

TECHNICAL FIELD

The present invention relates to a semiconductor
5 memory card for storing digital contents, and a data reading
apparatus for reading out the digital contents from the
semiconductor memory card. More particularly, the present
invention relates to a semiconductor memory card and a data
reading apparatus suitable for copyright protection of digital
10 contents.

BACKGROUND ART

The multimedia network technology has developed to the
extent that digital contents such as music contents are
distributed via a communication network such as the Internet.
15 This makes it possible to access a variety of music or the like
provided from around the world at home. For example, a music
content can be downloaded into a personal computer (hereafter
referred to as PC), then stored in a semiconductor memory card
loaded into the PC. Also, the semiconductor memory card can be
20 removed from the PC and can be loaded into a portable music
player. This enables one to listen to the music while walking.
The semiconductor memory cards are compact and lightweight cards

5 beforehand using a key or the like to prevent unauthorized
copying of the digital contents. Also, an arrangement is
required so that file management software programs, many of
which are standard equipments on commercial PCs, cannot copy the
digital contents to other storage mediums.

10 In one possible method for preventing unauthorized
copying, only dedicated software programs are allowed to access
the semiconductor memory card. For example, when an
authentication process between a PC and a semiconductor memory
card has completed affirmatively, a PC is allowed to access the
15 semiconductor memory card; and when the authentication process
has not completed affirmatively due to the lack of a dedicated
software program, the PC is not allowed to access the
semiconductor memory card.

 However, in the above method in which PCs should
20 always have a dedicated software program to access the
semiconductor memory card, free data exchange with users via the
semiconductor memory card is not available. As a result, the
above method loses a merit of conventional semiconductor memory
cards, namely, a merit that file management software programs
25 being standard equipments on commercial PCs can be used to

memory cards function to protect copyright of the digital contents. However, the semiconductor memory cards have a problem that they cannot be used as auxiliary storage apparatuses in general-purpose computer systems.

DISCLOSURE OF INVENTION

10 It is therefore an object of the present invention to provide a semiconductor memory card that can be used as a storage medium for storing digital contents and as a storage medium for storing general-purpose computer data (not an object of copyright protection), and to provide an apparatus for
15 reading data from the storage medium.

 The above object is fulfilled by a semiconductor memory card that can be used/removed in/from an electronic device, comprising: a rewritable nonvolatile memory; and a control circuit which controls accesses by the electronic device
20 to an authentication area and a non-authentication area in the rewritable nonvolatile memory, wherein the control circuit includes: a non-authentication area access control unit which controls accesses by the electronic device to the non-authentication area; an authentication unit which performs an

5 access the authentication area only when the authentication unit affirmatively authenticates the electronic device.

With the above construction, the data being an object of copyright protection can be stored in the authentication area and other data can be stored in the non-authentication area, 10 which makes it possible to achieve such a semiconductor memory card as can store both digital contents to be copyright-protected and other data together.

In the above semiconductor memory card, the authentication unit may generate a key reflecting a result of 15 the authentication process, and the authentication area access control unit decrypts an encrypted instruction using the key generated by the authentication unit, and controls accesses by the electronic device to the authentication area in accordance with the decrypted instruction, the encrypted instruction being 20 sent from the electronic device.

With the above construction, even if the communication between the semiconductor memory card and an electronic device is tapped, the instruction to access the authentication area has been encrypted, reflecting the result of the preceding 25 authentication. Accordingly, such a semiconductor memory card

5 authentication with the electronic device, and generates the key
from challenge data and response data, the challenge data being
sent to the electronic device to check whether the electronic
device is proper, and the response data being generated to show
the authentication unit is proper.

10 With the above construction, the key is shared by the
semiconductor memory card and the electronic device only when
both devices affirmatively authenticate each other.
Furthermore, the key changes for each authentication. This
enhances the security of the authentication area since the
15 authentication area cannot be accessed without using the key.

In the above semiconductor memory card, the encrypted
instruction sent from the electronic device may include a tag
field and an address field, the tag field not having been
encrypted and specifying a type of an access to the
20 authentication area, the address field having been encrypted and
specifying an address of an area to be accessed, wherein the
authentication area access control unit decrypts the address
field using the key, and controls accesses by the electronic
device to the authentication area so that an access of the type
25 specified in the tag field is made to the area indicated by the

5 semiconductor memory card which receives the instruction.

The above semiconductor memory card may further comprise: an identification data storage circuit which prestores identification data which is unique to the semiconductor memory card and enables the semiconductor memory card to be
10 discriminated from other semiconductor memory cards, wherein the authentication unit performs a mutual authentication with the electronic device using the identification data stored in the identification data storage circuit, and generates the key from the identification data.

15 With the above construction, in the mutual authentication process, data unique to each semiconductor memory card is exchanged. This keeps a superior level security against unlawful decoding of the mutual authentication.

The above semiconductor memory card may further
20 comprise: an area resizing circuit which resizes the authentication area and the non-authentication area.

With the above construction, the semiconductor memory card can be used dynamically. That is, the semiconductor memory card can be used mainly as a record medium for digital contents
25 and can be used as an auxiliary storage apparatus in a commuter

5 in the rewritable nonvolatile memory into two, and the area
resizing circuit resizes the authentication area and the non-
authentication area by changing an address marking a boundary
between the authentication area and the non-authentication
area.

10 With the above construction, the size of the
authentication and non-authentication areas can be changed only
by moving the boundary. This reduces the circuit size.

In the above semiconductor memory card, the area
resizing circuit may include: an authentication area conversion
15 table which shows correspondence between logical addresses and
physical addresses in the authentication area; a non-
authentication area conversion table which shows correspondence
between logical addresses and physical addresses in the non-
authentication area; and a conversion table change unit which
20 changes contents of the authentication area conversion table and
the non-authentication area conversion table in accordance with
an instruction from the electronic device, wherein the
authentication area access control unit controls accesses by the
electronic device to the authentication area by referring to the
25 authentication area conversion table, and the non-authentication

5 separately manage the authentication area and the non-authentication area in terms of the area size and relationships between the logical addresses and physical addresses since conversion tables for these areas are independently operated.

10 In the above semiconductor memory card, an area addressed with higher physical addresses and an area addressed with lower physical addresses both constituting the area having the predetermined size may be respectively allocated to the authentication area and the non-authentication area, the non-authentication area conversion table shows correspondence
15 between logical addresses arranged in ascending order and physical addresses arranged in ascending order, and the authentication area conversion table shows correspondence between logical addresses arranged in ascending order and physical addresses arranged in descending order.

20 With the above construction which enables the logical addresses to be used in ascending order, the area size can be changed easily since the probability of use of an area around the boundary between the authentication area and the non-authentication area becomes low. This also lowers the
25 probability of occurrence of data saving or moving which is

5 With the above construction, the function of copyright protection is enhanced by storing identification data of the semiconductor memory card in the dedicated memory and storing the digital contents depending on the results of identification based on the identification data.

10 In the above semiconductor memory card, each of the authentication area and the non-authentication area may include: a read/write storage area from/to which the electronic device can read/write data; and a read-only storage area from which the electronic device can read data but to which the electronic
15 device cannot write data, the control circuit further includes: a random number generator which generates a random number each time the electronic device writes data to the rewritable nonvolatile memory, and each of the authentication area access control unit and the non-authentication area access control unit
20 encrypts data using the random number, writes the encrypted data to the read/write storage area, and writes the random number to the read-only storage area.

 With the above construction, unlawful attempts such as tampering of the read/write storage area can be detected by
25 checking the compatibility with the random number stored in the

5 correspondence between logical addresses and physical addresses
in each of the authentication area and the non-authentication
area; and a conversion table change circuit which changes
contents of the conversion table in accordance with an
instruction from the electronic device, and the authentication
10 area access control unit and the non-authentication area access
control unit control accesses by the electronic device to the
authentication area and the non-authentication area,
respectively, by referring to the conversion table.

With the above construction, even if the plurality of
15 logical blocks constituting the same file are fragmented, they
can be easily changed to become logically successive. This
increases the speed of accessing the same file.

In the above semiconductor memory card, the control
circuit may further include: an encryption/decryption unit which
20 encrypts data to be written to the authentication area and the
non-authentication area and decrypts data read out from the
authentication area and the non-authentication area.

With the above construction, it is possible to defend
the authentication area and the non-authentication area against
25 unlawful attacks such as destroying the semiconductor memory

5 accordance with an instruction from the electronic device,
identifies not-deleted areas in the authentication area and the
non-authentication area, and sends information indicating the
not-deleted areas to the electronic device.

