

Key Technology for Digital Content

Memory Stick Copyright Protection Technology — MagicGate —

- Authentication
- Content encryption and decryption
- Conforms to the SDMI standard

Late last year, Sony released a Walkman product that uses the MagicGate Memory Stick (MG Memory Stick) as its recording media. (See photograph 1.) The MG Memory Stick can record one CD worth of music content stored on a PC in about 4 minutes. The Memory Stick Walkman uses ATRAC3 sound compression technology, and achieves the same sound quality, but without sound skipping, as the MD. However, due to its size and weight, the Memory Stick Walkman is far superior to MD in terms of portability.



■ Photograph 1 Memory Stick Walkman

Copyright control has become extremely important when dealing with music content. To conform to the SDMI*1 standards, the Sony Memory Stick Walkman adopts two unique Sony-developed copyright protection technologies: OpenMG*2 and MagicGate. (See figure 1.) These two technologies allow the Memory Stick Walkman to handle corresponding media only and to prevent secondary copying.

In this article, we would like to present the MagicGate copyright protection technology and Sony LSIs that incorporate that technology.

MAGICGATE™

This copyright protection technology is incorporated in both the MG Memory Stick semiconductor media and appliance that uses that media (referred to as "MG appliance" in this article). This technology provides two main functions.

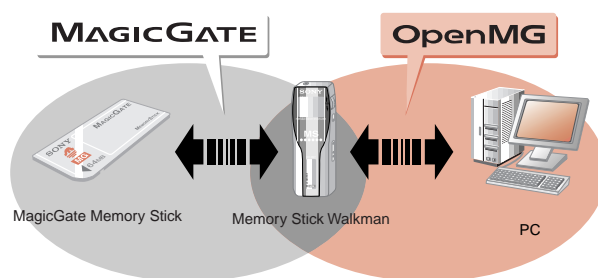
- Mutual confirmation between the media and the appliance that both the media and the MG appliance support copyright protection (authentication).
- Content encryption and decryption performed by MG appliance with authorized media.

If authentication is not established mutually, data exchange operations are not possible. This prevents inappropriate copying and protects the copyright on the content.

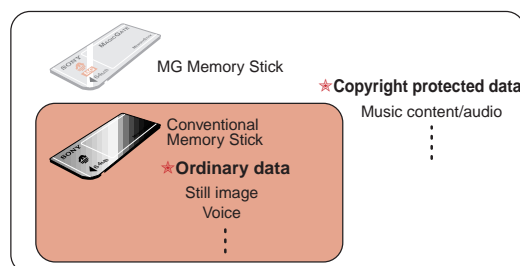
Note that these functions are provided in addition to the conventional functions of Memory Stick products (i.e., conventional products), and the MG Memory Stick assures upward compatibility. (See figure 2.)

*1 SDMI (Secure Digital Music Initiative) is an international standards organization concerned with music distribution.

*2 OpenMG is a copyright protection technology for managing digital music content acquired on a personal computer from sources such as CDs or the Internet.



■ Figure 1 Technological Relationship between MagicGate and OpenMG



* MG Memory Sticks can store both copyright protected data and ordinary data at the same time.

■ Figure 2 Upward Compatibility Concept

* MagicGate and the MagicGate logo are Sony Corporation trademarks.
 * MagicGate is the name of a copyright protection technique proposed by Sony. It does not guarantee compatibility between different media.
 * OpenMG and the OpenMG logo are Sony Corporation trademarks.

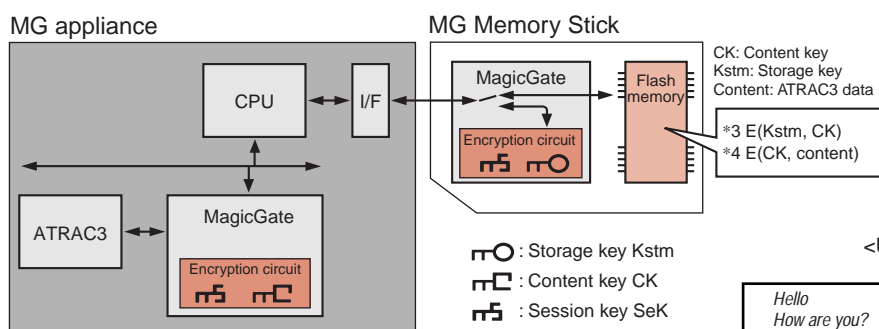
Systems

Figure 3 presents an overview of an MG appliance system that provides MagicGate functionality. The MG appliance itself includes a CPU, MagicGate, ATRAC3, and other technologies, while the MG Memory Stick includes MagicGate and flash memory. Recording and playback are possible after authentication has been established. Then content encryption or decryption and key transformation is performed during that recording or playback.

