Digital Content Protection LSI for PC-Based Digital TV Receivers

● Kiyoshi Kohiyama ● Hiroyuki Fujiyama ● Toshiyuki Yoshitake

(Manuscript received October 3, 2005)

This paper describes a "digital content protection LSI" that prevents the hacking of PC-based digital TV receivers. Given the wide public knowledge about PC architecture, crackers may gain unauthorized access to PC software. Consequently, many broadcasters and other content holders are concerned that digital broadcast content may be stolen. This situation has curtailed the development of PC-based digital TV receivers for some time. Therefore, we have designed a protection scheme whereby content is protected even in open architecture environments such as the PC environment. This protection has been implemented in the form of a digital content protection LSI. These LSIs will open the way for the continued development of PC-based digital TV receivers.

1. Introduction

PC-type analog TV receivers are common in the homes of many users. A large percentage of desktop PCs have TV tuner boards so that people can capture analog broadcasts, store the content on PC hard disks, and then view the broadcasts later.

However, recent years have witnessed a significant increase in digital broadcasting. Some countries such as Japan have already set dates by which to replace conventional analog broadcasts with digital ones. Thus, analog broadcasts will eventually be phased out, with frequencies previously allotted to analog broadcasting being reallocated to cellular phones and other applications.

Consequently, the majority of PC-type receivers are expected to support digital broadcasting in the near future. There is a major problem, however, posed by crackers. The digital content stored on a PC hard disk is vulnerable to hacking and may be distributed over the Internet. For digital broadcasting, this situation represents a major risk because, unlike analog content, digital content can be copied with no deterioration in quality. Content providers, broadcasters, and other sources of content are becoming increasingly concerned about this risk and a solution is urgently needed.

This paper details the development of a "digital content protection LSI" that addresses this problem for the Japanese market. This chip can be utilized to comply with the "robustness rules" on content protection prescribed by the Association of Radio Industries and Businesses (ARIB)[1),2)] which is a standardization organization that includes most of Japan's major broadcasters and manufacturers.

The chip was used in a Fujitsu desktop PC (model FMV-TX90LD) released in April 2005. This chip enabled Japanese PC customers to store and view high-definition TV (HDTV) digital broadcasts for the first time. Previous PCs could receive HDTV digital broadcasts, but picture quality was downgraded to the standard definition TV (SDTV) level in order to comply with the robustness rules

set forth by ARIB.

2. Current problems

Figure 1 shows a block diagram of a typical PC-type digital broadcast receiver. Digital content is broadcast using the compression algorithm of the Moving Picture Experts Group (MPEG). Upon reception, content is stored on a HDD in encrypted format. This encryption basically protects the content. However, to view the content, it must be decrypted, decompressed, and subject to post processing for the best viewing experience. Moreover, this decryption, decompression, and post processing should be done in a "secure environment" that is safe from crackers. The problem is how to realize such an environment.

2.1 Realizing a secure environment in hardware

It is possible to achieve a secure environment by using hardwired logic circuits integrated on LSIs. It is most difficult or virtually impossible for typical crackers to analyze and alter LSIs, and then steal content. Thus, this offers a very secure solution. Conversely, this approach is very costly since dedicated LSIs are needed.

PCs are basically software-oriented products that can do almost anything, given the appropriate software. Therefore, using dedicated LSIs runs counter to this concept, thus negating a major PC advantage.

2.2 Realizing a secure environment in software

A large part of PC architecture is part of the public domain. Open publications have allowed third parties to develop thousands of software applications, thus transforming the PC into an all-purpose product that can do virtually anything.

Conversely, software runs in the PC memory area for which access is basically public knowledge. As a result, crackers may illegally access memory areas that are allocated to other users.

More specifically in the case of the typical PC-type digital broadcast receiver shown in Figure 1, the software used to decrypt, decompress and post process digital content resides in the PC memory area. Consequently, crackers could 1) access that area, 2) analyze the original software code, and 3) corrupt the code so that decrypted content is dumped onto the HDD, for example. Such activities must be prevented by all means.

