Recordable storage medium with protected data area

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 292 946 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
02.03.2005 Bulletin 2005/09

(21) Application number: **01938199.5**

(22) Date of filing: **08.05.2001**

(51) Int Cl.7: **G11B 20/00**

(86) International application number:
PCT/EP2001/005195

(87) International publication number:
WO 2001/095327 (13.12.2001 Gazette 2001/50)

(54) **RECORDABLE STORAGE MEDIUM WITH PROTECTED DATA AREA**

BESCHREIBBARES SPEICHERMEDIUM MIT GESCHÜTZTEM DATENBEREICH

SUPPORT DE STOCKAGE ENREGISTRABLE AVEC ZONE DE DONNEES PROTEGEE

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

(30) Priority: **02.06.2000 EP 00201951**

(43) Date of publication of application:
19.03.2003 Bulletin 2003/12

(60) Divisional application:
04103756.5 / 1 492 107

(73) Proprietor: **Koninklijke Philips Electronics N.V.**
5621 BA Eindhoven (NL)

(72) Inventors:
- **LINNARTZ, Johan, P., M., G.**
  NL-5656 AA Eindhoven (NL)
- **KALKER, Antonius, A., C., M.**
  NL-5656 AA Eindhoven (NL)
- **TALSTRA, Johan, C.**
  NL-5656 AA Eindhoven (NL)

(74) Representative:
Deguelle, Wilhelmus Hendrikus Gerardus
Philips
Intellectual Property & Standards
P.O. Box 220
5600 AE Eindhoven (NL)

(56) References cited:
EP-A- 0 593 305
EP-A- 0 984 346
EP-A- 0 997 899
US-A- 5 752 009
US-A- 5 761 301
US-A- 5 982 886
US-A- 6 028 936

EP 1 292 946 B1

Description

[0001] The invention relates to a method of storing data on a rewritale data storage medium, to a storage medium, to a recording apparatus for storing data on a rewritable data storage medium and to a playback apparatus for playback of user data stored on a rewritable data storage medium.

[0002] The invention addresses a storage medium on which users can store copyrighted and copy-free material. Often the user has a right to store and copy content, but there are restrictions to the number of (generations of) copies that he can make. Encryption is used to ensure that copy-righted content can only be interpreted by "compliant" devices which adhere to copy protective restrictions. A further protection is needed to avoid that non-compliant devices can make a bitwise copy of encrypted data. This is often avoided by storing essential information, e.g. a decryption key, in a manner that can not be copied.

[0003] More generally it is concluded that copy-protective measures require that on recordable discs some data must be stored which shall not be modifiable or erasable by consumer end products. These data will be called "system data" in the following. Examples of "system data" are:

- a unique disc identifier number which is used to encrypt the data that the user stores on the disc,
- a list consisting of a single key which has been encrypted with a number of different manufacturer-specific or device-specific keys,
- a list of electronic serial numbers of revoked devices or revoked discs. By storing such a list on all blank discs, revocation instructions can be disseminated to consumer devices. Upon receipt of such revocation instructions, compliant devices refuse to communicate with revoked devices.

[0004] Content or data recorded by the user will be called "user data" in the following. Moreover, the term "fixed data area" will be used for an area of the storage medium in which any information is stored that is read-only and not modifiable by consumer devices. On the contrary, in the "recordable data area" information is stored which can be modified by consumer devices. Also data, which can only be written by consumer devices after some modifications ("hacks") have been made to the device by malicious users will be stored in the recordable data area. Such modifications can be a change in the firmware or software used to control the recorder.

[0005] To store data in the fixed data area requires the use of components which are typically not available in consumer devices. An example of a technique to store such data is a "wobble", which is a radial deviation of the pit positions or the pregroove from a perfect spiral. Laws of physics and mechanics prohibit that such a wobble can be written on the fly by a laser as available in a consumer recorder for optical discs. Other examples of data stored in the fixed data area are the BCA code, proposed for DVD-ROM, selectively damaged spots on the disc material burned by high power lasers, or data stored in a special area of the disc which contains read-only material.

[0006] A practical problem is the storage of large quantities of data in the fixed data area. Typically the capacity is limited to a few (hundreds of) bits. Meanwhile the amount of system data that needs to be stored may well exceed the storage capacity available in the fixed data area.

[0007] The invention has therefore for its object to provide a method of storing data on a rewritable data storage medium according to which the above mentioned problems are overcome and which allows the storage of large quantities of system data in a tamper-resistant manner. Further, a corresponding storage medium, a corresponding recording apparatus and a corresponding playback apparatus shall be provided.

[0008] These objects are achieved according to the invention by a method as set forth in claim 1 or 9, by a storage medium as set forth in claim 10 or 14, by a recording apparatus as set forth in claim 19 or 20 and by a playback apparatus as set forth in claim 21 or 22.

[0009] The invention is mainly based on the idea that there exists some cryptographic relationship between data stored in the fixed data area and system data. This relationship is made up by the cryptographic summary which is according to the invention generated from the system data alone or from both the system data and identification data which can be a random number stored in the fixed data area. This cryptographic summary is used by a recording or playback apparatus to detect whether the system data have been tampered with, e.g. erased or modified in order to manipulate the copy proctection of the storage medium. The cryptographic summary is thus used for verification of the system data which means that in case of a verification failure playback or recording of the content of the storage medium can be stopped.

[0010] According to a first solution the system data are written in the recordable data area, e.g. as part of the formatting of the storage medium. A cryptographic summary, e.g. a cryptographic hash, is computed over the system data, and the result of that cryptographic summary, e.g. the result of that hash, is stored in the fixed data area. A recording apparatus will then only accept a storage medium with a valid combination of system data and fixed data, i.e. cryptographic summary.

[0011] According to an alternative solution identification data, e.g. a random number, are created and stored in the fixed data area. The recordable data area then contains the user data, the system data and a cryptographic summary of the system data and the identification data, e.g. an electronic signature thereof. A recording or playback apparatus will then use a verifier (e.g. a public key) to check the validity of the cryptographic

summary, the system data and the identification data, i. e. the validity of the signature will be checked. Instead of using an electronic signature a message authentication code (MAC) can be used for the verification which is cheaper but less secure.

[0012] EP-A-0984346 describes a copy protection scheme suitable for DVDs, according to which a disk comprises an identification area located in on a read-only part of the disk and a data area. In the identification area a possibly unique medium identifier is present, while in the data area Copy Control Information is present, which together with the medium identifier allows a reading apparatus to determine whether the disk is original or has been unlawfully copied. The Copy Control Information may be for example a copy of the identifier or a hashed version of it. This copy protection scheme rests on the fact that an apparatus available to the end user is not capable of modifying the identifier present in the identification area, and therefore a bit-by-bit copied disk can easily be discovered.