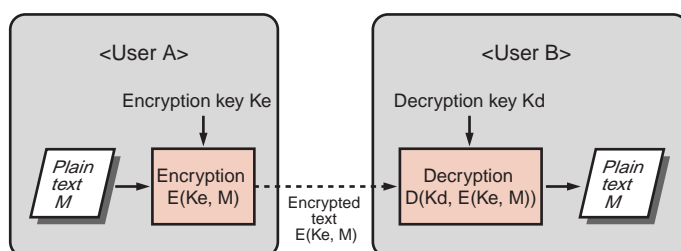
MG Memory Sticks record and store music content/audio data(*4) that is encrypted with a storage key and encrypted with the content key(*3).

Encryption and Keys

MagicGate uses encryption not only for encryption and decryption of content, but also for uses encryption in authentication. "Keys" play a critical role in encryption.



■ Figure 3 Application Appliance System Overview



■ Figure 4 Encryption and Keys

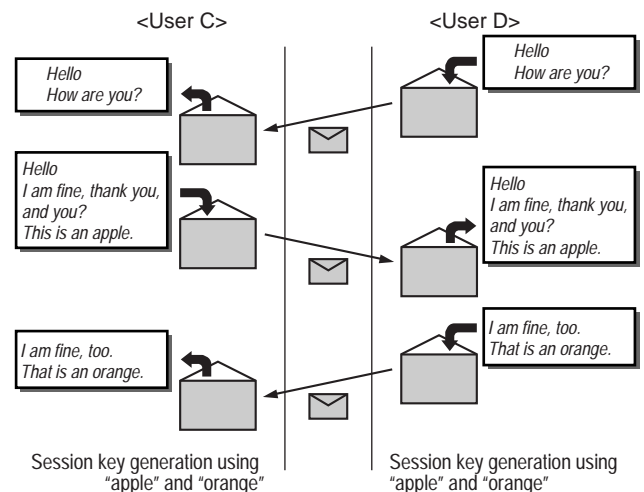
Figure 4 shows the situation when A sends content (plain text) to B using encryption. A uses the encryption key (Ke) to encrypt the plain text, and sends it to B. B decodes the received encrypted text with the decryption key (Kd) to convert it to plain text. If a third party acquires the encrypted text during this process, they will not be able to decrypt it (that is, view the plain text) unless they have the decryption key. This means that third parties cannot obtain the content that was sent. Thus the keys used in encryption play a critical role.

Authentication

The first operation performed between an MG Memory Stick and the MG appliance is authentication. That is, both the MG Memory Stick and the MG appliance must first determine that the other supports the corresponding functionality. Figure 5 shows this interaction using the exchange of letters as a metaphor. Here, consider C to be the MG appliance and D to be the MG Memory Stick.

First, D inserts a letter that contains the greeting "Hello, how are you?" in an envelope and sends it to C. Then C returns, as his reply, a letter in which he has written "Hello," "I am fine, thank you, and you?" and "This is an apple." When D receives that reply, he can determine (authentication by D) that C is the correct correspondent, since C responded to the "How are you?" inquiry. Then, D responds with "I am fine, too." and "That is an orange." C is then able to determine (authentication by C) that D is the correct correspondent, since D responded with "I am fine, too." This allows both C and D to authenticate the corresponding party.

MG Memory Stick and MG appliance authenticate each other in a similar manner. Instead of "How are you?" and "I am fine.", actual MG Memory Stick and MG appliance use their unique ID numbers and encryption. The data that corresponds to "apple" and "orange" in this example are then used for key generation in exchanges that take place after authentication.



■ Figure 5 Authentication

Record and Playback

Recording and playback of content becomes possible once authentication between the MG Memory Stick and the MG appliance has completed. To present an overview of these operations, we first introduce the three encryption keys that are used.

- **Content key CK:** This key is used for content encryption and decryption. The MG appliance uses this key.
- **Session key SeK:** This key is generated at each authentication and is used for temporary data exchanges. Both the MG appliance and the MG Memory Stick use this key.
- **Storage key Kstm:** This key is used for CK encryption and decryption. The MG Memory Stick uses this key.

1) Record mode

Figure 6 presents an overview of record mode.

- **Content encryption**

First, the music content acquired from CD or other source is compressed using ATRAC3. MagicGate uses the content key to encrypt that compressed data.

- **Record key transformation**

Next, the content key is encrypted using the session key and passed to the MG Memory Stick. After decrypting the content key with the session key, the MG Memory Stick encrypts it with the storage key and returns it to the MG appliance. (See figure 7.)