10 With the above construction, the electronic device can
identify not-deleted areas and delete the identified not-deleted
areas before the flash memory is rewritten. This increases the
speed of the rewriting.

In the above semiconductor memory card, the
authentication unit may request a user of the electronic device
15 to input a user key, which is information unique to the user,
during the authentication process, and the control circuit
further includes: a user key storage unit which stores the user
key; an identification information storage unit which stores a
piece of identification information identifying an electronic
20 device that has been affirmatively authenticated by the
authentication unit; and a user key request prohibition unit
which obtains a piece of identification information from a
target electronic device after the authentication unit starts
the authentication process, checks whether the piece of
25 identification information obtained from the target electronic

5 target electronic device has already been stored in the
identification information storage unit.

With the above construction, the user need not input
a password or personal data each time the user accesses the
semiconductor memory card. This prevents the occurrence of
10 unlawful tapping and using of the personal data.

The above object is also fulfilled by a data reading
apparatus for reading out a digital content from the above
semiconductor memory card, the digital content having been
stored in the non-authentication area of the semiconductor
15 memory card, and information indicating the number of times the
digital content can be read out being prestored in the
authentication area, the data reading apparatus comprising: a
judgement means for, when the digital content is to be read out
from the non-authentication area, reading out the information
20 indicating the number of times the digital content can be read
out from the authentication area, and judging whether the
digital content can be read out based on the number of times
indicated in the information; and a reproduction means for
reading out the digital content from the non-authentication area
25 only when the judgement means judges that the digital content

5 the number of times the digital content is read out from the semiconductor memory card. This enables the present invention to be applied to chargeable, rental music contents.

The above object is also fulfilled by a data reading apparatus for reading out a digital content from the above
10 semiconductor memory card and reproducing the read-out digital content as an analog signal, the digital content, which can be reproduced as an analog signal, having been stored in the non-authentication area of the semiconductor memory card, and information indicating the number of times the digital content
15 can be digitally output by the electronic device having been stored in the authentication area, the data reading apparatus comprising: a reproduction means for reading out the digital content from the non-authentication area and reproducing the read-out digital content as an analog signal; a judgement means
20 for reading out the information indicating the number of times the digital content can be digitally output by the electronic device, and judging whether the digital content can be digitally output based on the number of times indicated in the information; and a digital output means for digitally outputting
25 the digital content only when the judgement means judges that

5 the number of times the digital content is digitally copied from
the semiconductor memory card. This provides a copyright
protection detailed with caution and attentiveness as intended
by the copyright owner.

As described above, the present invention is a
10 semiconductor memory card functioning with flexibility both as
a record medium for storing digital contents and an auxiliary
storage apparatus of a computer. The present invention
especially secures healthy distribution of digital contents for
electronic music distribution. This is practically valuable.

15 BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 shows the appearance of a PC which is an
embodiment of the present invention and is related to an
electronic music distribution, and shows the appearance of a
semiconductor memory card which can be loaded into and removed
20 from the PC.

FIG. 2 shows the appearance of a portable player for
which the semiconductor memory card is used as a record
medium.

FIG. 3 is a block diagram showing the hardware

5 of the semiconductor memory card.

FIG. 6 shows various storage areas in the semiconductor memory card which can be recognized by the PC and the player.

10 FIGs. 7A, 7B, and 7C show limitations and command formats when the PC or the player accesses an area in the semiconductor memory card. FIG. 7A shows rules to be followed for accessing each area. FIG. 7B shows rules to be followed for changing the size of each area. FIG. 7C is a schematic representation of areas in the semiconductor memory card.

15 FIG. 8 is a flowchart showing a procedure in which the PC (or the player) writes a music content or the like to the semiconductor memory card.

FIG. 9 is a flowchart showing a procedure in which a music content or the like is read out from the semiconductor
20 memory card and played by the player (or the PC).

FIG. 10 is a flowchart showing the operation in which the player (or the PC) handles the number of read-outs stored in the authentication area in the semiconductor memory card.

FIG. 11 is a flowchart showing the operation in which
25 the player (or the PC) handles the number of permitted digital

5 memory card, and also shows a flowchart of the reading/writing process corresponding to the data structure.

FIGs. 13A to 13D show a change in the relationship between the logical addresses and physical addresses. FIG. 13A shows the relationship before the change. FIG. 13B shows the relationship after the change. FIG. 13C shows a conversion table corresponding to FIG. A. FIG. 13D shows a conversion table corresponding to FIG. B.

FIGs. 14A to 14D show functions related to not-deleted blocks in the semiconductor memory card. FIG. 14A shows the use state of logical and physical blocks and physical blocks. FIG. 14B shows the not-deleted block list corresponding to the use state of the blocks shown in FIG. 14A. FIG. 14C is a flowchart showing the procedure of the PC or the player for deleting blocks beforehand using the not-deleted block list command and the delete command. FIG. 14D is a table showing the use state of the logical blocks.

FIG. 15 shows a communication sequence in an authentication between the player and the semiconductor memory card and also shows main components used in the authentication.

5 procedure of the mutual authentication shown in FIG. 16.

FIGs. 18A to 18C show the state before the boundary between the authentication and non-authentication areas of the semiconductor memory card is changed. FIG. 18A is a memory map showing the construction of the physical blocks in the flash
10 memory. FIG. 18B shows a conversion table dedicated to the non-authentication area. FIG. 18C shows a conversion table dedicated to the authentication area.

FIGs. 19A to 19C show the state after the boundary between the authentication and non-authentication areas of the
15 semiconductor memory card is changed. FIG. 19A is a memory map showing the construction of the physical blocks in the flash memory. FIG. 19B shows a conversion table dedicated to the non-authentication area. FIG. 19C shows a conversion table dedicated to the authentication area.

20 BEST MODE FOR CARRYING OUT THE INVENTION

An embodiment of the present invention will be described with reference to the drawings.

FIG. 1 is a schematic representation of a PC which downloads digital contents such as music contents via a

5 speakers 106, and is connected to a communication line 101 via
a modem embedded in the PC 102. A memory card writer 107 has
been inserted into a card slot (a memory card writer insertion
slot 105) of the PC 102. The memory card writer insertion slot
105 is based on PCMCIA (Personal Computer Memory Card
10 International Association) standards or the like. The memory
card writer 107 is an adaptor which electrically connects the PC
102 and a memory card 109. The memory card 109 is inserted into
a memory card insertion slot 108 of the memory card writer
107.

15 The user obtains music data from a contents provider
on the Internet using the above system and the following
procedure.

 First, the user downloads a desired music content into
a hard disk in the PC 102 via the communication line 101.

20 However, since the music content has been encrypted, the user is
required to execute a certain procedure to play the obtained
music content on the PC 102.

 To play the obtained music content, the user needs to
pay the charge to the contents provider using a credit card or
25 the like beforehand. When the user pays the charge, the user

5 the PC, such as the number of permitted plays, the number of permitted writings to the memory card, an expiration date indicating a period permitted for the user to play the content.

After having obtained the password and the rights
10 information, the user, when intending to output the music from the speakers 106 of the PC 102, inputs the password through the keyboard 104 to the PC 102 while a dedicated application program (hereafter referred to as application) having a copyright protection function is running on the PC 102. The application
15 then checks the rights information, decrypts the encrypted music content using the password, plays the decrypted music content to output the sounds from the speakers 106.

When the rights information indicates that the content is permitted to be written to the memory card, the application
20 can write the encrypted music data, password, and rights information to the memory card 109.

FIG. 2 is a schematic representation of a portable copy/play apparatus (hereafter referred to as player) 201 for which the memory card 109 is used as a record medium.

25 On the upper surface of the player 201, a liquid

5 206, and the communication port 213 is achieved by USB
(Universal Serial Bus) or the like and connects to the PC 102.
On a side of the player 201, an analog output terminal 204, a
digital output terminal 205, and an analog input terminal 223
are formed.

10 The player 201, after the memory card 109 storing
music data, a password, and rights information is loaded into
the player 201, checks the rights information. When the music
is permitted to be played, the player 201 reads out the music
data, decrypts the read-out music data, converts the decrypted
15 music content into an analog signal, and outputs the sounds of
the analog signal through headphones 208 connected to the analog
output terminal 204. Alternatively, the player 201 outputs
digital data of the music data to the digital output terminal
205.

20 The player 201 can also convert an analog audio
signal, which is input to the player 201 through a microphone or
the like then the analog input terminal 223, into digital data
and stores the digital data in the memory card 109. The player
201 can also download music data, a password, and rights
25 information from the PC 102 via the communication port 213 and

5 recorded on the memory card 109.