[0013] Other preferred embodiments of the invention are disclosed in the dependent claims.

[0014] The invention and preferred embodiments thereof are explained hereinafter in more detail with reference to the following drawings in which

Fig. 1 shows a recording method according to a first embodiment,
Fig. 2 shows a playback method according to a first embodiment,
Fig. 3 shows a recording method according to a second embodiment,
Fig. 4 shows a playback method according to the second embodiment,
Fig. 5 shows a recording method according to a third embodiment and
Fig. 6 shows a playback method according to the third embodiment.

[0015] Figure 1 shows a diagram explaining the method of storing data on a rewritable data storage medium according to a first embodiment of the invention. The storage medium 1, which can be a disc for optical recording of data, e.g. at DVD or a CD, is separated into a read-only fixed data area 2 and a recordable data area 3, 4 which is subdivided into a system data area 3 and a user data area 4. Data stored in the fixed data area 2 can not be modified by consumers. A typical implementation of the fixed data area 2 is the pressing of pits into a rewritable disc, i.e. part of the rewritable disc is used as a CD-ROM or DVD-ROM medium. Another implementation is the BCA (Burst Cut Area), a barcode pattern at the very inner radius of the disc, written by a YAG laser in the disc-factory. A third implementation is to store the fixed data in the radial displacement of the pre-pressed pits ("pit-wobble") or the radial displacement of the pre-groove ("pre-groove wobble").

[0016] Data stored in the recordable data area 3, 4 can be modified by a consumer. Nevertheless, the system data area is reserved for system data like copy protection information as outlined at the beginning. The largest part 4 of the recordable data area can be used for a storing user data, e.g. audio or video data.

[0017] Since the capacity of the fixed data 2 area is limited, but a growing amount of system data shall be stored but shall not be modifiable, the invention proposes to store the system data in the recordable data area 3 and to install a cryptographic relationship between the system data and a specific information stored in the fixed data area 2 which can not be modified during subsequent recording or replay. Therefore a cryptographic summary of the system data is computed by the generating means 5, which compute a hash of the system data in this embodiment. The cryptographically secure result of that hash is then stored in the fixed data area 2.

[0018] The method described in Fig. 1 is preferably implemented on a recording apparatus for storing the system data and the cryptographic summary on an empty medium using the same or separate recording means.

[0019] In the playback apparatus as shown in figure 2 a hash of the system data stored in the system data area 3 is computed by similar generating means 5 contained in the playback apparatus. The result of that computation is forwarded to verifying means 6 in the playback apparatus which also receive the cryptographic summary read from the fixed data area 2 of the medium 1. If this cryptographic summary equals the result of the hash computation the verification is successfull and the playback of user data can start or continue whereas after a verification failure the playback can be stopped since the probabilty is high that the system data have been manipulated. Reading means for reading the system data and the cryptographic summary from the medium are not shown.

[0020] In a pratical realization the medium 1 can be imagined as an (at first empty) DVD-RAM or a CD-RW or some other rewritable medium which is sold and contains a list of serial-numbers of known pirated recorders, hereafter referred to as 'naughty' recorders already, written in the disc factory. The list is used by honest players of DVD-RAM/CD-RW or the other media to refuse to playback recordings of these naughty recorders, because they have been known to be involved in illegal copying. Such a list is usually too long (typically more than one MB) to store in a fixed data area (typically a few hundreds of bits). Therefore the list is written like a normal file on the rewritable medium in the factory. To prevent that anybody just erases or modifies this list, the hash of this list is computed. This hash is much shorter than the system data and can therefore easily be written into the fixed data area during the production of the medium. The honest player then would first, upon insertion of the medium, compute the hash of the system data and check the result with the hash stored in the fixed data area. If they don't match, the system data has been tampered with.

[0021] In this basic form no cryptographic secret (e.g. a cryptographic key) has to be used anywhere in the system. A disadvantage is, however, the lack of flexibility. This means that the actual bit-content of the fixed data area on the rewritable medium is fixed forever at the time of the production of the disc in the factory. Thus, the hash has to be computed of the system data that shall be protected prior to production of the disc. If the system data shall be changed, e.g. by adding more naughty recorders to the list, the hash necessarily also changes. New media then have to be produced by the factory, because the old ones no longer have the correct hash for the new system data. There are also other reasons why the system data shall be changed or updated at a time after the production of the disc and fixing of the hash.

[0022] More flexibility is achieved in a second embodiment of the invention as shown in figures 3 and 4. According to this embodiment identification data, e.g. a random number, is stored in the fixed data area during production of the medium. The system data area is subdivided into a first area 31 for the actual system data and a second area 32 for storing a cryptographic summary. This cryptographic summary is generated by using a public key signature algorithm computed in the generating means 7. Therein a digital signature of the identification data and the system data which are at first hash-coded by the generating means 5 is computed using a secret private key $K_{private}$. This computation can also be written as

ED = E (hash (system data, identification data), private key)

wherein ED means extra data (=cryptographic summary) and E means the public-key encryption. The computed digital signature is then stored as cryptographic summary in the second system data area 32.

[0023] In a replay apparatus or a recording apparatus as shown in figure 4 the system data are verified by at first computing the hash over the identification data and the system data and then using the public key signature verification algorithm in verifying means 8 and the public key K_{public} to check the validity of the signature stored in the data area 32. The private key used for producing the digital signature in figure 3 must be kept secret, while the public key used for verification in the playback or the recording apparutus as shown in figure 4 can be distributed freely, because this public key is useless in the encryption step as described in figure 3.

[0024] A third embodiment is explained with reference to figures 5 and 6. As in the second embodiment identification data are stored in a fixed data area 2 and the actual system data are stored in a system data area 31. For encryption the cryptographic summary which shall be stored in the system data area 32 is generated by the generating means 9 from the identification data and the system data using a message authentication code algorithm (MAC algorithm) and a secret MAC key. This MAC-encryption can be in short written as

ED = E (system data, fixed data, MAC-key)

wherein ED means extra data (=cryptographic summary) and E means MAC-encryption.

[0025] In the recording or playback apparatus as shown in figure 6 corresponding generating means 9 are provided for computing the message authentication code from the identification data and the system data using the same secret MAC-key. The computed MAC is compared in a verifying means 6 with the cryptographic summary (the MAC) stored in the system data area 32 for verification reasons.