- **Recording to the MG Memory Stick**

The MG appliance writes the encrypted content and storage keys to the flash memory in the MG Memory Stick according to the Memory Stick file operation.

2) Playback mode

Figure 8 presents an overview of playback mode.

- **Readout from the MG Memory Stick**

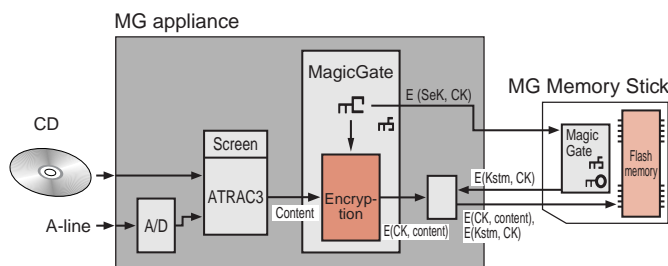
The MG appliance reads out both the encrypted content and content key from the flash memory in the MG Memory Stick. At this time, it can check if the content is an illegal copy.

- **Playback key transformation**

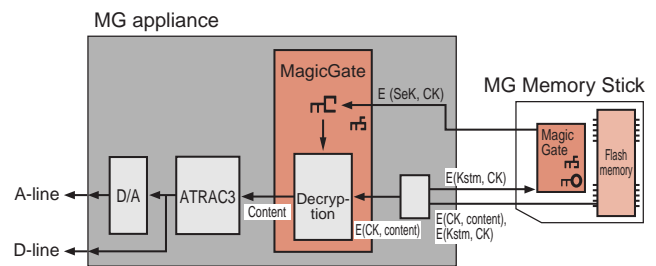
The MG appliance sends the content key encrypted with the storage key to the MG Memory Stick. After decrypting the content key with the storage key, the MG Memory Stick encrypts the session key and sends it to the MG appliance. (See figure 9.)

- **Content decryption**

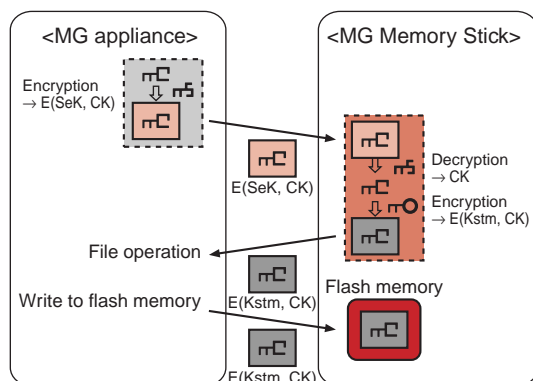
First, the MG appliance decrypts the content key with the session key and then, using the content key, decrypts the encrypted content, resulting in compressed music content/audio data. It then decodes that data with ATRAC3 and plays it back.



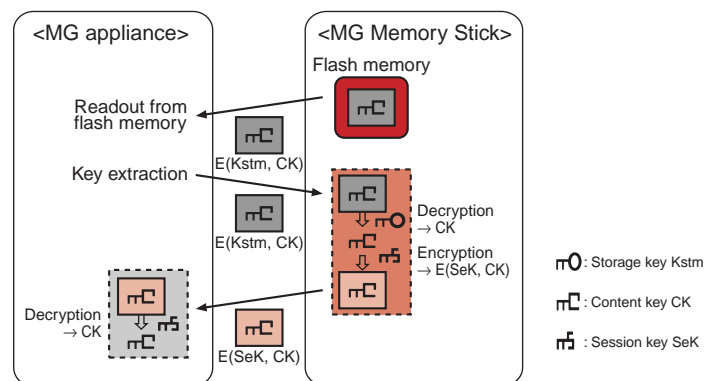
■ Figure 6 Record Mode



■ Figure 8 Playback Mode



■ Figure 7 Key Transformation during Recording



■ Figure 9 Key Transformation during Playback

\circ : Storage key Kstm
 \square : Content key CK
 ∇ : Session key SeK

MagicGate LSIs

Sony has developed two special-purpose LSIs to implement MagicGate: the MagicGate (D) security control LSI for use in MG appliance, and the MagicGate (M) security control LSI for use in MG Memory Stick. (See figures 10 and 11 and table 1.)

1) MagicGate (D)

MagicGate (D) provides a CPU interface that supports 16-bit bus width DMA and an ATRAC3 interface. It also includes a 512-byte FIFO, an encryption circuit, and an authentication circuit. It stores the information necessary for authentication in nonvolatile memory (NVM), and uses anti-tampering technology to protect that information. It also provides clock outputs for the ATRAC3, D/A converter, A/D converter, and other peripheral LSIs.

