System LSIs with Cryptographic Functions and Their Applications

Kazuo Takaragi, Ph.D.
Kunihiko Nakada
Tooru Yamada
Takao Arai
Hideyuki Hara

OVERVIEW: Because of the rapid growth of the Internet, a large amount of information, including everything from financial information to image data, are being converted to digital data and transmitted at high speeds. Digital data is very useful, but there are real problems related to information security (safety). Since the digital data may be secretly looked at or tampered with by third parties with bad intentions, information security has become an urgent necessity. The techniques for providing this security can be found in the field of cryptography. Particular attention is currently focused on the use of system LSIs with cryptographic functions. To meet these needs, Hitachi makes MULTI2 cryptographic LSIs that can be applied to digital broadcasting or other systems.

INTRODUCTION

THE rapid development of the Internet has led to the conversion of a large amount of analog information of various kinds, such as documents and voice, and image information, to digital information. Digital data composed of bits of zeroes and ones can be easily transmitted over the Internet and processed on a computer. This kind of data is very useful, but there are real problems related to information security (safety), such as the ease of theft, tampering, and illegal use. The amount of damage caused by such behavior has increased rapidly on the Internet.

Basic techniques for solving this problem can be found in the field of cryptography. Cryptographic function incorporated in a system LSI can encrypt data passing through the LSI. The encrypted data can be protected from illegal use or tampering, even if it is located within an insecure environment such as the Internet.

This review describes trends of using system LSIs with new cryptographic functions, including standardization of electronic commerce, copyright protection, and electronic toll collection systems. In addition, a system LSI product that incorporates RSA

Fig. 1—Digital Data Requiring Protection by Cryptography.
The higher the value or price of information on the Internet, or the longer the effective period of the information, the more frequently the information is targeted by people with dishonest intentions. System LSIs with cryptographic functions are used to protect data from such people.
with public-key cryptography and MULTI2 with secret-key cryptography, as well as the systems applications, is also described.

THE NECESSITY OF SECURITY TECHNOLOGY UNDER PRESENT CONDITIONS

In general, the higher the value or price of data, or the longer its effective period, the greater the need for data protection (Fig. 1). If security measures are insufficient, much harm may result to businesses using such data. Therefore, information security technology is urgently needed.

Information security technologies have recently been standardized (Table 1). The new standards will be implemented in Hitachi’s system LSIs with cryptographic functions. Some of the new standards that have recently received a lot of attention are described in the following sections.

Illegal-copy Protection Systems ‡2

When large-capacity digital video discs (DVDs) appeared on the market, a problem suddenly arose in which original-quality duplicates were being redistributed or edited without permission, since they can easily be created. The recent progress of high-performance personal computers has aggravated this problem. In May 1996, the Motion Pictures Association of America (MPAA), Consumer Electronics Association (CEA), and information technology industries organized the Copy Protection Technical Working Group (CPTWG) to discuss copy protection technology for the content of movies or other information.

There are three main illegal-copy protection technologies: cryptography of content, cryptography of digitally transmitted data, and electronic watermark technology.

(1) Cryptography of content

Image and voice data in DVDs is encrypted by a system called the contents scramble system (CSS). A DVD player has a circuit in its playback unit that decrypts the data and restores the original content.

(2) Cryptography of digitally transmitted data

Data is encrypted for protection and transmitted on networks connecting consumer electronic appliances and computers. Hitachi M6 cryptography has been adopted for this cryptographic system, called digital transmission copy protection (DTCP). Detailed information can be obtained under license from Toshiba, Matsushita, Sony, and Intel, as well as from Hitachi.