[0026] Compared to the second embodiment shown in figures 3 and 4 the use of the MAC is less secure than the use of the public-key signature. The key used to compute the MAC is present in every playback apparatus in the system, if someone breaks open any single player and gets hold of the key, this person can go ahead and replace the system data by other system data that still certify the MAC in the fixed data area. In contrast, in the public-key system of the second embodiment a secret private key is used in the encryption process whereas a published public key is used for verification.

[0027] By use of the invention it can be prevented that system data are manipulated. By storing special data in the fixed data area malevolent recorders can be prevented from copying old valid system data to new media, e.g. to replace a new large list of naughty recorders by an old short one. Since the system data itself are stored in the recordable data area the problem of limited capacity of the fixed data area is overcome.

[0028] Typically system data is stored or hidden in an area that is inaccessible to the user, or an area of the medium, where it doesn't interfere with the usual purpose of the disc, i. e. with user data storage. For DVD and CD media an example would be the so-called 'lead-in' and 'lead-out' areas of the disc. Hereafter such areas will collectively be referred to as 'corner area'. This has the advantage that it doesn't bother the user, and it also generally makes the production process much cheaper since corner areas can be stamped very fast, whereas recordable data have to be recorded at normal speed. In general players are much cheaper and simpler than recorders, so it is a relatively larger burden to players than to recorders to read out the system data in the corner area of the medium. So it makes sense to have the recorder, upon first use of the medium, read out the system data and copy its information to the main user data area in the recordable data area. The player can then just find the system data information in the main user data area which it can read anyway. A problem is that the player can not trust the recorder since the latter might not faithfully copy the system data. If, however, as according to the first embodiment of the invention a hash of the system data is stored in the fixed data area, the player can then verify that the incarnation of the system data in the main user data area agrees with the hash in the fixed data area. The recorder obviously can then not have manipulated the fixed data area.

[0029] It shall be noted that everytime any detail of the invention is described with reference to a playback apparatus the playback apparatus can be substituted by a recording apparatus. Both may comprise appropriate reading and/or recording means for reading and/or recording of data from or to the medium. Further, it shall be understood that the storage medium, the recording apparatus and the playback apparatus as set forth in the claims can be developed further in the same or a corresponding way as described above and as set forth in the subclaims with reference to the method of storing data.

Claims

1. Method of storing data on a rewritable data storage medium (1) comprising a read-only fixed data area (2) and a recordable data area (3,4), in which method system data are stored in the recordable data area (3), **characterized in that**

   - a cryptographic summary of the system data is generated and stored in the fixed data area (2), and
   - the cryptographic summary is used for verification of the system data before reading and/or recording of user data.

2. Method as set forth in claim 1, **characterized in that** the recordable data area (3,4) comprises a corner area and the system data are stored in the corner area.

3. Method as set forth in claim 1, **characterized in that** a hash function (5) is used for generating the cryptographic summary and for verifying the system data.

4. Method as set forth in claim 1, **characterized in that** a message authentication code algorithm is used for generating the cryptographic summary and for verifying the system data.

5. Method as set forth in claim 1, **characterized in that** a key signature algorithm is used for generating the cryptographic summary and for verifying the system data and that a signature is stored as cryptographic summary.

6. Method as set forth in claim 1, **characterized in that** the cryptographic summary is generated and the system data are stored in the recordable data area (3) as part of the formatting of the storage medium (1).

7. Method as set forth in claim 1, **characterized in that** copy protection information is stored as system data, in particular a unique storage medium identifier, a key encrypted by one or more different manufacturer-specific or device-specific keys or one or more lists of revoked devices or revoked storage mediums.

8. Method as set forth in claim 1, **characterized in that** the system data is originally stored in a corner area of the recordable data area (3) and that during first use of the storage medium (1) in a recording apparatus the system data are copied to a user data area (4) of the recordable data area (3,4).

9. Method of storing data on a rewritable data storage medium (1) comprising a read-only fixed data area (2), **characterized in that**

   - the read-only fixed data area comprises a first data area and a corner area,
   - system data are stored in the corner area,
   - a cryptographic summary of the system data is generated and stored in the first data area, and
   - the cryptographic summary is used for verification of the system data before reading and/or recording of user data.

10. Rewritable storage medium (1) for storing data, comprising:

    - a recordable data area (3,4) in which system data are stored, and
    - a read-only fixed data area (2), **characterized in that** in the read-only fixed data area (2) a cryptographic summary of the system data is stored, the cryptographic summary being provided for verification of the system data before reading and/or recording of user data.

11. Storage medium (1) as set forth in claim 10, **characterized in that** the recordable data area (3,4) comprises a corner area and the system data are stored in the corner area.

12. Storage medium as set forth in claim 11, **characterized in that** the storage medium comprises a lead-in, the corner area being situated in the lead-in.

13. Storage medium (1) as set forth in claim 10, **characterized in that** the storage medium (1) is a rewritable optical storage medium, in particular a CD or a DVD.

14. Rewritable storage medium (1) for storing data, comprising a read-only fixed data area (2), **characterized in that** the read-only fixed data area comprises a first data area and a corner area in which system data are stored, and a cryptographic summary of the system data is stored in the first data area, the cryptographic summary being provided for

verification of the system data before reading and/or recording of user data.

15. Storage medium as set forth in claim 14, **characterized in that** the first data area is a Burst Cut Area and the corner area comprises a pit-wobble and/or a pre-groove wobble.

16. Storage medium as set forth in claims 14, **characterized in that** the first data area is a Burst Cut Area and the corner area comprises prepressed pits.

17. Storage medium as set forth in claim 10 or 14, **characterized in that** the cryptographic summary of the system data comprises the result of a hash of the system data.

18. Method for verification of system data present on a rewritable data storage medium (1) before reading and/or recording of user data, the rewritable data storage medium (1) comprising a read-only fixed data area (2) and a recordable data area (3,4), **characterized in that**

- the system data and a cryptographic summary of the system data, which cryptographic summary is stored in the read-only fixed data area, are read,
- a cryptographic summary of the system data read from the medium is generated, and,
- the cryptographic summary read from the medium and the cryptographic summary generated are compared.

19. Recording apparatus for storing data on a rewritable data storage medium (1) comprising recording means for storing system data in a recordable data area (3) of the medium, **characterized in that** generating means (5) are present for generating a cryptographic summary of the system data, and the recording means are suitable for storing the cryptographic summary in a read-only fixed data area (2) of the medium (1), the cryptographic summary being provided for verification of the system data before reading and/or recording of user data.

20. Recording apparatus for storing data on a rewritable data storage medium (1) comprising a read-only fixed data area (2), **characterized in that**

- the read-only fixed data area comprises a first data area and a corner area,
- recording means are present for storing system data in the corner area, and for storing a cryptographic summary of the system data in the first data area, the cryptographic summary being provided for verification of the system data before reading and/or recording of user data, and
- generating means (5) are present for generating the cryptographic summary of the system data.