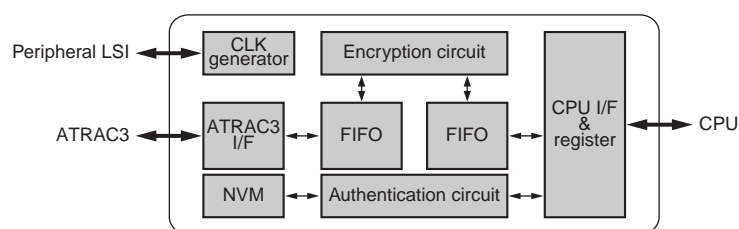
2) MagicGate (M)

The MagicGate (M) LSI integrates

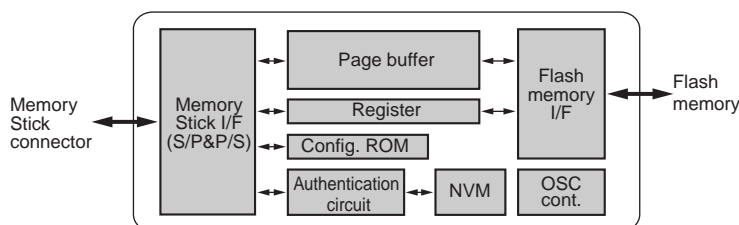
MagicGate functionality with conventional memory controller functions on a single chip for use in MagicGate Memory Sticks. MagicGate (M) conforms to the Memory Stick Standard Format specifications ver. 1.2, which is the Memory Stick standard*³, and the MagicGate Format specifications ver. 1.0.

The Memory Stick interface converts between serial and parallel data, and exchanges data with registers, a page buffer (512 bytes), the authentication circuit, and other functions. The flash memory interface supports NAND-type flash memory. Based on values loaded into registers, the MagicGate (M) LSI transfers data between the page buffer and flash memory and controls the read, write, and erase operations. Like the MagicGate (D), this LSI also provides anti-tampering technology and stores its unique ID and key in nonvolatile memory.

*³ The Memory Stick standard is only made available to corporations who have concluded a licensing agreement.



■ Figure 10 MagicGate (D)



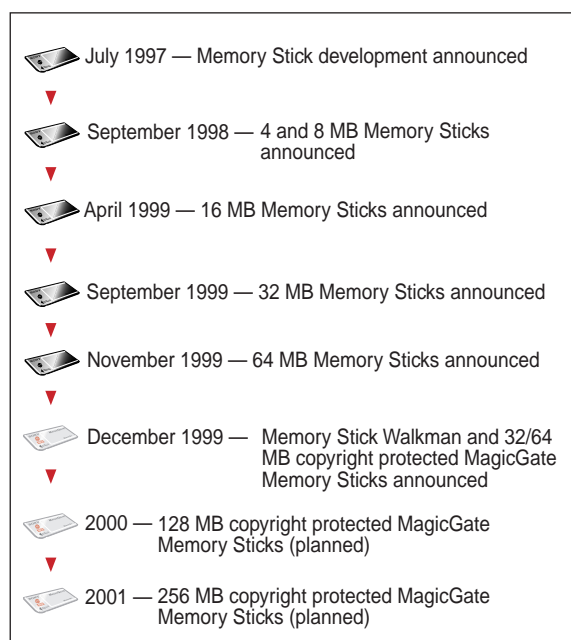
■ Figure 11 MagicGate (M)

■ Table 1 MagicGate LSI Product Overview

	MagicGate(D)	MagicGate(M)
Supply voltage	2.7 to 3.6 V	2.7 to 3.6 V
Operating frequency	22.58 MHz	20 MHz
Operating temperature	-20 to +80 °C	-20 to +80 °C
Package	113-pin TFBGA	64-pin TQFP
Interface	CPU I/F; SH2-DSP ATRAC3 I/F	Memory Stick I/F NAND flash memory I/F

Future Development

With digital music distribution services over the Internet and other networks growing rapidly, Sony aimed to create a highly reliable music copyright protection technology that can respond to the needs of the network age. Towards this goal, Sony developed the unique MagicGate and OpenMG technologies, and released products that conform to SDMI standard at the end of 1999. (See figure 12.) This article introduced two MagicGate structural component LSIs: the MagicGate (D) MG appliance security controller and the MagicGate (M) Memory Stick security controller. In the future, Sony will be developing a wide range of MG appliance products that include MagicGate Memory Stick technology to support the growth of all forms of digital music content delivery. Sony plans to aggressively expand their product line of semiconductor devices required for these applications, and, in particular, strive for increased capacities in Memory Stick media and higher integration levels in the devices for use in MG appliance products.



■ Figure 12 Memory Stick/MG Memory Stick Road Map