FIG. 3 is a block diagram showing the hardware construction of PC 102.

The PC 102 includes a CPU 110, a ROM 111 prestoring a device key 111a and a control program 111b, a RAM 112, the display 103, a communication port 113 including a modem port used for connection to the communication line 101 and an USB used for connection to the player 201, the keyboard 104, an internal bus 114, the memory card writer 107 connecting the memory card 109 and the internal bus 214, a descrambler 117 for descrambling the encrypted music data read out from the memory card 109, an AAC decoder 118 conforming to MPEG2-AAC (ISO13818-7) standard for decoding the descrambled music data, a D/A converter 119 for converting the decoded digital music data into an analog audio signal, the speakers 106, and a hard disk 120 storing a file management software program and an application.

The PC 102 can perform the following:

(1) use the memory card 109 as an auxiliary storage apparatus having an independent file system (e.g., ISO9293) as hard disks have by executing the file management software program stored in the hard disk 120,

5 (3) store the music contents or the like in the memory card 109
after a mutual authentication, and
(4) read out the music contents or the like from the memory card
109 and output the read-out contents to the speakers 106 for
playing.

10 The device key 111a stored in the ROM 111 is a secret
key unique to the PC 102 and is, as will be described later,
used for the mutual authentication or the like.

FIG. 4 is a block diagram showing the hardware
construction of the player 201.

15 The player 201 includes a CPU 210, a ROM 211
prestoring a device key 211a and a control program 211b, a RAM
212, a liquid crystal display unit 203, a communication port 213
achieved by an USB or the like used for connection to the PC
102, operation buttons 202, an internal bus 214, a card I/F unit
20 215 connecting the memory card 109 and the internal bus 214, an
authentication circuit 216 for executing a mutual authentication
with the memory card 109, a descrambler 217 for descrambling the
encrypted music data read out from the memory card 109, an AAC
decoder 218 conforming to MPEG2-AAC (ISO13818-7) standard for
25 decoding the descrambled music data, a D/A converter 219 for

5 AAC (ISO13818-7) standard for encoding the digital music data,
a scrambler 222 for scrambling the encoded music data, an analog
output terminal 204, a digital output terminal 205, and an
analog input terminal 223.

10 The player 201 loads the control program 211b from the
ROM 211 into the RAM 212 to allow the CPU 210 to execute the
control program 211b. By doing this, the player 201 can read
out music contents from the memory card 109, play and output the
read-out music contents to the speakers 224 and can also store
music contents input via the analog input terminal 223 and
15 communication port 213 into the memory card 109. That is to
say, the user can use the player 201 not only for copying and
playing music personally as with ordinary players, but also for
copying and playing such music contents (protected by copyright)
as are distributed by an electronic music distribution system
20 and downloaded by the PC 102.

FIG. 5 shows the appearance and hardware construction
of the memory card 109.

The memory card 109 contains a rewritable nonvolatile
memory to which data can be written repeatedly. The rewritable
25 nonvolatile memory has capacity of 64MB, and is driven by power

5 electrically connected to an external apparatus via a 9-pin connection terminal formed at an end of the memory card 109.

The memory card 109 contains three IC chips: a control IC 302, a flash memory 303, and a ROM 304.

10 The flash memory 303 is a flash-erasable, rewritable nonvolatile memory of a block deletion type, and includes logical storage areas: an authentication area 332 and a non-authentication area 331. The authentication area 332 can be accessed only by the apparatuses that have been authenticated as proper apparatuses. The non-authentication area 331 can be
15 accessed by any apparatuses whether they are authenticated or not. In the present embodiment, the authentication area 332 is used for storing important data related to copyright protection, and the non-authentication area 331 is used as an auxiliary storage apparatus in a typical computer system. Note that a
20 certain address in the flash memory 303 is used as a boundary between these two storage areas.

The ROM 304 includes a storage area which is a read-only area and is called special area. The special area prestores information including: a medium ID 341 which is an
25 identifier of the memory card 109; and a maker name 342 which

5 authentication between apparatuses and used for preventing an
unauthorized access to the authentication area 332.

The control IC 302 is a control circuit composed of
active elements (logic gates and the like), and includes an
authentication unit 321, a command judgement control unit 322,
10 a master key storage unit 323, a special area access control
unit 324, an authentication area access control unit 325, a non-
authentication area access control unit 326, and an
encryption/decryption circuit 327.

The authentication unit 321 is a circuit that performs
15 a challenge-response-type mutual authentication with a remote
apparatus attempting to access the memory card 109. The
authentication unit 321 includes a random number generator and
an encryption unit, and authenticate the remote apparatus as a
proper one when having confirmed that the remote apparatus has
20 the same encryption unit as the local apparatus. Note that in
the challenge-response-type mutual authentication, both two
apparatuses in communication perform the following: the local
apparatus first sends challenge data to the remote apparatus,
the remote apparatus in return generates response data by
25 processing the received challenge data for certifying the

5 The command judgement control unit 322 is a controller composed of a decoding circuit and a control circuit. The decoding circuit identifies a command (an instruction to the memory card 109) input via a command pin and execute the identified command. The command judgement control unit 322
10 controls the components 321 to 327 in accordance with the received commands.

 The commands received by the command judgement control unit 322 includes not only commands to read, write, and delete data from/into the flash memory 303, but commands to control the
15 flash memory 303 (commands related to an address space, not-deleted data, etc.).

 For example, in relation to reading/writing data, the SecureRead address count command and the SecureWrite address count command are defined as commands for accessing the
20 authentication area 332, and the Read address count command and the Write address count command are defined as commands for accessing the non-authentication area 331. In the above commands, "address" is a serial number of the first sector of a sequence of sectors from/on which data is read or written by the
25 command. "Count" is the total number of sectors from/on which

5 The master key storage unit 323 prestores a master key
323a which is used by the remote apparatus during the mutual
authentication and is used to protect data in the flash memory
303.

10 The special area access control unit 324 is a circuit
for reading out information such as the medium ID 341 from the
special area (ROM) 304.

15 The authentication area access control unit 325 and
the non-authentication area access control unit 326 are circuits
for reading/writing data from/to the authentication area 332 and
the non-authentication area 331, respectively. Each of the
units 325 and 326 sends/receives data to/from external
apparatuses (the PC 102, the player 201, etc.) via four data
pins.

20 It should be noted here that the access control units
325 and 326 each contains a buffer memory as large as one block
(32 sectors, or 16K bytes), and logically, inputs/outputs data
in units of sectors to/from the area 332 or 331 in response to
a command issued from an external apparatus, although it
inputs/outputs data in units of blocks when the flash memory 303
25 is rewritten. More specifically, when a sector in the flash

5 block of data including the rewritten sector to the flash memory
303.

10 The encryption/decryption circuit 327 is a circuit
which performs encryption and decryption using the master key
323a stored in the master key storage unit 323 under the control
of the authentication area access control unit 325 and the non-
authentication area access control unit 326. The
15 encryption/decryption circuit 327 encrypts data before writing
the data to the flash memory 303, and decrypts the data after
reading out the data from the flash memory 303. These
encryption and decryption are performed to prevent unlawful acts
such as an act of disassembling the memory card 109, analyzing
the contents of the flash memory 303 directly, and stealing the
password from the authentication area 332.

20 It should be noted here the control IC 302 includes
a synchronization circuit, a volatile storage area, and a
nonvolatile storage area as well as the main components 321 to
327. The synchronization circuit generates an internal clock
signal in synchronization with a clock signal supplied from a
clock pin, and supplies the generated internal clock signal to
25 each component.

5 303. In this case, the special area access control unit 324 may
impose a limitation on writing data to the information, or the
encryption/decryption circuit 327 may encrypt the information
before the information is stored in the flash memory 303.

FIG. 6 shows various storage areas in the memory card
10 109 which can be recognized by the PC 102 and the player 201.
The storage areas in the memory card 109 are classified into
three main areas: special area 304; authentication area 332; and
non-authentication area 331.

The special area 304 is a read-only area. A dedicated
15 command is used to read data from the special area 304.
Reading/writing data from/to the authentication area 332 is
possible only when the authentication between the PC 102 or the
player 201 and the memory card 109 has been affirmative. An
encrypted command is used to access the authentication area 332.

20 The non-authentication area 331 can be accessed by commands on
public use such as the commands conforming to the ATA (AT
Attachment) or SCSI (Small Computer System Interface) standard.
That is to say, data can be read/written from/to the non-
authentication area 331 without an authentication process.

