless to recover the control word. Sending K_C in the clear does not thus open any security hole.

The converter card handle more elaborate business models by delaying the erasure of K_A and K_C. For instance, erasing the keys half an hour after the end of the content allows a half-hour time shifting. During the allowed time-shifting window, the converter card can answer the challenge. For a play-twice content, the erasure will only be made after the second play.

Analog Hole Handling

This section focuses on the use of watermarking in CP systems and, in particular, its integration in SmartRight. It does not detail the watermarking technique itself.

SmartRight enforces usage rules and manages devices in the PPN with highly secure cryptographic protocols. The weakest link of the delivery chain is now the analog link. Video has to be rendered on a display. Audio has to be spoken by loud speakers. Pirates, as dishonest users, can play content, record the resulting analog signal, digitize it, and distribute the pirated files. This threat is called the analog hole. SmartRight aims at preventing the pirated content from coming back in a compliant network. There is actually no way to preclude the playback outside SmartRight domain.

The current technical answer is watermarking. The watermark signal carries data, hereafter called the payload, invisibly embedded in multimedia content, that can survive the analog to digital conversion. At the playback, this information may allow detection of illegally recorded contents. The problem for CP experts is the integration of the watermarking primitive in the global system architecture. The typical issues are what information the payload represents, when content is watermarked, and in which device the watermark is decoded [26]. An example of a video watermarking technique dedicated to copy protection is found in article [27].

In many approaches (e.g., Analog Reconversion Discussion Group), the payload describes the kind of content, i.e., the usage rules associated with its consumption. Videos are watermarked at the content source, and the payload is decoded by consumer devices. This approach brings severe drawbacks when mapped to advanced business models. For instance, recording devices have to change the watermark signal to differentiate between the original material such as "copy once" and its copy labeled "copy no more." A second pitfall is that, assuming use cases mentioned earlier, servers must have two different versions of each piece of content with the information "view only" or "private copy" embedded in. Customers of the basic offer receive the first version whereas the second version is delivered to the customers of the premium offer.

The key idea underlying the integration of the watermarking primitive in the SmartRight system is that there is no need to embed information related to content, as its management is already perfectly tackled by the above-mentioned cryptographic protocols. The only needed information is the presence of a watermark signal. Hence, the payload is null. Protected content is watermarked and scrambled. A piece of content that would be in the clear and watermarked would necessarily be illegal. Display devices check this condition before rendering digital content.

The trust model of other approaches expects that all devices comply with good behavior. This requires security functionality to the gateway rendering and recording devices. Unfortunately, this assumption is wrong when dealing with noncompliant recording devices. In SmartRight approach, detection only occurs at rendering and the system makes no assumption regarding the receivers and recording devices. This reduces the number of security requirements renders SmartRight trust model simpler.

Another drawback of other approaches is the management of the payload. First, decoding embedded bits is more complex than detecting the presence of a watermark signal. Moreover, embedding watermark is restricted to production. Protected content is watermarked in the studio whatever its consumption rules are. Only display devices implement the detection functionality. Second, there is a tradeoff between nonperceptibility, payload, and robustness [25]. Thus, reducing payload to the minimum guarantees a better resistance to any malicious attack against the watermark technology itself. For instance, asymmetric watermarking techniques [13] and the JANIS method [14] have shown higher security levels than the classical spread spectrum watermarking method.

Conclusion

With the advent of the digital age, copy protection becomes a major issue for all the actors of the video chain. Copy protection is necessary to protect content owner rights. But copy protection must also respect consumers rights. The SmartRight system replaces current piecemeal solutions by a global solution that protects the entire home network. This approach introduces two new features of a copy protection system: renewability and PPN. Renewability provides an active defense against

inevitable hacks. This feature should be an asset for content owners and manufacturers. PPNs allow consumers' private use similar to analog age without the risk of mass uncontrolled distribution. This feature should be an asset for consumers. Furthermore, this article presented an original key management scheme. This scheme based on the concepts of virgin, progenitor, and sterile allows a limited number of principals to securely share a common secret key without the need of a central authority. This security scheme may be useful in secure networking.

Jean-Pierre Andreaux received his DEA in applied mathematics from the University of Limoges in 1996. He is now working on cryptographic protocols and algorithms with Thomson Corporate Research in France. His research interests are primarily in the area of copy protection and security of home networks.

Alain Durand graduated from Ecole Nationale Supérieure de Techniques Avancées (ENSTA) in 1995. He received his DEA in computer science from the University of Paris VII that same year. From 1997 to 1999, he worked in Oberthur Smart Cards as a cryptography implementer. He then joined the security laboratory of Thomson Corporate Research in France. His research interests are mainly content protection and secure protocols.