A standard method of providing protection against such activities is obfuscation.[3] This refers to making the program code so confusing that it is difficult to interpret and analyze. Since analyzing program code is the first step in creat-

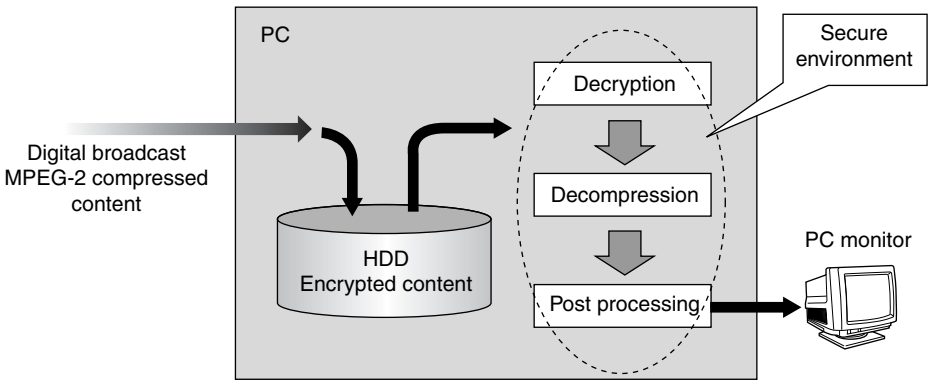

Figure 1
Block diagram of typical PC-type digital broadcast receiver.

ing cracker programs, obfuscated program code can help to achieve a secure environment. However, there is no known, totally reliable way to obfuscate program code at present. Thus, through persistent efforts, crackers could succeed in analyzing an obfuscated program.

To summarize, the hardware solution is very expensive and the software solution fails to provide a sufficient degree of security.

3. Realizing a secure environment through a software/hardware hybrid solution

To address the cracker problem described above, we developed a software/hardware hybrid solution that combines hardware-level security with software-level cost effectiveness. **Figure 2** shows a block diagram of a PC-type digital broadcast receiver protected against crackers by hardware, that is, the digital content protection LSI.

There are two main points regarding the hybrid software/hardware solution.

The first main point is that the functions used to ensure content security are only implemented in hardware. Conversely, most content processing functions, such as the decryption, decompression, and post processing of digital content, are implemented in software. As a result, the hardware circuitry was minimized, resulting in a solution that combines hardware-level security with software-level cost effectiveness.

The second main point is that hardware controls the flow of content. If the hardware detects any tampering of the software, it can stop the flow of content regardless of the software's operation. To do this, the hardware first encrypts all content stored on the HDD using a randomly generated key. This gives the hardware control over content. Then the hardware checks the software on a real-time basis. If any suspicious activity is detected, the hardware stops the flow of content.

4. Characteristics of digital content protection LSI

Table 1 lists the basic specifications of the digital content protection LSI. **Figure 3** shows a block diagram of the hardware that ensures content security, including an encryption/decryption circuit, a 32-bit RISC microprocessor core, and various peripherals. The microprocessor uses external Synchronous Dynamic Random Access Memory (SDRAM) and flash memory as program and data memory areas. Microprocessor software monitors related software running on the PC on a

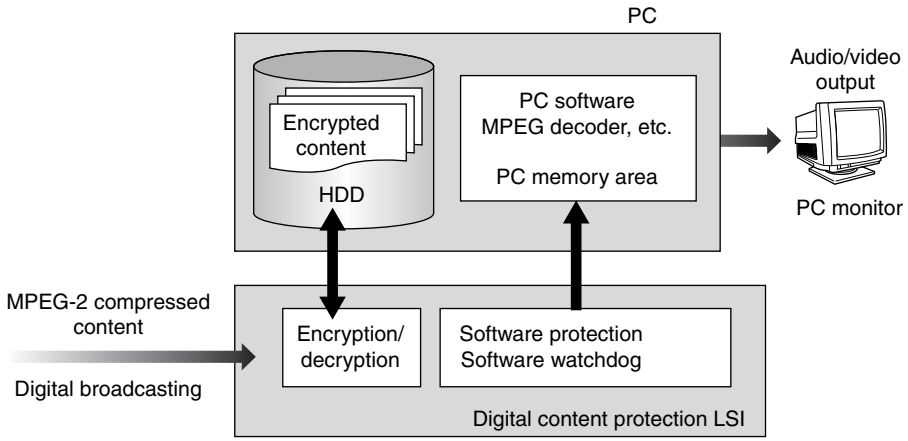

Figure 2
PC protected against crackers by digital content protection LSI.

Table 1
Basic specifications of digital content protection LSI.