25 Accordingly, a file management software program being a standard

5 shown below which provide the areas with a function as an auxiliary storage apparatus for a typical PC, and a function to copyright-protect the music data distributed by an electronic music distribution system.

10 The non-authentication area 331 stores an encrypted content 426, user data 427, etc. The encrypted content 426 is music data being an object of copyright protection and having been encrypted. The user data 427 is general data irrelevant to copyright protection. The authentication area 332 stores an encryption key 425 which is a secret key used for decrypting the
15 encrypted content 426 stored in the non-authentication area 331. The special area 304 stores the medium ID 341 which is necessary for accessing the authentication area 332.

The PC 102 or the player 201 first reads out the medium ID 341 from the special area 304 in the memory card 109
20 loaded into itself, then extracts the encryption key 425 and the rights information from the authentication area 332 using the medium ID 341. When it is confirmed from the rights information that the encrypted content 426 stored in the non-authentication area 331 is permitted to be played, the encrypted content 426
25 can be read out and played while being decrypted with the

5 attempts to play the music data from the memory card 109 loaded
into the player 201. In this case, although the non-
authentication area 331 in the memory card 109 stores the music
data, no encryption key 425 or rights information corresponding
to the music data is stored in the authentication area 332.
10 Therefore, the player 201 fails to play the music data. With
such a construction in which when only a music content is copied
to the memory card 109 without authorized encryption key or
rights information, the music content cannot be played,
unauthorized copying of digital contents is prevented.

15 FIGs. 7A, 7B, and 7C show limitations and command
formats when the PC 102 or the player 201 accesses an area in
the memory card 109. FIG. 7A shows rules to be followed for
accessing each area. FIG. 7B shows rules to be followed for
changing the size of each area. FIG. 7C is a schematic
20 representation of the areas in the memory card 109.

The special area 304 is a read-only area and can be
accessed by a dedicated command without an authentication
process. The medium ID 341 stored in the special area 304 is
used to generate or decrypt the encrypted command which is used
25 to access the authentication area 332. More specifically, the

5 the encrypted command using the medium ID 341, interprets and executes the command.

The authentication area 332 can be accessed only when an authentication between an apparatus attempting to access the memory card 109 such as the PC 102 or the player 201 and the
10 memory card 109 has been affirmative. The size of the authentication area 332 is equal to the size of (YYYY+1) sectors. That is to say, the authentication area 332 is composed of sector 0 to sector YYYY (YYYYth sector) logically, and is composed of sectors having XXXXth sector address to
15 (XXXX+YYYY)th sector address in the flash memory 303, physically. Note that sector addresses are serial numbers assigned uniquely to all the sectors constituting the flash memory 303.

The non-authentication area 331 can be accessed by a standard command conforming to the ATA or SCSI standard. The
20 size of the non-authentication area 331 is equal to XXXX sectors. That is to say, the non-authentication area 331 is logically and physically composed of sector 0 to (XXXX-1)th sectors.

It should be noted here that an alternate block area
25 501 may be allocated in the flash memory 303 beforehand. The

5 authentication area 331.

In the present embodiment, the special area 304 can be accessed without authentication. However, to prevent unlawful analysis by any persons, the special area 304 may be made accessible only by such apparatus as having been
10 authenticated affirmatively, or commands used for accessing the special area 304 may be encrypted.

Now, changing the size of the authentication area 332 and the non-authentication area 331 will be described with reference to FIGs. 7B and 7C.

15 The total storage capacity of the authentication area 332 and the non-authentication area 331 in the flash memory 303 is equal to the capacity of $(XXXX+YYYY+1)$ sectors which is a fixed value obtained by subtracting the alternate block area 501 and others from all the storage areas in the flash memory 303.
20 The sizes of the areas 332 and 331 are each variable and can be changed by changing the boundary address value XXXX.

The first step in the procedure for changing the size of an area is to execute authentication. This authentication is executed to prevent any users from easily changing the size of
25 the area using one of standard equipment programs prevalent

5 changing the area size.

The memory card 109, on receiving the above dedicated command for changing the area size, stores the value XXXX in the nonvolatile storage area or the like in the memory card 109, then controls the succeeding accesses to the authentication area 332 and the non-authentication area 331 using the value XXXX as
10 a new boundary address. More specifically, the memory card 109 assigns physical sector 0 to XXXXth sector in the flash memory 303 to the non-authentication area 331, and XXXXth to (XXXX+YYYY)th sector to the authentication area 332. The access
15 control units 325 and 326 perform the address conversion between a logical address and a physical address, and monitors generation of an improper access to outside an allocated storage area. It should be noted here that logical addresses are recognized by an external apparatus as addresses in a data space
20 of the memory card 109, corresponding to the values used in the commands, and that the physical addresses are addresses in a data space of the flash memory 303 contained in the memory card 109.

If the authentication area 332 is increased in size
25 by reducing the boundary address, an arrangement will be

5 address, for example. With this arrangement, physical addresses correspond to the new logical addresses starting from the new boundary address. With this arrangement, the data space of the authentication area 332 is enlarged while logical addresses for the data stored in the authentication area 332 are maintained.

10 The dedicated command for changing the area size may be encrypted before use to prevent unlawful accesses.

FIG. 8 is a flowchart showing a procedure in which the PC 102 (or the player 201) writes a music content or the like to the memory card 109. In the following description, it is
15 supposed that the PC 102 writes music data to the memory card 109 (S601).

(1) The PC 102 executes a challenge-response-type authentication with the authentication unit 321 of the memory card 109 using the device key 111a and the like, and extracts the master key
20 323a from the memory card 109 when the authentication has been affirmative (S602).

(2) The PC 102 then extracts the medium ID 341 from the special area 304 in the memory card 109 using a dedicated command (S603).

25 (3) The PC 102 then generates a random number, and generates a

5 card 109 during the authentication process.

(4) The generated password is encrypted using the master key 323a and the medium ID 341, then is written to the authentication area 332 as the encryption key 425 (S605). By this time, before the data (encryption key 425) is transmitted, 10 the command to write data to the authentication area 332 has been encrypted and sent to the memory card 109.

(5) The music data is encrypted using the password and stored in the non-authentication area 331 as the encrypted content 426 (S606).

15 FIG. 9 is a flowchart showing a procedure in which a music content or the like is read out from the memory card 109 and played by the player 201 (or the PC 102). In the following description, it is supposed that music data stored in the memory card 109 is played by the player 201 (S701).

20 (1) The player 201 executes a challenge-response-type authentication with the authentication unit 321 of the memory card 109 using a device key 211a and the like, and extracts the master key 323a from the memory card 109 when the authentication has been affirmative (S702).

25 (2) The player 201 then extracts the medium ID 341 from the

5 109 (S704). By this time, before the data (encryption key 425)
is read out, the command to read out data from the
authentication area 332 has been encrypted and sent to the
memory card 109.

10 (4) The obtained encryption key 425 is decrypted using the
master key 323a and the medium ID 341 to extract a password
(S705). This decryption step is a reversed step of the
encryption step S605 shown in FIG. 8.

15 (5) The encrypted content 426 is read out from the non-
authentication area 331 and decrypted using the password
extracted in the step S705, while the decrypted content is
played as music (S706).

As described above, the music data stored in the non-
authentication area 331 in the memory card 109 cannot be
decrypted without the encryption key 425 stored in the
20 authentication area 332. Accordingly, even if only music data
is unlawfully copied to another memory card, the copied music
data cannot be normally played. With this construction, the
copyright of the music data is safely protected.

25 As also described above, only apparatuses that have
been authenticated affirmatively are permitted to access the

5 selectively using the device key, the encryption algorithm or
the like that are used for authentication.

In the above example, when an encrypted content is
written to the memory card 109, first the password used in the
encryption is encrypted using the master key and the medium ID,
10 then the encrypted password is stored in the authentication area
332 as the encryption key (S605). However, either the master
key or the medium ID may be used to encrypt the password. This
construction simplifies the encryption and provides a merit that
the circuit size of the memory card 109 or the player 102 is
15 reduced, although there is a possibility that the intensity of
the encryption is weakened.

In the above example, the player 201 and the PC 102
can extract the master key 323a from the memory card 109 only
when the authentication has been affirmative. However, the
20 master key 323a may be embedded in the player 201 or the PC 102
beforehand. Alternatively, the master key 323a may be encrypted
and stored in the special area 304 as an encrypted master key.

Now, two examples of the use of the authentication
area of the memory card will be described. In the two examples,
25 "the number of read-outs" and "the number of permitted digital

5 In the present example, the player 201 can play the music data stored in the non-authentication area 331 in the memory card 109 as an audio signal as many times as indicated by the number of read-outs 812 stored in the memory card 109 (S801).