21. Playback apparatus for playback of user data stored on a rewritable data storage medium (1) comprising reading means for reading system data stored in the recordable data area (3,4) of the medium (1), **characterized in that** the reading means are also suitable for reading a cryptographic summary of the system data stored in a read-only fixed data area (2) of the medium (1), and verifying means (5,6) are present for generating a cryptographic summary of the system data read from the medium (1) and for verification of the system data by use of the generated cryptographic summary.

22. Playback apparatus for playback of user data stored on a rewritable data storage medium (1) comprising a read-only fixed data area (2), **characterized in that** the read-only fixed data area comprises a first data area and a corner area, and the playback apparatus comprises:

- reading means for reading system data stored in the corner area, and for reading a cryptographic summary of the system data stored in the first data area (2), and
- verifying means (5,6) for generating a cryptographic summary of the system data read from the medium (1), and for verification of the system data by use of the generated cryptographic summary.

23. Playback apparatus as set forth in claims 21 or 22, **characterized by** further comprising recording means for recording the user data on the rewritable data storage medium (1).

Patentansprüche

1. Verfahren zum Speichern von Daten auf einem wiederbeschreibbaren Datenspeichermedium (1) mit einem nur lesbaren festen Datenbereich (2) und einem beschreibbaren Datenbereich (3, 4), bei welchem Verfahren Systemdaten in dem beschreibbaren Datenbereich (3) gespeichert werden, **dadurch gekennzeichnet, dass**

- eine kryptographische Zusammenfassung der Systemdaten erzeugt und in dem festen Datenbereich (2) gespeichert wird und
- die kryptographische Zusammenfassung zur Verifikation der Systemdaten vor dem Lesen und/oder Aufzeichnen von Benutzerdaten verwendet wird.

2. Verfahren nach Anspruch 1 **dadurch gekennzeichnet, dass** der beschreibbare Datenbereich (3, 4) einen Eckbereich umfasst und die Systemdaten in dem Eckbereich gespeichert werden.

3. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** eine Hash-Funktion (5) zum Erzeugen der kryptographischen Zusammenfassung und zum Verifizieren der Systemdaten verwendet wird.

4. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** ein Nachrichtenauthentifikationscode-Algorithmus zum Erzeugen der kryptographischen Zusammenfassung und zum Verifizieren der Systemdaten verwendet wird.

5. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** ein Schlüsselsignatur-Algorithmus zum Erzeugen der kryptographischen Zusammenfassung und zum Verifizieren der Systemdaten verwendet wird und dass eine Signatur als kryptographische Zusammenfassung gespeichert wird.

6. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass**, als Teil des Formatierens des Speichermediums (1), die kryptographische Zusammenfassung erzeugt wird und die Systemdaten in dem beschreibbaren Datenbereich (3) gespeichert werden.

7. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** Kopierschutz-Information als Systemdaten gespeichert wird, insbesondere eine einmalige Speichermediumkennung, ein durch einen oder mehrere unterschiedliche herstellerspezifische oder gerätespezifische Schlüssel verschlüsselter Schlüssel oder eine oder mehrere Listen von widerrufenen Einrichtungen oder widerrufenen Speichermedien.

8. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** die Systemdaten ursprünglich in einem Eckbereich des beschreibbaren Datenbereiches (3) gespeichert werden und dass während einer ersten Benutzung des Speichermediums (1) in einem Aufzeichnungsgerät die Systemdaten in einen Benutzerdatenbereich (4) des beschreibbaren Datenbereiches (3, 4) kopiert werden.

9. Verfahren zum Speichern von Daten auf einem wiederbeschreibbaren Datenspeichermedium (1), welches einen nur lesbaren festen Datenbereich (2) umfasst, **dadurch gekennzeichnet, dass**

   - der nur lesbare feste Datenbereich einen ersten Datenbereich und einen Eckbereich umfasst
   - Systemdaten in dem Eckbereich gespeichert werden.
   - eine kryptographische Zusammenfassung der Systemdaten erzeugt und in dem ersten Datenbereich gespeichert wird und
   - die kryptographische Zusammenfassung zur Verifikation der Systemdaten vor dem Lesen und/oder Aufzeichnen von Benutzerdaten verwendet wird.

10. Wiederbeschreibbares Speichermedium (1) zum Speichern von Daten, mit

    - einem beschreibbaren Datenbereich (3, 4), in dem Systemdaten gespeichert sind, und
    - einem nur lesbaren festen Datenbereich (2), **dadurch gekennzeichnet, dass** in dem nur lesbaren festen Datenbereich (2) eine kryptographische Zusammenfassung der Systemdaten gespeichert ist, wobei die kryptographische Zusammenfassung zur Verifikation der Systemdaten vor dem Lesen und/oder Aufzeichnen von Benutzerdaten vorgesehen ist.

11. Speichermedium (1) nach Anspruch 10, **dadurch gekennzeichnet, dass** der beschreibbare Datenbereich (3, 4) einen Eckbereich umfasst und die Systemdaten in dem Eckbereich gespeichert sind.

12. Speichermedium nach Anspruch 11, **dadurch gekennzeichnet, dass** das Speichermedium einen Lead-in-Bereich umfasst, wobei der Eckbereich in dem Lead-in-Bereich liegt.

13. Speichermedium (1) nach Anspruch 10, **dadurch gekennzeichnet, dass** das Speichermedium (1) ein wiederbeschreibbares optisches Speichermedium ist, insbesondere eine CD oder eine DVD.

14. Wiederbeschreibbares Speichermedium zum Speichern von Daten, mit einem nur lesbaren festen Datenbereich (2) **dadurch gekennzeichnet, dass** der nur lesbare feste Datenbereich einen ersten Datenbereich und einen Eckbereich umfasst, in dem Systemdaten gespeichert sind, und eine kryptographische Zusammenfassung der Systemdaten in dem ersten Datenbereich gespeichert ist, wobei die kryptographische Zusammenfassung zur Verifikation der Systemdaten vor dem Lesen und/oder Aufzeichnen von Benutzerdaten vorgesehen ist.

15. Speichermedium nach Anspruch 14, **dadurch gekennzeichnet, dass** der erste Datenbereich ein Burst-Cut-Bereich (BCA: Burst Cut Area) ist und der Eckbereich eine Pitwobbelung und/oder eine Vorrillenwobbelung umfasst.

16. Speichermedium nach Anspruch 14, **dadurch gekennzeichnet, dass** der erste Datenbereich ein

Burst-Cut-Bereich ist und der Eckbereich vorgepresste Pits umfasst.