Technology	0.18-µm CMOS AL5 Layer
Package	FBGA-288
Power supply	VDDI (for internal circuitry) 1.65 V to 1.95 V VDDE (for I/O) 3.00 V to 3.60 V
Microprocessor	32-bit RISC processor

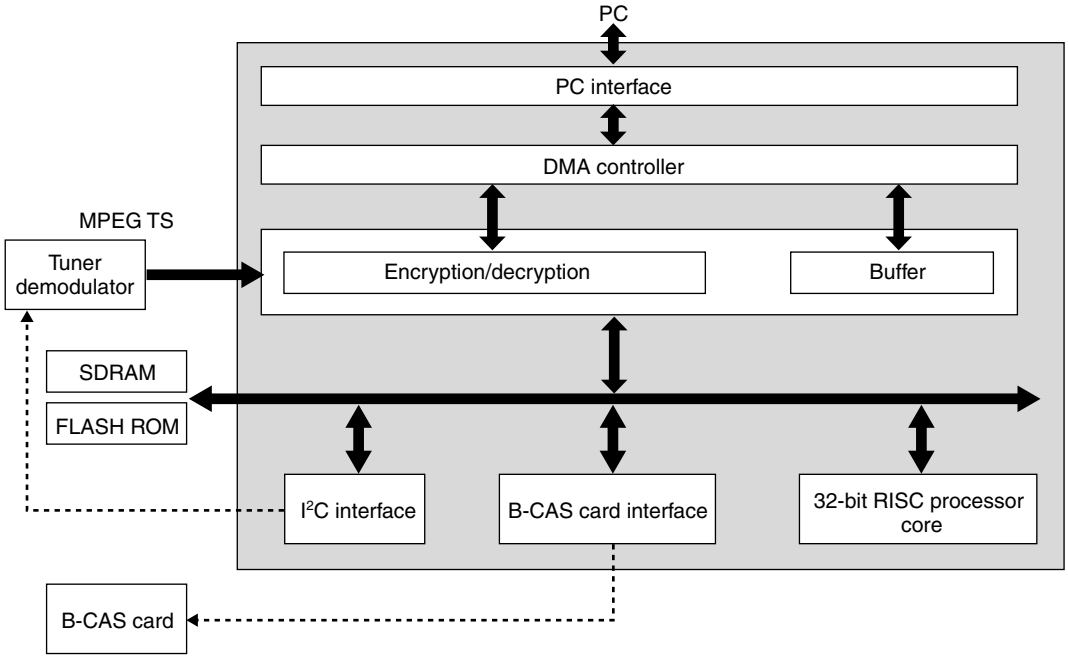

Figure 3
Block diagram of digital content protection LSI.

real-time basis. Therefore, the detection of any software tampering stops the flow of content. This monitoring and other functions ensure content security.

The following describes some of the circuits on the chip.

4.1 Encryption/decryption circuit

The encryption/decryption circuit contains MULTI2 decryption circuitry to decrypt MPEG-2 broadcast content. The decryption key (called the scrambling key) is contained on the Broadcasting Satellite Conditional Access Systems (B-CAS) card and transmitted to the digital content protection LSI via the IC card interface. The scrambling key is updated every few seconds. In effect, the microprocessor requests a new key each time from the B-CAS card.

The encryption/decryption circuit also includes encryption/decryption circuitry for local encryption. Locally encrypted content is stored on the HDD via the local bus interface.

Encrypted content stored on the HDD is used for viewing. Content on the HDD or local bus is always encrypted. This is necessary in order to comply with the robustness rules established by ARIB.

4.2 HDD functions

Various features are realized using the content stored on the HDD. For example, time shifting is realized by storing content on the HDD