(1) The player 201 executes a challenge-response-type authentication with the authentication unit 321 of the memory card 109 using a device key 211a and the like, and extracts the master key 323a from the memory card 109 when the authentication has been affirmative (S802).

(2) The player 201 then extracts the medium ID 341 from the special area 304 in the memory card 109 using a dedicated command (S803).

(3) The player 201 then extracts the encryption key 425 of the music data from the authentication area 332 in the memory card 109 (S804). By this time, before the data (encryption key 425) is read out, the command to read out data from the authentication area 332 has been encrypted and sent to the memory card 109.

(4) The player 201 then extracts the number of read-outs 812 from the authentication area 332 in the memory card 109, and checks the number of read-outs 812 (S804). When the number

5 reading out is allowed (S805), and the play process ends (S809).
When the number of read-outs 812 is a value other than 0 and
does not indicate allowance of limitless reading out, the player
201 reduces the number by one, writes the resultant number to
the authentication area 332 (S805), then plays the music in
10 accordance with the procedure (S704 to S706) shown in FIG. 9
(S806 to S808).

As described above, it is possible for the player 201
to control the number of times the player 201 plays the music by
prestoring the number of read-outs 812 which shows the number of
15 times the music can be played. This enables the present
technique to be applied to analog reproduction of music obtained
through, for example, rental CDs or kiosk terminals (online
vending machines for music distribution connected to a
communication network).

20 It should be noted here that "read-out time" may be
stored instead of the number of read-outs 812 to impose a
limitation on the total time the music content can be played.
Alternatively, combined information of the number of times and
a time may be stored instead. As another example, the number of
25 read-outs 812 may be reduced when the content is kept to be

5 the player 201 (or the PC 102) handles the number of permitted digital outputs 913 stored in the authentication area in the memory card 109. In the present example, the player 201 can read out the music data from the non-authentication area 331 in the memory card 109 and output the read digital music data as
10 many times as indicated by the number of permitted digital outputs 913 stored in the memory card 109 (S901).

(1) The player 201, as in the steps S701 to S705 shown in FIG. 9, executes an authentication with the memory card 109 to extract the master key 323a (S902), extracts the medium ID 341
15 (S903), extracts the encryption key 425 (S904), and extracts a password (S905).

(2) The player 201 then extracts the number of permitted digital outputs 913 from the authentication area 332 in the memory card 109, and checks the number of permitted digital outputs 913
20 (S906). When the number indicates allowance of limitless digital output, the player 201 reads out the encrypted content 426 from the non-authentication area 331, and decrypts the encrypted content 426 to digital data using the password extracted in the step S905 and outputs the decrypted digital
25 data from the digital output terminal 205 as digital music data

5 encrypted content 426 is read out from the non-authentication
area 331, and music is played while the content is decrypted
using the password (S908).

(4) When the number of permitted digital outputs 913 is a value
other than 0 and does not indicate allowance of limitless
10 digital output, the player 201 reduces the number by one, writes
the resultant number to the authentication area 332 (S907), then
reads out the encrypted content 426 from the non-authentication
area 331, decrypts the encrypted content 426 to digital data
using the password extracted in the step S905 and outputs the
15 decrypted digital data from the digital output terminal 205
(S909).

As described above, the number of digital outputs from
the player 201 can be controlled by storing the number of
permitted digital outputs 913 in the authentication area 332 in
20 the memory card 109. This enables the present technique to be
applied to digital reproduction of music obtained through, for
example, rental CDs or kiosk terminals, which is to say, digital
dubbing of music data stored in a memory card can be permitted
a certain times in the authority of the copyright owner.

25 It should be noted here that as with "the number of

5 number of permitted digital outputs and a time may be stored
instead. As another example, the number of permitted digital
outputs 913 may be reduced when the content is kept to be output
after a certain period (e.g., 10 seconds). As another example,
the number of permitted digital outputs 913 may be encrypted
10 then stored so that the information is protected from
tampering.

A function may be added so that the number of
permitted digital outputs can be increased by a number which is
specified by the copyright owner in correspondence to a charge
15 the copyright owner receives.

Now, the physical data structure (structure of the
sector and the ECC block) of the memory card 109 will be
described.

The memory card 109 adopts such a data structure as
20 is suitable for preventing unlawful acts related to the back up
or restoration of the data stored in the flash memory 303 and
for preventing unlawful acts related to the data tampering.
Such a data structure is adopted due to the necessity for
dealing with the unlawful operations that may be performed on
25 the above methods in which "the number of read-outs" or "the

5 after the whole data recorded in the flash memory 303 is backed
up to an external auxiliary storage apparatus of the like. By
doing this, when the number of permitted play operations becomes
0, the music can be repeatedly played again by restoring the
back up data. Also, the music may unlawfully be played
10 repeatedly by tampering the number of read-outs. As a result,
it is necessary to make some arrangement to prevent such
unlawful acts.

FIG. 12 shows a data structure which is common to the
authentication and non-authentication areas 332 and 331 of the
15 memory card 109, and also shows a flowchart of the
reading/writing process corresponding to the data structure.

In the present example, the counter value generated
by the random number generator 103 of the authentication unit
321 in the control IC 302 is used as a time-variant key.

20 A 16-byte extension area 1005 is assigned to each of
512-byte sectors 1004 in the flash memory 303. Each sector
stores data which has been encrypted using the counter value.
The extension area 1005 is composed of ECC data 1006 and a time-
variant area 1007. The ECC (Error-Correcting Code) data 1006 is
25 8-byte data being an ECC for the encrypted data stored in the

5 be accessed logically (i.e., using a public command or the like), and that only the extension area 1005 can be accessed physically (i.e., controlled by an apparatus that reads/writes data from/to the memory card).

10 With the above construction, unlawful data tampering can be prevented by comparing the sector data with the contents of the time-variant area 1007, where even if the sector data is tampered using a command or the like, the contents of the time-variant area 1007 do not change.

15 More specifically, the PC 102 or the player 201 writes/reads data to/from the authentication area 332 or the non-authentication area 331 in the flash memory 109 following the procedure shown below in units of sectors 1004. First, the procedure in which the PC 102 writes data to the memory card 109 (S1001) will be described.

20 (1) The PC 102 requests the memory card 109 to issue a counter value. In response to this request, the control IC 302 in the memory card 109 generates a random number using a random number generator 1003 contained in the control IC 302 (S1005), and sends the generated random number to the PC 102 as the counter
25 value (S1002).

5 password and sent to the memory card 109 (S1004). Together with the encrypted data, (i) information specifying the location of a sector to which the encrypted data is to be written, and (ii) the counter value used for the encryption are sent to the memory card 109.

10 (4) The memory card 109 writes the encrypted data to the specified sector 1004 (S1006).

(5) An ECC is obtained by calculation from the encrypted data, and the obtained ECC is written to the extension area 1005 as the ECC data 1006 (S1007).

15 (6) The counter value received together with the encrypted data is written to the time-variant area 1007 (S1008).

Next, the procedure in which the PC 102 reads out data from the memory card 109 (S1011) will be described.

(1) The PC 102 requests the memory card 109 to read out data by
20 specifying the location of a sector from which the data is to be read out. On receiving the request, the memory card 109 first reads out encrypted data from the specified sector 1004 and outputs the read-out data to the PC 102 (S1016). The PC 102 receives the encrypted data (S1012).

25 (2) The memory card 109 then reads out a counter value from the

5 (3) A password is generated from the read-out counter value and the master key 323a and the media ID 341 which have already been obtained (S1014).

(4) The encrypted data is decrypted using the password (S1005).

10 Here, if the data in the sector 1004 has been changed by tampering or the like, the decryption fails due to mismatch between the counter value read out from the time-variant area 1007.

15 As described above, the flash memory 303 contains the time-variant area 1007, a hidden area which cannot be seen (accessed) by users. Data is encrypted and stored using a password which is generated using a counter value stored in the time-variant area 1007. With this construction, the data is protected from unlawful tampering by users.

20 In the above example, the time-variant area 1007 is provided in the extension area 1005 for storing the ECC. However, it is possible to provide the time-variant area 1007 within another area in the flash memory 303 in condition that data stored in the area cannot be changed from outside the
25 memory card.

5 Now, a desirable example of a relationship between the logical addresses and physical addresses in the flash memory 303 will be described.

FIGs. 13A to 13D show a change in the relationship between the logical addresses and physical addresses. FIG. 13A shows the relationship before the change. FIG. 13B shows the relationship after the change. FIG. 13C shows a conversion table 1101 corresponding to FIG. A. FIG. 13D shows the conversion table 1101 corresponding to FIG. B.