17. Speichermedium nach Anspruch 10 oder 14, **dadurch gekennzeichnet, dass** die kryptographische Zusammenfassung des Systems das Ergebnis eines Zerhackens der Systemdaten ist.

18. Verfahren zur Verifikation von Systemdaten, die sich vor dem Lesen und/oder Aufzeichnen von Benutzerdaten auf einem wiederbeschreibbaren Speichermedium (1) befinden, wobei das wiederbeschreibbare Speichermedium (1) einen nur lesbaren festen Datenbereich (2) und einen beschreibbaren Datenbereich (3, 4) umfasst, **dadurch gekennzeichnet, dass**

- die Systemdaten und eine kryptographische Zusammenfassung der Systemdaten gelesen werden, wobei die kryptographische Zusammenfassung in dem nur lesbaren festen Datenbereich gespeichert wird.
- eine kryptographische Zusammenfassung der aus dem Medium ausgelesenen Systemdaten erzeugt wird und
- die aus dem Medium ausgelesene kryptographische Zusammenfassung und die erzeugte kryptographische Zusammenfassung verglichen werden.

19. Aufzeichnungsgerät zum Speichern von Daten auf einem wiederbeschreibbaren Datenspeichermedium (1), das Aufzeichnungsmittel zum Speichern von Systemdaten in einem beschreibbaren Datenbereich (3) des Mediums umfasst, **dadurch gekennzeichnet, dass** Erzeugungsmittel (5) zum Erzeugen einer kryptographischen Zusammenfassung der Systemdaten vorhanden sind und die Aufzeichnungsmittel zum Speichern der kryptographischen Zusammenfassung in einem nur lesbaren festen Datenbereich (2) des Mediums (1) geeignet sind, wobei die kryptographische Zusammenfassung zur Verifikation der Systemdaten vor dem Lesen und/oder Aufzeichnen von Benutzerdaten vorgesehen ist.

20. Aufzeichnungsgerät zum Speichern von Daten auf einem wiederbeschreibbaren Datenspeichermedium (1) mit einem nur lesbaren festen Datenbereich (2), **dadurch gekennzeichnet, dass**

- der nur lesbare feste Datenbereich einen ersten Datenbereich und einen Eckbereich umfasst
- Aufzeichnungsmittel zum Speichern von Systemdaten im Eckbereich und zum Speichern der kryptographischen Zusammenfassung und der Systemdaten in dem ersten Datenbereich vorhanden sind, wobei die kryptographische Zusammenfassung zur Verifikation der Systemdaten vor dem Lesen und/oder Aufzeichnen von Benutzerdaten vorgesehen ist, und
- Erzeugungsmittel (5) zum Erzeugen der kryptographischen Zusammenfassung der Systemdaten vorhanden sind.

21. Abspielgerät zum Abspielen von auf einem wiederbeschreibbaren Datenspeichermedium (1) gespeicherten Benutzerdaten, das Lesemittel zum Lesen von in dem beschreibbaren Datenbereich (3, 4) des Mediums (1) gespeicherten Systemdaten umfasst, **dadurch gekennzeichnet, dass** die Lesemittel auch zum Lesen einer kryptographischen Zusammenfassung der in einem nur lesbaren festen Datenbereich (2) des Mediums (1) gepeicherten Systemdaten geeignet sind und dass Verifizierungsmittel (5, 6) zum Erzeugen einer kryptographischen Zusammenfassung der aus dem Medium (1) ausgelesenen Systemdaten und zur Verifikation der Systemdaten durch Verwendung der erzeugten kryptographischen Zusammenfassung vorhanden sind.

22. Abspielgerät zum Abspielen von auf einem wiederbeschreibbaren Datenspeichermedium (1) mit einem nur lesbaren festen Datenbereich (2) gespeicherten Benutzerdaten, **dadurch gekennzeichnet, dass** der nur lesbare feste Datenbereich einen ersten Datenbereich und einen Eckbereich umfasst und dass das Abspielgerät umfasst:

- Lesemittel zum Lesen von in dem Eckbereich gespeicherten Systemdaten und zum Lesen einer kryptographischen Zusammenfassung der in dem ersten Datenbereich (2) gespeicherten Systemdaten und
- Verifizierungsmittel (5, 6) zum Erzeugen einer kryptographischen Zusammenfassung der aus dem Medium (1) ausgelesenen Systemdaten und zur Verifikation der Systemdaten durch Verwendung der erzeugten kryptographischen Zusammenfassung.

23. Abspielgerät nach Anspruch 21 oder 22, **dadurch gekennzeichnet, dass** es weiterhin Aufzeichnungsmittel zum Aufzeichnen der Benutzerdaten auf dem wiederbeschreibbaren Datenspeichermedium (1) umfasst.

Revendications

1. Procédé de stockage de données sur un support de stockage de données réinscriptible (1) comprenant une zone de données fixe à lecture seule (2) et une zone de données enregistrable (3,4), procédé dans

le quel les données système sont stockées dans la zone de données enregistrable (3), **caractérisé en ce que**:

- un résumé cryptographique des données système est généré et stocké dans la zone de données fixe (2), et
- le résumé cryptographique est utilisé pour la vérification des données système avant la lecture et/ou l'enregistrement de données utilisateur.

2. Procédé comme exposé suivant la revendication 1, **caractérisé en ce que** la zone de données enregistrable (3, 4) comprend une zone de coin et les données système sont stockées dans la zone de coin.

3. Procédé comme exposé suivant la revendication 1, **caractérisé en ce qu'**une fonction de hachage (5) est utilisée pour générer le résumé cryptographique et pour vérifier les données système.

4. Procédé comme exposé suivant la revendication 1, **caractérisé en ce qu'**un algorithme de code d'authentification de message est utilisé pour générer le résumé cryptographique et pour vérifier les données système.

5. Procédé comme exposé suivant la revendication 1, **caractérisé en ce qu'**un algorithme de signature à clé est utilisé pour générer le résumé cryptographique et pour vérifier les données système, et **en ce qu'**une signature est stockée comme résumé cryptographique.

6. Procédé comme exposé suivant la revendication 1, **caractérisé en ce que** le résumé cryptographique est généré et les données système sont stockées dans la zone de données enregistrable (3) en tant que partie du formatage du support de stockage (1).

7. Procédé comme exposé suivant la revendication 1, **caractérisé en ce que** des informations de protection contre la copie sont stockées sous la forme de données système, en particulier d'un identificateur de support de stockage unique, d'une clé chiffrée par une ou plusieurs clés différentes spécifiques au fabricant ou spécifiques au dispositif, ou d'une ou de plusieurs listes de dispositifs révoqués ou de supports de stockage révoqués.