Teddy Furon graduated from Ecole Nationale Supérieure des Télécommunications in Digital Communication engineering in 1998. He received his Ph.D. degree in 2002. From 1998 to 2001, he worked in the security laboratory of Thomson Corporate Research. From 2001 to 2002, he was a postdoctoral fellow at the Université catholique de Louvain-la neuve. He is the inventor of the JANIS watermarking technique. He is currently a researcher at the TEMICS project in Institut National de Recherche en Informatique et Automatique (INRIA). His research interests are in the area of watermarking, especially detection, use of side information, and security analysis through signal processing techniques. He cochaired special sessions on watermarking at IEEE MMSP 2001 workshop and at EUSIP CO 2002 conference.

Eric Diehl graduated from Ecole Nationale Supérieure d'Electronique et Radio-électricité de Grenoble (ENSERG) in 1985. In 1987, he joined LEREA, a subsidiary of Thomson. He worked on CDI, pay TV, home networking, user interface and security. Since 1999, he has been leading the security laboratory of Thomson Corporate Research. The current primary interest of this team is content protection, and security of networks. He filed more than 60 patents in the fields of security, pay TV, and user interface.

References

[1] Market data pages of the Web site [Online]. Available: http://www.riaa.org

[2] Geneva Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms, 6 Sept. 1952. Available: http://www.ifpi.org/site-content/legal/treaties.html

[3] Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations, 26 Oct. 1961. Available: http://www.ifpi.org/site-content/legal/treaties.html

[4] Digital Millennium Copyright Act, Oct. 1998 [Online]. Available: www.loc.gov/copyright/ legislation/dmca.pdf

[5] IFPI Piracy Report, June 2002 [Online]. Available: http://www.ifpi.org/site-content/antipiracy/ piracy2002.html

[6] S.E. Siwek, *Copyright Industries in the U.S. Economy: The 2002 Report.* Apr. 2002. Available: http://www.iipa.com/copyright_us_economy.html

[7] IFPI, World Sales 2001 [Online]. Available: http://www.ifpi.org/site-content/statistics/worldsales.html

[8] Agreement on trade-related aspects of intellectual property rights (TRIP), Apr. 1994.

[9] WIPO Copyright Treaty and Performances and Phonograms Treaty, Dec. 1996.

[10] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001, Official Journal L 167, pp. 10–19 [Online] Available: http://eucd.info/directive-2001-29-ce.pdf

[11] Digital transmission content protection white paper [Online]. Available: http://www.dtcp.com/data/wp_spec.pdf

[12] High-bandwidth digital content protection [Online]. Available: http://www.digital-cp.com/data/HDCP10.pdf

[13] T. Furon and P. Duhamel, "An asymmetric watermarking method," *IEEE Trans. Signal Processing*, vol. 51, pp. 981–995, Apr. 2003.

[14] T. Furon, "Watermarking for copy protection," Ph.D. dissertation, ENST Paris, Mar. 2002.

[15] A. Eskicioglu, J. Town, and E. Delp, "Security of digital entertainment content from creation to consumption," *Signal Processing: Image Commun.*, vol. 18, pp. 237–262, 2003.

[16] D. Kahn, The Codebreakers, *The Comprehensive History of Secret Communications from Ancient Times to the Internet*, 2nd ed. New York: Scribner, 1996.

[17] *Digital Interface for Consumer audio/video equipment—Part 1: General.* CEI/IEC 61883-1, 1998.

[18] *Wireless LAN Medium Access Control and Physical Layer Specifications.* ISO/IEC 8802-11, 1999.

[19] Nagravision CA system [Online]. Available: http://www.nagravision.com/ pdf/ ConditionalAccess.pdf

[20] NDS Videoguard [Online]. Available: http://www.nds.com/conditional_access/ conditional_access.html

[21] Intertrust DRM [Online]. Available: http://www.intertrust.com/main/ technology/ index.html

[22] Microsoft Windows Media DRM System Version 7 available at http://msdn.microsoft.com/msdnmag/issues/01/12/DRM/default.aspx

[23] J. Valenti, Piracy Treathens to Destroy Movie Industry ans U.S. Economy, In testimony before the Senate Foreign Relations Committee, Feb. 12, 2002 [Online]. Avialable: http://www.mpaa.org/jack/2002/ 2002_02_12a.htm

[24] M. Alberganti, "CD et DVD: les vertus du piratage privé," *Le Monde,* p. 17, 23 Jan. 2003.

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

[26] J.A. Bloom, I.J. Cox, T. Kalker, J.-P. Linnartz, M.L. Miller, and C.B.S. Traw, "Copy protection for DVD video," *Proc. IEEE,* vol. 87, pp. 1267–1276, July 1999.

[27] M. Maes, T. Kalker, J.-P. Linnartz, J. Talstra, G. Depovere, and J. Haitsma, "Digital watermarking for DVD video copy protection," *IEEE Signal Processing Mag.*, vol. 17, pp. 47–57, Sept. 2000.