The conversion table 1101 is a table in which all the logical addresses (in FIGs. 13A to 13D, serial numbers of the logical blocks) are stored with corresponding physical addresses (in FIGs. 13A to 13D, serial numbers of the physical blocks constituting the flash memory 303). The conversion table 1101 is stored in a nonvolatile area in the control IC 302 or the like and is referred to by the authentication area access control unit 325 or the non-authentication area access control unit 326 when, for example, a logical address is converted into a physical address.

Devices accessing the memory card 109 cannot write data to all the data storage spaces that physically exist in the

5 The above arrangement is made, for one reason, to
secure an alternative area which would replace an area from/to
which data cannot be read/written due to a partial defect of the
flash memory 303. Even if such a defect block has been replaced
by an alternative block, changing the conversion table so as to
10 reflect the change in the correspondence between the logical and
physical block numbers enables the flash memory 303 to pretend
against external devices that no defects have been caused. This
is because in each file, the logical continuity, which
corresponds to a plurality of continuous physical blocks, is
15 maintained.

 However, the fragmentation of logical blocks increases
when, for example, a file composed of a plurality of blocks is
repeatedly stored or deleted in/from the memory card 109. A
specific example of this is shown in FIG. 13A in which the
20 logical addresses (0 and 2) of the logical blocks constituting
"file 1" are discontinuous.

 When such discontinuity of logical blocks occurs, for
example, music data cannot be written to continuous logical
areas in the memory card 109. This necessitates issuance of the
25 write command "Write address count" for each block, resulting in

5 To solve the above problem, the control IC 302 of the
memory card 109 has a function to rewrite the conversion table
1101 based on a command issued from an external device. More
specifically, when a dedicated command for rewriting the
conversion table 1101 is input from a command pin, the control
10 IC 302 of the memory card 109 interprets the dedicated command
and rewrites the conversion table 1101 using a parameter that is
sent after the dedicated command.

The above operation will be detailed using an example
shown in FIGs. 13A to 13D. Suppose that before the above
15 dedicated command is received, the flash memory 303 contains
data constituting the file "file1" at locations indicated by
physical addresses 0 and 2, and data constituting the file
"file2" at a location indicated by physical address 1, as shown
in FIG. 13A, and that the conversion table 1101 shows that the
20 logical addresses match the physical addresses. That is to say,
in the logical addresses, as well as in the physical addresses,
the data of "file2" is sandwiched by the data of "file1".

With an intention of solving the above state, an
external device sends the above dedicated command and a
25 parameter to the flash memory 303, the dedicated command

5 relationship between the logical and physical addresses in the flash memory 303 after the above sequence of operations.

As understood from FIG. 13B, though the arrangement of the physical blocks has not been changed, the logical blocks constituting "file1" have been relocated to be successive. With
10 this arrangement, the external device can access "file1" at a higher speed than before in the next access and after.

The conversion table 1101 can be rewritten as above not only to solve the fragmentation of logical blocks, but also to change the size of each of the authentication area 332 and
15 non-authentication area 331 in the flash memory 303. In the latter case, a high-speed area relocation is possible since the conversion table 1101 is rewritten so that a physical block to become small is located as a physical block to become large.

Now, a function of the memory card 109 related to not-
20 deleted blocks will be described. More specifically, operations of the memory card 109 when receiving a not-deleted block list command and an delete command will be described. Here, the not-deleted blocks are physical blocks in the flash memory 303 which contain data that has not physically been deleted. That is to
25 say, data in the not-deleted blocks needs to be deleted at once

and execute, and is used to obtain a list of all the not-deleted blocks in the flash memory 303.

The existent data stored in the flash memory 303 of the memory card 109 must be deleted in units of blocks before data is newly written to the flash memory 303. The time for the deletion is approximately a half of the total time of writing. As a result, the total time of writing is reduced if the deletion has been completed beforehand. Accordingly, to achieve this, the memory card 109 provides the external device the not-deleted block list command and the delete command.

Suppose that the current use state of the logical blocks and physical blocks of the flash memory 303 is shown in FIG. 14A. As shown in FIG. 14A, logical blocks 0 to 2 are currently used, and physical blocks 0 to 2, 4, and 5 are not-deleted blocks.

A not-deleted block list 1203 is stored in the command judgement control unit 322 in the above state. The contents of the not-deleted block list 1203 corresponding to the use state of the blocks shown in FIG. 14A are shown in FIG. 14B. Here, the not-deleted block list 1203 is a storage table composed of entries corresponding to all the physical blocks constituting

FIG. 14C is a flowchart showing the procedure of the PC 102 or the player 201 for deleting blocks beforehand using the not-deleted block list command and the delete command in the above-stated states. It is presumed here that the flash memory 303 contains a table such as FAT (File Allocation Table) which shows the use state of the logical blocks, as shown in FIG. 14D.

An external device such as the PC 102 or the player 201 issues the not-deleted block list command to the memory card 109 during an idle time in which the memory card 109 is not accessed (S1201). On receiving the command, the command judgement control unit 322 of the memory card 109 refers to the not-deleted block list 1203 contained in the command judgement control unit 322, detects that physical blocks 0 to 2, 4, and 5 are assigned a state value "1", and sends the physical block numbers to the external device.

The external device then refers to the table that shows the use state of logical blocks in the flash memory 303 shown in FIG. 14D to identify the blocks that are not used logically (S1202).

5 (S1203). The external device then issues the delete command specifying the physical block numbers 4 and 5 to the memory card 109 (S1204). On receiving the command, the command judgement control unit 322 of the memory card 109 deletes the physical blocks 4 and 5 by sending instructions to the authentication
10 area access control unit 325 and the non-authentication area access control unit 326.

After the above operation is complete, data is written to the physical blocks 4 and 5 at a high speed since the deletion process is not required for the writing.

15 Now, a function of the memory card 109 related to personal data protection will be described. More specifically, the personal data protection function is used when the memory card 109 checks an external device for authentication and requires personal data of the user of the external device.
20 Here, each piece of the personal data is unique to a user and is used to identify the user. The user with proper personal data is recognized by the memory card 109 as an authorized user permitted to access the authentication area 332 in the memory card 109.

25 Here, if the user is requested to input the personal

user who has an authority to access the authentication area
332.

One possible solution to this problem would be
encrypting the personal data using a password provided by the
user personally and storing the encrypted personal data, in the
10 same way as music data.

However, in the above case, the user needs to input
the password each time the personal data is checked. The
procedure is troublesome and the management of the password is
also required. Accordingly, the memory card 109 provides a
15 function to sidestep the problem of unnecessarily and repeatedly
inputting the personal data.

FIG. 15 shows a communication sequence in an
authentication between the player 201 and the memory card 109
and also shows main components used in the authentication. Note
20 that the processes shown in FIG. 15 are mainly achieved by the
authentication circuit 216 of the player 201 and the
authentication unit 321 of the memory card 109.

As shown in FIG. 15, the authentication circuit 216
of the player 201 has the encryption and decryption functions,
25 and also prestores a master key 1301 which is a secret key being

5 the encryption, decryption, and comparison functions, and also
has two nonvolatile storage areas: a device ID group storage
area 1310 and a user key storage area 1311. The device ID group
storage area 1310 stores device IDs of all the devices permitted
to access the authentication area 332 in the memory card 109.
10 The user key storage area 1311 stores a user key sent from a
device as personal data.

The authentication procedure will be described in
detail below. Note that in the transmissions and receptions,
all the data is encrypted before transmission, and the encrypted
15 data is decrypted in the reception side. A key to be used in
the encryption and decryption is generated during the following
procedure.

(1) After the memory card 109 is connected to the player 201,
first, the player 201 encrypts the device ID 1302 using the
20 master key 1301, and sends the encrypted device ID 1302 to the
memory card 109.

(2) The memory card 109 decrypts the received encrypted device
ID 1302 using the master key 323a, and checks whether the
obtained device ID 1302 has already been stored in the device ID
25 group storage area 1310.

5 player 201 to send a user key.

(4) The player 201 urges the user to input the user key, obtains the user key as personal data of the user, and sends the obtained user key to the memory card 109.

10 (5) The memory card 109 compares the received user key with the user key having been prestored in the user key storage area 1311. When having judged that the two user keys match, or when the user key storage area 1311 is vacant, the memory card 109 notifies the player 201 that the authentication has been affirmative, and stores the device ID 1302 obtained in the above
15 step (3) in the device ID group storage area 1310.