8. Procédé comme exposé suivant la revendication 1, **caractérisé en ce que** les données système sont à l'origine stockées dans une zone de coin de la zone de données enregistrable (3) et **en ce que**, lors de la première utilisation du support de stockage (1) dans un appareil d'enregistrement, les données système sont copiées dans une zone de données utilisateur (4) de la zone de données enregistrable (3, 4).

9. Procédé de stockage de données sur un support de stockage de données réinscriptible (1), comprenant une zone de données fixe à lecture seule (2), **caractérisé en ce que**

- la zone de données fixe à lecture seule comprend une première sone de données et une zone de coin;
- les données système sont stockées dans la zone de coin;
- un résumé cryptographique des données système est généré et stocké dans la première zone de données, et
- le résumé cryptographique est utilisé pour la vérification des données système avant la lecture et/ou l'enregistrement de données utilisateur.

10. Support de stockage réinscriptible (1) destiné à stocker des données, comprenant :

- zone de données enregistrable (3, 4) dans laquelle des données système sont stockées, et
- zone de données fixe à lecture seule (2), **caractérisé en ce qu'**un résumé cryptographique des données système est stocké dans la zone de données fixe à lecture seule (2), le résumé cryptographique étant prévu pour une vérification des données système avant lecture et/ou enregistrement des données utilisateur.

11. Support de stockage (1) comme exposé suivant la revendication 10, **caractérisé en ce que** la zone de données enregistrable (3, 4) comprend une zone de coin, et les données système sont stockées dans la zone de coin.

12. Support de stockage (1) comme exposé suivant la revendication 11, **caractérisé en ce que** le support de stockage comprend une zone de coin d'entrée située dans la zone d'entrée.

13. Support de stockage (1) comme exposé suivant la revendication 10, **caractérisé en ce que** le support de stockage (1) est un support de stockage optique réinscriptible, en particulier un CD ou un DVD.

14. Support de stockage réinscriptible (1) destiné à stocker des données, comprenant une zone de données fixe à lecture seule (2), **caractérisé en ce que** la zone de données fixe à lecture seule comprend une première zone de données et une zone de coin dans lesquelles des données système sont stockées, et **en ce qu'**un résumé cryptographique

des données système est stocké dans la première zone de données, le résumé cryptographique étant prévu pour une vérification des données système avant lecture et/ou enregistrement des données utilisateur.

15. Support de stockage (1) comme exposé suivant la revendication 14, **caractérisé en ce que** la première zone de données est une zone de type Burst Cut Area, et la zone de coin comprend une oscillation de creux et/ou une oscillation de préspirale.

16. Support de stockage (1) comme exposé suivant la revendication 14, **caractérisé en ce que** la première zone de données est une zone de type Burst Cut Area et la zone de coin comprend des creux ayant été pressés au préalable.

17. Support de stockage (1) comme exposé suivant la revendication 10 ou 14, **caractérisé en ce que** résumé cryptographique des données système comprend le résultat d'un hachage des données système.

18. Procédé destiné à la vérification de données système présentes sur un support de stockage de données réinscriptible (1) avant lecture et/ou enregistrement de données utilisateur. le support de stockage de données réinscriptible (1) comprenant une zone de données fixe à lecture seule (2) et une zone de données enregistrable (3, 4),
caractérisé en ce que

- les données système et un résumé cryptographique des données système, lequel résumé cryptographique est stocké dans la zone de données fixe à lecture seule, sont lus;
- un résumé cryptographique des données système lues sur le support est généré, et
- le résumé cryptographique lu sur le support et le résumé cryptographique généré sont comparés.

19. Appareil d'enregistrement destiné à stocker des données sur un support de stockage de données réinscriptible (1) comprenant des moyens d'enregistrement destinés à stocker des données système dans une zone de données enregistrable (3) du support, **caractérisé en ce que** les moyens de génération (5) sont présents afin de générer un résumé cryptographique des données système, et les moyens d'enregistrement conviennent au stockage du résumé cryptographique dans une zone de données fixe à lecture seule (2) du support (1), le résumé cryptographique étant prévu pour une vérification des données système avant lecture et/ou enregistrement des données utilisateur.

20. Appareil d'enregistrement destiné à stocker des données sur un support de stockage réinscriptible (1) comprenant une zone de données fixe à lecture seule (2), **caractérisé en ce que**

- la zone de données fixe à lecture seule comprend une première zone de données et une zone de coin;
- des moyens d'enregistrement sont présents afin de stocker des données système dans la zone de coin, et afin de stocker un résumé cryptographique dans la première zone de données, le résumé cryptographique étant prévu pour une vérification des données système avant lecture et/ou enregistrement des données utilisateur, et
- des moyens de génération (5) sont présents afin de générer le résumé cryptographique des données système.

21. Appareil de lecture pour la lecture de données utilisateur stockées sur un support de stockage de données réinscriptible (1), comprenant des moyens de lecture destinés à lire des données système stockées dans la zone de données enregistrable (3, 4) du support (1), **caractérisé en ce que** les moyens de lecture conviennent également à la lecture d'un résumé cryptographique des données système stockées dans une zone de données fixe à lecture seule (2) du support (1), et **en ce que** des moyens de vérification (5, 6) sont présents afin de générer un résumé cryptographique des données système lues sur le support (1) et afin de vérifier les données système en utilisant le résumé cryptographique généré.

22. Appareil de lecture destiné à la lecture de données utilisateur stockées sur un support de stockage de données réinscriptible (1) comprenant une zone de données fixe à lecture seule (2), **caractérisé en ce que** la zone de données fixe à lecture seule comprend une première zone de données et une zone de coin, et l'appareil de lecture comprend :

- des moyens de lecture destinés à lire des données système stockées dans la zone de coin, et destinés à lire un résumé cryptographique des données système dans la première zone de données (2), et
- des moyens de vérification (5, 6) destinés à générer un résumé cryptographique des données système lues sur le support (1), et destinés à la vérification des données système à l'aide du résumé cryptographique généré.

23. Appareil de lecture comme exposé suivant la revendication 21 ou 22, **caractérisé en ce qu'**il comprend en outre des moyens d'enregistrement des-

tinés à enregistrer les données utilisateur sur le support de stockage de données réinscriptible (1).