(3) Electronic watermark technology

Depending on content, there may be a need to store copy control information in some types of content. Copy management information includes information that prevents copies to be made only allows a single copy to be made. To meet this need, the CPTWG is examining the use of electronic watermark technology to embed copy management information into content. The information can only be recognized by particular equipment and otherwise cannot be seen. Illegal use of content can be prevented because separating the electronic watermark from the content is difficult. Hitachi is affiliated with Galaxy (member companies: Hitachi, IBM, NEC, Pioneer, and Sony), and is

<table>
<thead>
<tr>
<th>Type</th>
<th>Organization</th>
<th>Target for Standardization</th>
<th>Typical technology</th>
<th>Adopted cryptography</th>
<th>Year of adoption</th>
<th>Refer to section marked (†1-4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>International standard</td>
<td>SETCo</td>
<td>Electronic commerce procedure on the Internet</td>
<td>SET v1.0</td>
<td>RSA, DES</td>
<td>1998</td>
<td>†1</td>
</tr>
<tr>
<td></td>
<td>MAOSCO</td>
<td>Smart-card system for electronic commerce</td>
<td>MULTOS v3</td>
<td>RSA, DES</td>
<td>1998</td>
<td>†2</td>
</tr>
<tr>
<td></td>
<td>CTPWG</td>
<td>Illegal-copy protection systems for digital products</td>
<td>5C</td>
<td>Elliptic curve</td>
<td>1998</td>
<td>†2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>M6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Electronic watermark)</td>
<td>1999 (Plan)</td>
<td></td>
</tr>
<tr>
<td>Japanese standard</td>
<td>The Ministry of Posts and</td>
<td>Limiting reception of CS and BS digital broadcasting</td>
<td>(CS or BS conditional access system)</td>
<td>MULTI2</td>
<td>1996</td>
<td>†3</td>
</tr>
<tr>
<td></td>
<td>Telecommunications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Ministry of Construction</td>
<td>Electronic toll collection system for expressways</td>
<td>ETC</td>
<td>(Under evaluation)</td>
<td>1999</td>
<td>†4</td>
</tr>
</tbody>
</table>

Table 1. Standardization of Information Security Technologies

Standardization is rapidly progressing both inside and outside Japan. Manufacturers provide system LSIs incorporating cryptographic algorithms determined as standards.

CS: communication satellite   BS: broadcast satellite
supporting international standardization activities in this field.

ETC System

The electronic toll collection (ETC) system is a new system that allows road traffic to flow through toll gates without stopping by automatically deducting the toll using a wireless communication system.

The automobile must be equipped with a special system to use the ETC service. The user inserts a smart card (in which certain information is stored) into an apparatus in the automobile, then drives on a toll road. As the automobile approaches a toll gate, the apparatus sends encrypted data to the toll gate, automatically paying the toll, without the driver having to stop the automobile.

Hitachi is developing a system LSI with cryptographic security functions especially for ETC equipment installed in automobiles (Fig. 2).

LSIs that implement existing standards are also extensively used. Some typical examples are described in the following sections.

**LSIs FOR ELECTRONIC CASH SYSTEM**

**SMART CARD**

Recently, smart cards have attracted a lot of attention since they can make digital signatures, perform cryptographic processing, and are more difficult to copy illegally than magnetic stripe cards.

Smart cards that incorporate a central processing unit (CPU) on an IC chip can provide tight security. Tampering or illegal copying of information, especially sensitive information such as financial information, can be avoided by storing the data in an internal non-volatile memory. The smart-card microcomputer also enables different methods of cryptography.

Hitachi started manufacturing smart-card microcomputers in 1986. In 1995, a smart-card microcomputer incorporating a co-processor that increases the cryptographic processing speed was mass-produced for electronic cash applications.

Fig. 3 is a block diagram of the H8/3113 smart-card microcomputer developed for electronic cash applications. The H8/3113 incorporates a high-performance 8-bit CPU, a large-capacity non-volatile EEPROM, ROM, and RAM. The CPU processes at high speed both secret-key cryptography, such as Hitachi’s MULTI2 and the US standard DES, and public-key cryptography, such as RSA and elliptic-curve cryptography. Encryption, such as Hitachi’s MULTI2 or the US Data Encryption Standard (DES), at high speed.