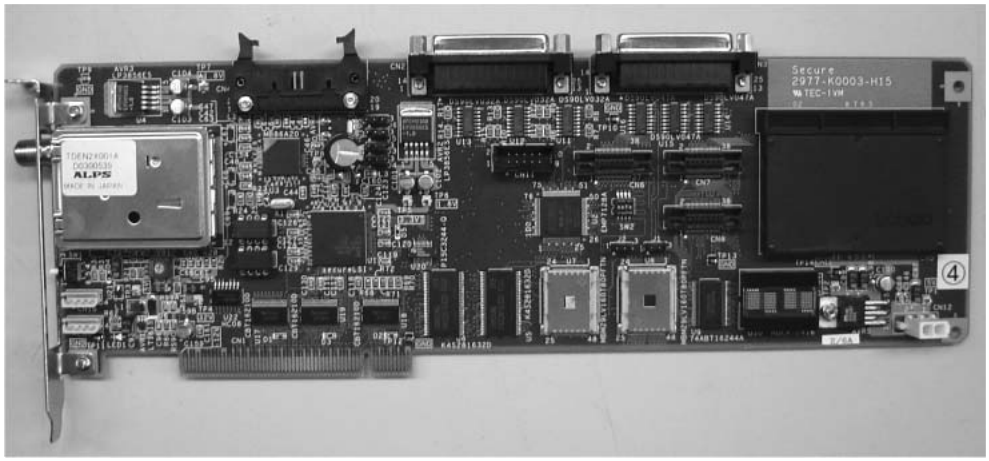

Figure 4
Experimental board.

and reading it out at a convenient time. This function is very convenient for busy people; for example, they can record the 8 o'clock evening news for later viewing when they return home at 12 o'clock. For this purpose, it is sometimes necessary to store and read HDD content simultaneously. Our LSI supports this capability. Also included are functions to achieve such trick play operations as fast forwarding and rewinding.

4.3 Peripherals

The LSI has basically all the peripheral interfaces necessary to realize a digital TV.

The I^2C interface was included to control external circuits such as for tuners and demodulator LSIs. The IC card interface was included to receive "scrambling keys" from the B-CAS card as previously described.

5. Experimental board

Figure 4 shows a photograph of the experimental board that we developed and **Figure 5** shows a photograph of the digital content protection LSI. This board was used to test functions in a PC environment. It has all the functions necessary to receive Japanese terrestrial digital broadcasts. The board includes a tuner to receive digital terrestrial broadcasts, an Orthogonal

Size: 18 mm × 18 mm

Figure 5
Photograph of chip.

Frequency Division Multiplexing (OFDM) demodulator LSI, a B-CAS card, SDRAM, and flash memory. The board interfaces with the PC through the PC bus. Moreover, application software for receiving digital broadcasts was developed for use on PCs. This includes the decryption, decompression, and post-processing functions shown in Figure 1. As a result, MPEG-ML@HL streams can be decoded in real time.

6. Conclusion

This paper presented the characteristics of a digital content protection LSI that can be used to protect broadcast digital content against crackers in the PC environment. By using these LSIs, it is possible to develop PCs that comply with the robustness rules on content protection prescribed by ARIB. Moreover, these LSIs have been used in the first PC to store and view HDTV digital broadcasts in Japan.

In the future we expect a variety of applications for this LSI. For example, the content protection function could be used to receive content over the Internet in a secure manner. Adapting this LSI for US or European digital broadcasting is also a possibility. For the time being, the LSI is utilized in the Windows OS environment, but could also be used in Linux systems as well. The LSI has many other applications, for example, it can be used to securely transfer content between PCs.

References

1) ARIB TR-B14. (in Japanese), Association of Radio Industries and Businesses, 2005.
2) ARIB STD-B25. (in Japanese), Association of Radio Industries and Businesses, 2003.
3) C. Collberg et al.: A Taxonomy of Obfuscating Transformations. Technical Report #148, Department of Computer Science, The University of Auckland, 1997.

Kiyoshi Kohiyama, *Fujitsu Laboratories Ltd.*
Mr. Kohiyama received the B.S. degree in Electronic Engineering from Keio University, Kawasaki, Japan in 1977. He joined Fujitsu Ltd. in 1977, where he had been engaged in research and development of TV signal processing LSIs. In 1993 he joined Fujitsu Laboratories Ltd. He received the Oyama Matsujiro Award from the Promotion Foundation for Electrical Science and Engineering in 1992 and the Development of Technical Promotion Award from the Institute of Image Information and Television Engineers (ITE) in 1996.

Hiroyuki Fujiyama, *Fujitsu Laboratories Ltd.*
Mr. Fujiyama joined Fujitsu Ltd. in 1986, where he has since been engaged in research and development of microprocessors. His current focus of work is on network and security system LSIs.

Toshiyuki Yoshitake, *Fujitsu Laboratories Ltd.*
Mr. Yoshitake received the M.S. degree in Electrical Engineering from Nagoya University, Nagoya, Japan in 1988. He then joined Fujitsu Laboratories Ltd. in Tokyo, Japan, where he has been engaged in research and development of digital TVs and computer graphics.