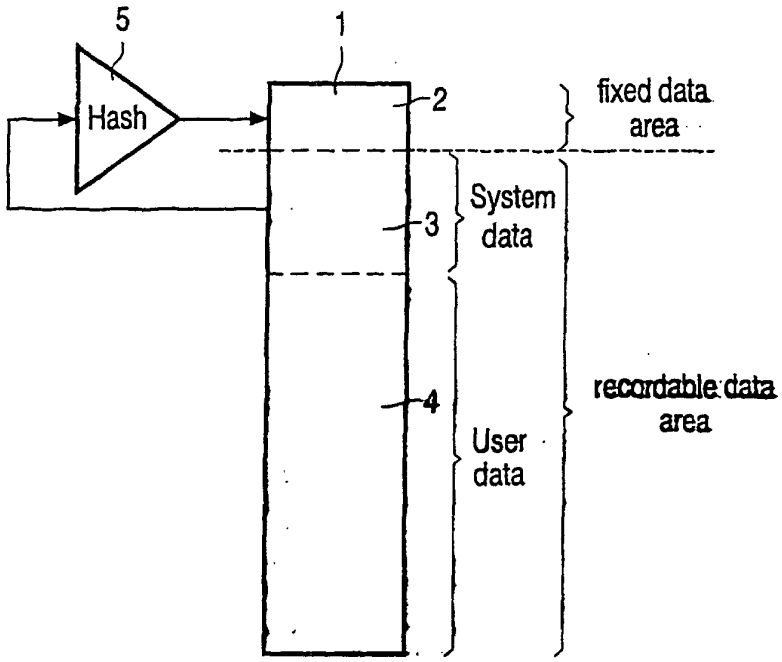
5
1
Hash
2
fixed data area
System data
3
recordable data area
4
User data

FIG. 1

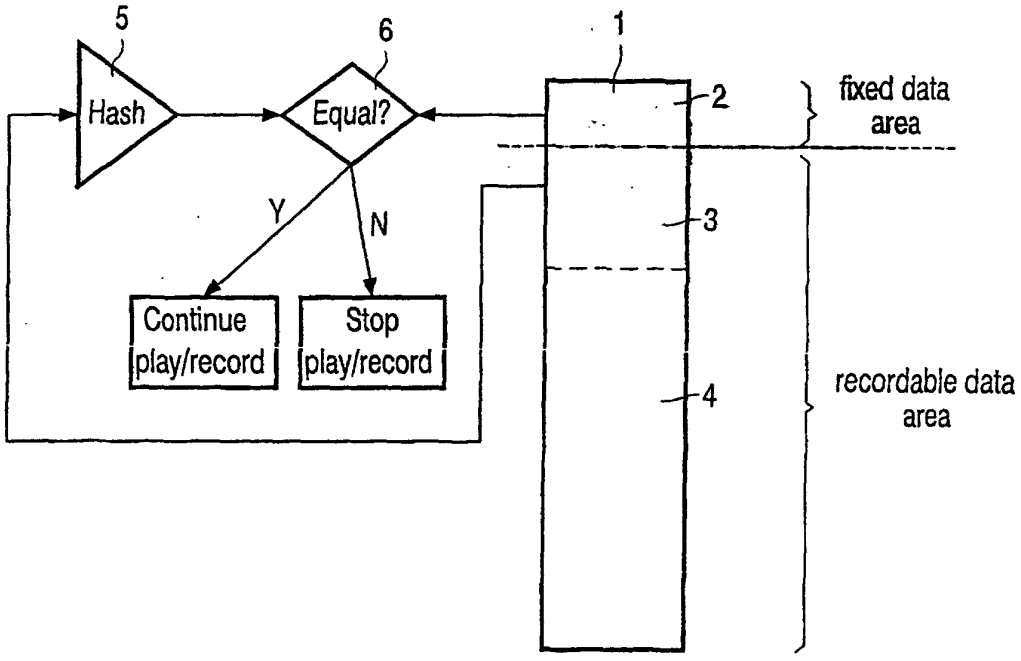
5
6
1
Hash
Equal?
2
fixed data area
Y
N
3
Continue play/record
Stop play/record
4
recordable data area

FIG. 2

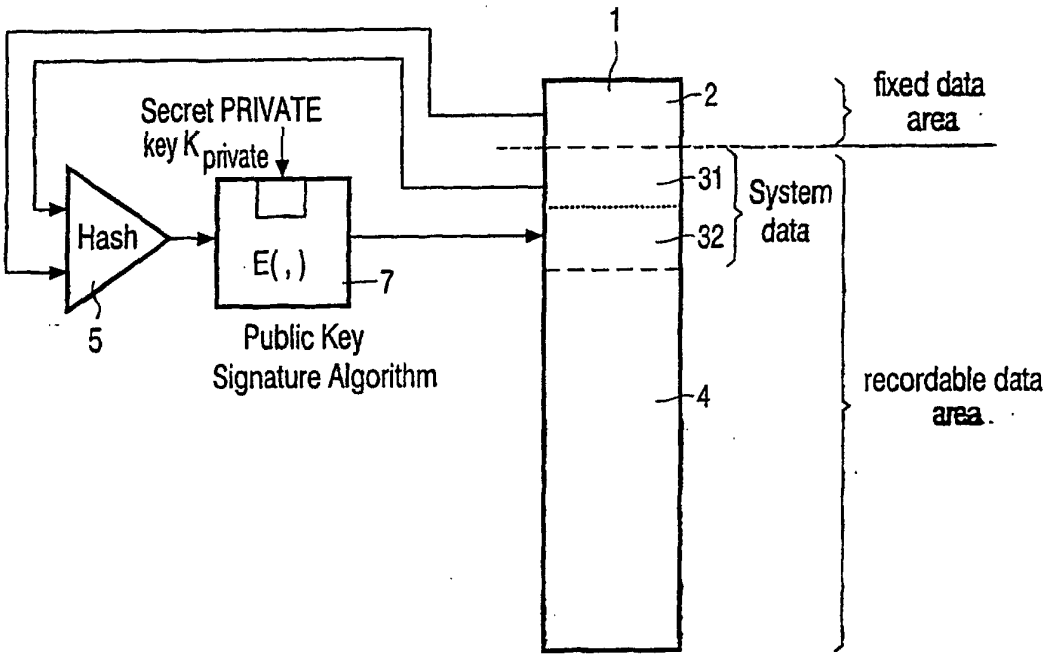
1
2
fixed data area
Secret PRIVATE key K private
31
System data
32
Hash
E(,)
7
5
Public Key Signature Algorithm
4
recordable data area