With the above arrangement, when a device of the user is connected to the memory card 109 for the first time, the user is required to input personal data (a user key). However, in the second connection and after, the user is no more requested
20 to input the personal data since automaticall, the authentication completes affirmatively using the device ID.

Now, a variation of the authentication protocol between the memory card 109 and an external device such as the PC 102 or the player 201 will be described with reference to
25 FIGs. 16 and 17.

5 achieved by the authentication circuit 216 of the player 201, a
control program 111b of the PC 102, and the authentication unit
321 of the memory card 109. It is presumed here that the master
key storage unit 323 of the memory card 109 stores an encrypted
master key (encrypted master key 323), and that the special area
10 304 stores a secure medium ID 343 as well as the medium ID 341,
the secure medium ID 343 being generated by encrypting the
medium ID 341.

First, the player 201 issues a command to the memory
card 109 to obtain the master key 323b from the memory card 109,
15 and decrypts the obtained master key 323b using the device key
211a. The decryption algorithm used in this decryption
corresponds to the encryption algorithm used in the encryption
of the master key 323b which has now been read out from the
memory card 109. Therefore, when the device key 211a the player
20 201 has is an authorized one, the decryption is expected to
restore the original master key.

The player 201 then issues a command to the memory
card 109 to obtain the medium ID 341 from the memory card 109,
and encrypts the obtained medium ID 341 using the restored
25 master key. The encryption algorithm used in this encryption is

The player 201 and the memory card 109 performs a mutual authentication using the secure medium IDs they respectively have. Through this mutual authentication, each of the devices generates (OK/NG) information and a secure key, the (OK/NG) information indicating whether the remote device has been authenticated, and the secure key being a time-variant key that depends on the authentication result. The secure keys owned by both devices match only when both devices 201 and 109 affirmatively authenticate the other devices, and the secure keys change each time a mutual authentication is performed.

After a mutual authentication has completed affirmatively, the player 201 generates a command which is used to access the authentication area 332 in the memory card 109. More specifically, for example, when data is read out from the authentication area 332, a parameter (a 24-bit address "address" and an 8-bit count "count") of the command "SecureRead address count" is encrypted using the secure key, and an encrypted command, which is generated by combining the encrypted parameter and a tag (a 6-bit code indicating a command type "SecureRead") of the command, is sent to the memory card 109.

5 When the command is judged to be a command to access
the authentication area 332, the parameter contained in the
command is decrypted using the secure key obtained through the
mutual authentication. The decryption algorithm used in this
10 decryption corresponds to the encryption algorithm used in the
encryption of the command by the player 201. Therefore, when
the mutual authentication completes affirmatively, that is to
say, when the secure keys used by both devices match, the
parameter obtained by the decryption should be equal to the
original parameter used by the player 201.

15 The memory card 109 then reads out the encryption key
425 from a sector in the authentication area 332 indicated by
the decrypted parameter, encrypts the read-out encryption key
425 using the secure key, and sends the encrypted encryption key
to the player 201.

20 The player 201 decrypts the received data using the
secure key obtained through the mutual authentication. The
decryption algorithm used in this decryption corresponds to the
encryption algorithm used in the encryption of the encryption
key 425 by the memory card 109. Therefore, when the mutual
25 authentication completes affirmatively, that is to say, when the

key used in the command execution. With this arrangement, an external device attempting to access the authentication area 332 in the memory card 109 needs to perform a mutual authentication each time the external device issues a command and to be affirmative in the authentication beforehand.

10 FIG. 17 shows a communication sequence in a detailed procedure of the mutual authentication shown in FIG. 16. In the present example, the memory card 109 and the player 201 perform a challenge-response-type mutual authentication.

15 The memory card 109 generates a random number and sends the random number to the player 201 as challenge data to check the properness of the player 201. The player 201 encrypts the challenge data and returns the encrypted challenge data to the memory card 109 as response data to certify the properness of the player 201. The memory card 109 encrypts the random
20 number sent as challenge data, and compares the received response data with the encrypted challenge data. When the received response data and the encrypted challenge data match, the memory card 109 judges that the authentication of the player 201 has been affirmative (OK), and receives a command to access
25 the authentication area 332 from the player 201. When the

5 judgement, the memory card 109 rejects the command.

The player 201 performs a similar authentication procedure to check the properness of the memory card 109. That is to say, the player 201 generates a random number and sends the random number to the memory card 109 as challenge data to
10 check the properness of the memory card 109. The memory card 109 encrypts the challenge data and returns the encrypted challenge data to the player 201 as response data to certify the properness of the memory card 109. The player 201 encrypts the random number sent as challenge data, and compares the received
15 response data with the encrypted challenge data. When the received response data and the encrypted challenge data match, the player 201 judges that the authentication of the memory card 109 has been affirmative (OK), and accesses the authentication area 332 in the memory card 109. When the received response
20 data and the encrypted challenge data do not match, the player 201 judges that the authentication of the memory card 109 has not been affirmative (NG), and gives up accessing the authentication area 332.

All the encryption algorithms used in the mutual
25 authentication should be the same as far as the memory card 109

the propriety. The obtained secure key, or the result of the above exclusive-or operation, is used for accessing the authentication area 332 in the memory card 109. With this arrangement, it is possible for both devices 109 and 201 to share a time-variant secure key that is common to them only when they have been affirmative in the authentication. This renders the affirmative authentication a necessary condition for accessing the authentication area 332.

The secure key may be a result of an exclusive-or operation using the encrypted challenge data, the response data, and the secure medium ID.

Now, a variation of a function to change the boundary between the authentication area 332 and non-authentication area 331 in the memory card 109 will be described with reference to FIGs. 18 and 19.

FIGs. 18A to 18C show the use state of the flash memory 303 before the boundary is changed. FIG. 18A is a memory map showing the construction of the physical blocks in the flash memory 303.

FIG. 18B shows a conversion table 1103 which is dedicated to the non-authentication area 331 and is stored in a

5 control unit 326 refers to the conversion table 1103 to convert
a logical address into a physical address or to detect an
improper access accessing outside an allocated storage area.

FIG. 18C shows a conversion table 1102 which is
dedicated to the authentication area 332 and is stored in a
10 nonvolatile storage area in the authentication area access
control unit 325. The conversion table 1102 shows relationships
between the logical blocks and physical blocks in the
authentication area 332. The authentication area access control
unit 325 refers to the conversion table 1102 to convert a
15 logical address into a physical address or to detect an improper
access accessing outside an allocated storage area.

As shown in FIG. 18A, before the boundary is changed,
out of the flash memory 303 composed of physical blocks 0000 to
FFFF, physical blocks F000 to FFFF are allocated to the
20 alternate block area 501, physical blocks 0000 to DFFF whose
addresses are lower than the boundary are allocated to the non-
authentication area 331, and physical blocks E000 to FFFF whose
addresses are higher than the boundary are allocated to the
authentication area 332.

25 As understood from the conversion table 1103 shown in

5 numbers and the physical block numbers in the authentication
area 332. That is to say, logical blocks 0000 to 0FFF
correspond to physical blocks EFFF to E000, respectively. This
arrangement has been made by considering that the logical blocks
are used in ascending order, and that when the boundary is
10 moved, data in the physical blocks to be moved needs to be saved
or moved.

FIGs. 19A to 19C show the use state of the flash
memory 303 after the boundary is changed. FIGs. 19A to 19C
correspond to FIGs. 18A to 18C, respectively. Note that the
15 boundary change is achieved by the following procedure:

(1) A dedicated command specifying an address of the boundary is
input to the command judgement control unit 322 via a command
pin; and

(2) The command judgement control unit 322 rewrites the
20 conversion table 1102 in the authentication area access control
unit 325 and the conversion table 1103 in the non-authentication
area 331.

As shown in FIGs. 19A to 19C, the boundary is moved
from between the physical blocks E000 and DFFF to between the
25 physical blocks D000 and CFFF. That means the size of the non-

5 change, the size of the conversion table 1103 of the non-
authentication area 331 is reduced by 1000(hex) entries, and the
size of the authentication area 332 is increased by 1000(hex)
entries, so that the conversion table 1103 shows logical blocks
0000 to CFFF with corresponding physical blocks 0000 to CFFF.
10 In contrast, as shown in FIG. 19C, the size of the conversion
table 1102 of the authentication area 332 is increased by
1000(hex) entries, and the size of the authentication area 332
is increased by 1000(hex) entries, so that the conversion table
1102 shows logical blocks 0000 to 1FFF with corresponding
15 physical blocks EFFF to D000.