In addition, the H8/3113 includes a co-processor that can process RSA cryptography, which is the de facto world standard in public-key cryptography, at high speed. This co-processor can execute a 1,024-bit modular exponentiation in approximately 0.5 seconds.

Hitachi has also developed a program that can run elliptic curve cryptography on the H8/3113. This method has recently attracted a lot of attention as the next-generation public-key cryptographic method. The new program can carry out a 160-bit elliptic curve cryptography ECDSA (Elliptic Curve Digital Signature Algorithm) that provides the same degree of security as the 1,024-bit RSA operation in about 0.2 seconds.
Fig. 4 is a road map of Hitachi smart-card microcomputers. Products with an internal co-processor will be added to the line-up of the H8/3160 series, which are standard products with a variety of memory capacities. In addition, contactless specifications will be supported in the future. Moreover, highly reliable, easy-to-use smart-card microcomputers will be further developed through the application of non-volatile EEPROM fabrication techniques, miniaturizing process techniques for devices, such as the 0.35- and 0.18-µm scales, and high-performance CPU architecture.

**LSIs FOR DIGITAL BROADCAST SYSTEMS**

Digital Broadcast and Cryptography

Radio and television broadcasting, where analog techniques have been dominant for a long time, has started to go digital. Digital compression techniques for image and sound data and cryptographic techniques have rapidly made digital broadcasting techniques practical. In particular, the cryptographic technique can effectively and safely implement the three factors necessary to protect digital information: scrambling, conditional access (controlling the audience according to a pay-per-view contract), and copy protection.

A Scrambling Technique for Digital Broadcasting

When digital broadcasting was started, a scrambling technique based on cryptography was introduced. For analog broadcasting, scrambling is implemented indirectly, for example, by permuting the order of the scan lines in a TV signal. In digital broadcasting, however, image and sound data is represented digitally, and scrambling is achieved by directly applying cryptography to each bit.

By combining the contract management and scramble key control functions of the smart card, a system that supports various viewer-funded broadcasting systems can be configured, such as pay-per-view systems, where a fee is imposed in proportion to the length of time over which the subscriber receives broadcasts, or new interactive services.

The scrambling of digital broadcasts in Japan has been standardized using MULTI2 cryptography developed by Hitachi. The objective is to encourage the rapid spreading of digital broadcasting by assuring interoperability among all media. This was first implemented in the communication satellite broadcasting that started in 1996, and will be applied to satellite broadcasting in 2000. In the future, this technique will also be applied to terrestrial digital TV, terrestrial digital radio, and finally to satellite digital radio.

The major scrambling methods of the world are shown in Table 2.

<table>
<thead>
<tr>
<th>Country</th>
<th>Method</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Japan</td>
<td>MULTI2</td>
<td>Unified standard</td>
</tr>
<tr>
<td>Europe</td>
<td>DVB</td>
<td>Unified standard</td>
</tr>
<tr>
<td>US</td>
<td>(DES)</td>
<td>Uniquely employed by the respective enterprise</td>
</tr>
</tbody>
</table>

DVB: digital video broadcasting
Digital Broadcasting LSI with Cryptographic Function

A functional overview of a digital broadcasting receiver is shown in Fig. 5.

![Functional Diagram of Digital Broadcast Receiver](image)

Hitachi is now developing the HD814250, which is a system LSI for digital broadcasting receivers. The HD814250 incorporates the MULTI2 de-scrambler as a cryptographic function, and many other devices that support standardized technology, such as an MPEG2 transport demultiplexer conforming to the international standard ISO/IEC13818.

CONCLUSIONS

This review described trends in the use of system LSIs with new cryptographic functions, as well as standardization, related products, and examples of LSI applications.

In the future, the use of LSIs with cryptographic functions is expected to increase. Hitachi will further develop these technologies and propose products and systems that satisfy the requirements of the digital generation.

REFERENCE