FIG. 3

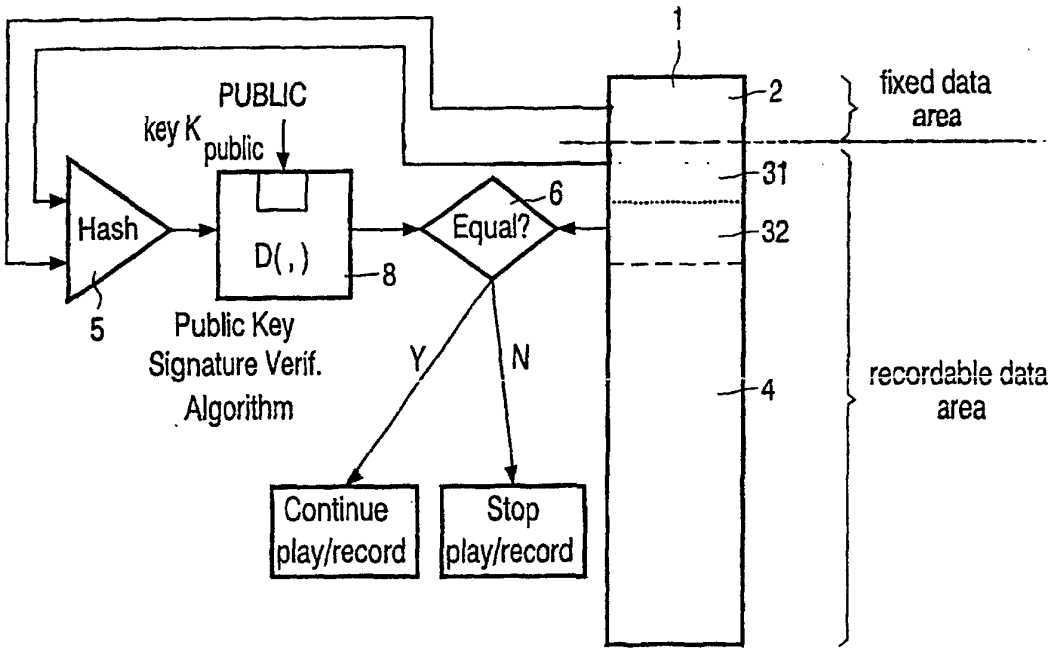
1
2
fixed data area
PUBLIC key K public
31
Hash
D(,)
6
Equal?
32
8
5
Public Key Signature Verif. Algorithm
Y
N
4
recordable data area
Continue play/record
Stop play/record

FIG. 4

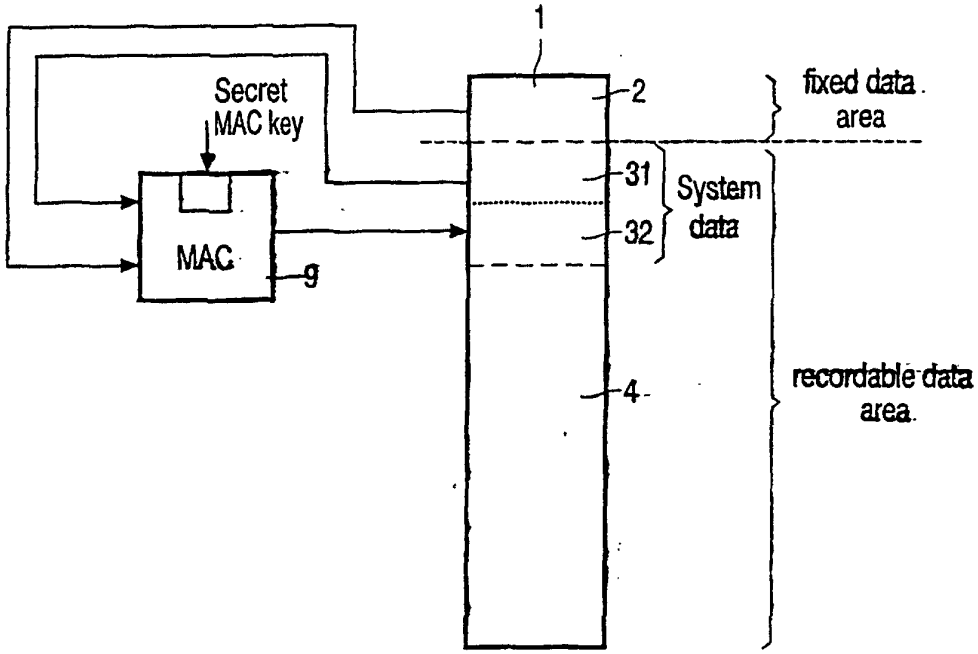
1
Secret
MAC key
MAC
9
2
31
32
4
fixed data
area
System
data
recordable data
area

FIG. 5.

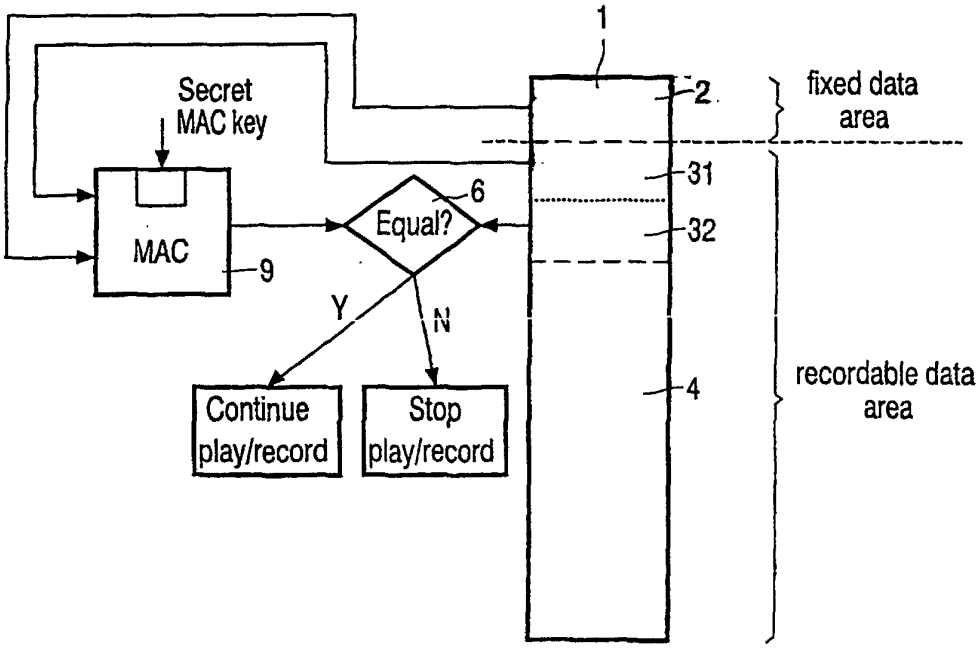
1
Secret
MAC key
MAC
9
6
Equal?
Y
N
Continue
play/record
Stop
play/record
2
31
32
4
fixed data
area
recordable data
area

FIG. 6