As described above, a boundary is set between the
authentication area and the non-authentication area in the flash
memory 303, and the size of both areas is changed by moving the
boundary. This enables the memory card 109 to be used for
20 various purposes. For example, the memory card 109 may be
mainly used for storing digital contents which need to be
protected by copyright, or the memory card 109 may be mainly
used for other than storing such digital contents.

In both the authentication area and the non-
25 authentication area, the amount of processing in moving and

physical blocks is easily achieved when the conversion table 1102 dedicated to the authentication area 332 and the conversion table 1103 dedicated to the non-authentication area 331 are separately provided.

10 In the above example, in the authentication area 332, there is an inverse relationship between the logical addresses and the physical addresses in units of blocks. However, other units may be used. For example, there may be an inverse relationship between the logical addresses and the physical
15 addresses in units of sectors or bytes.

Up to this point, the memory card of the present invention has been described in its embodiment and variations. However, the present invention is not limited to the embodiment and variations.

20 In the above embodiment, the PC 102 or the player 201 is required to perform a mutual authentication with the memory card 109 using the same procedure each time it issues a command to access the authentication area 332 in the memory card 109. However, a simplified authentication procedure may be used to
25 access the authentication area 332, depending on the command

105 may execute the write command successfully. With this a one-way authentication (an authentication of a device by the memory card 109) completes affirmatively. With this arrangement, commands which are little related to the copyright protection will be executed at high speed.

10 The flash memory 303 in the memory card 109 of the present invention may be replaced with another storage medium (e.g., a nonvolatile medium such as a hard disk, an optical disc, and a magnet optical disc). A portable storage card capable of securing a copyright on the stored data as the
15 present invention can be achieved using any of such mediums.

INDUSTRIAL APPLICABILITY

As understood from above description, the semiconductor of the present invention is suitable for use as a record medium for recording music contents via an electronic
20 music distribution using a network such as the Internet. The semiconductor of the present invention is also suitable for use as a record medium for recording computer programs or data, and is especially suitable for use as a small record medium for a portable recording/reproducing apparatus.

a control circuit (302) which controls accesses by the electronic device to an authentication area (332) and a non-authentication area (331) in the rewritable nonvolatile memory,

wherein the control circuit (302) includes:

a non-authentication area access control unit (326) which controls accesses by the electronic device to the non-authentication area (331),

an authentication unit (321) which performs an authentication process to check whether the electronic device has authority to access the semiconductor memory card (109), and affirmatively authenticates the electronic device when the electronic device has authority to access the semiconductor memory card (109), and

an authentication area access control unit (325) which permits the electronic device to access the authentication area (332) only when the authentication unit affirmatively authenticates the electronic device.

the semiconductor memory card (109) further comprises:

means for holding an address marking a boundary between the authentication area (332) and the non-authentication area (331), and

an area resizing circuit (322, 325, 326) which resizes the authentication area (332) and the non-authentication area (331), wherein the area resizing circuit (322, 325, 326) resizes the authentication area (332) and the non-authentication area (331) by changing the boundary marking address, and

the authentication area access control unit (325) and the non-authentication area access control unit (325) control accesses by the electronic device to the authentication area (332) and the non-authentication area (331) by referring to the boundary marking address.

2. A semiconductor memory card of Claim 1, wherein the authentication unit (321) generates a key reflecting a result of the authentication process, and the authentication area access control unit (325) decrypts an encrypted instruction using the key generated by the authentication unit (321), and controls accesses by the electronic device to the authentication area (332) in accordance with the decrypted instruction,

response type mutual authentication with the electronic device, and generates the key from challenge data and response data, the challenge data being sent to the electronic device to check whether the electronic device has authority to access the semiconductor memory card, and the response data being generated to show the authentication unit (321) has authority to access the semiconductor memory card.

4. A semiconductor memory card of Claim 3, wherein the encrypted instruction sent from the electronic device includes a tag field and an address field, the tag field not having been encrypted and specifying a type of an access to the authentication area (332), the address field having been encrypted and specifying an address of an area to be accessed, wherein

the authentication area access control unit (325) decrypts the address field using the key, and controls accesses by the electronic device to the authentication area (332) so that an access of the type specified in the tag field is made to the area indicated by the address in the decrypted address field.

5. A semiconductor memory card of Claim 4 further comprising:

an identification data storage circuit (304) which

the authentication unit (321) performs a mutual authentication with the electronic device using the identification data (341) stored in the identification data storage circuit (304) and generates the key from the identification data (341).

6. A semiconductor memory card of Claim 1, wherein the area resizing circuit (322, 325, 326) includes:

an authentication area conversion table (1102) which shows correspondence between logical addresses and physical addresses in the authentication area (332),

a non-authentication area conversion table (1103) which shows correspondence between logical addresses and physical addresses in the non-authentication area (331), and

a conversion table change unit (322) which changes contents of the authentication area conversion table (1102) and the non-authentication area conversion table (1103) in accordance with an instruction from the electronic device, wherein

the authentication area access control unit (325) controls accesses by the electronic device to the authentication area (332) by referring to the authentication area conversion table (1102), and

7. A semiconductor memory card of Claim 6, wherein an area addressed with higher physical addresses and an area addressed with lower physical addresses both constituting the area having the predetermined size are respectively allocated to the authentication area (332) and the non-authentication area (331), the non-authentication area conversion table (1103) shows correspondence between logical addresses arranged in ascending order and physical addresses arranged in ascending order, and the authentication area conversion table (1102) shows correspondence between logical addresses arranged in ascending order and physical addresses arranged in descending order.

8. A semiconductor memory card of claim 1 further comprising a read-only memory circuit which prestores data.

9. The semiconductor memory card of Claim 1, wherein the control circuit (302) further includes:

a conversion table (1102, 1103) which shows correspondence between logical addresses and physical addresses in each of the authentication area (332) and the non-authentication area (331), and

the non-authentication area access control unit (326) control accesses by the electronic device to the authentication area (332) and the non-authentication area (331), respectively, by referring to the conversion table.

10.A semiconductor memory card of Claim 1, wherein the control circuit (302) further includes:

an encryption/decryption unit (327) which encrypts data to be written to the authentication area (332) and the non-authentication area (331) and decrypts data read out from the authentication area (332) and the non-authentication area (331).

11.A semiconductor memory card of Claim 1, wherein the nonvolatile memory (303) is a flash memory, and the control circuit (302) further includes:

a not-deleted list holding unit (322) which holds a non-deleted list that shows a list of not-deleted areas in the authentication area (332) and the non-authentication area (331), and

a not-deleted area sending unit (322) which, in accordance with an instruction from the electronic device, refers to the not-deleted list to identify not-deleted areas in the authentication area (332)

authentication unit (321) requests a user of the electronic device to input a user key, which is information unique to the user, during the authentication process, and the control circuit (302) further includes:

a user key storage unit (1311) which stores the user key,

an identification information storage unit (1310) which stores a piece of identification information identifying an electronic device that has been affirmatively authenticated by the authentication unit (321), and

a user key request prohibition unit (321) which obtains a piece of identification information from a target electronic device after the authentication unit (321) starts the authentication process, checks whether the piece of identification information obtained from the target electronic device has already been stored in the identification information storage unit, and prohibits the authentication unit (321) from requesting a user of the electronic device to input a user key when the piece of identification information obtained from the target electronic device has already been stored in the identification information storage unit.

the non-authentication area (331) of the semiconductor memory card, and information 812) indicating the number of times the digital content can be read out being prestored in the authentication area (332), the data reading apparatus comprising:

a judgement means (S804) for, when the digital content is to be read out from the non-authentication area (331), reading out the information indicating the number of times the digital content can be read out from the authentication area (332), and judging whether the digital content can be read out based on the number of times indicated in the information, and

a reproduction means (S806-S808) for reading out the digital content from the non-authentication area (331) only when the judgement means judges that the digital content can be read out, and reducing the number of times the digital content can be read out in the information stored in the authentication area (332).

14.A storage system containing a semiconductor memory card according to claim 1 and a data reading apparatus (201) reading out a digital content (426) of the semiconductor memory card and reproducing the digital content as an analog signal the digital content, having been stored in the non-authentication area (331) of the semiconductor

a reproduction means (S908) for reading out the digital content from the non-authentication area (331) and reproducing the read-out digital content as an analog signal,

a judgement means (S906) for reading out the information indicating the number of times the digital content can be digitally output by the electronic device, and judging whether the digital content can be digitally output based on the number of times indicated in the information, and

a digital output means (S907, S909) for digitally outputting the digital content only when the judgement means judges that the digital content can be digitally output, and reducing the number of times the digital content can be digitally output in the information stored in the authentication area (332)