(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 December 2004 (29.12.2004)

PCT

(10) International Publication Number
WO 2004/114122 A2

(51) International Patent Classification[7]: G06F 7/58

(21) International Application Number:
PCT/IB2004/050968

(22) International Filing Date: 22 June 2004 (22.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03101903.7 26 June 2003 (26.06.2003) EP

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **FONTIJN, Wilhelmus, F., J.** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **LAMBERT, Nicolaas** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **DENISSEN, Adrianus, J., M.** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

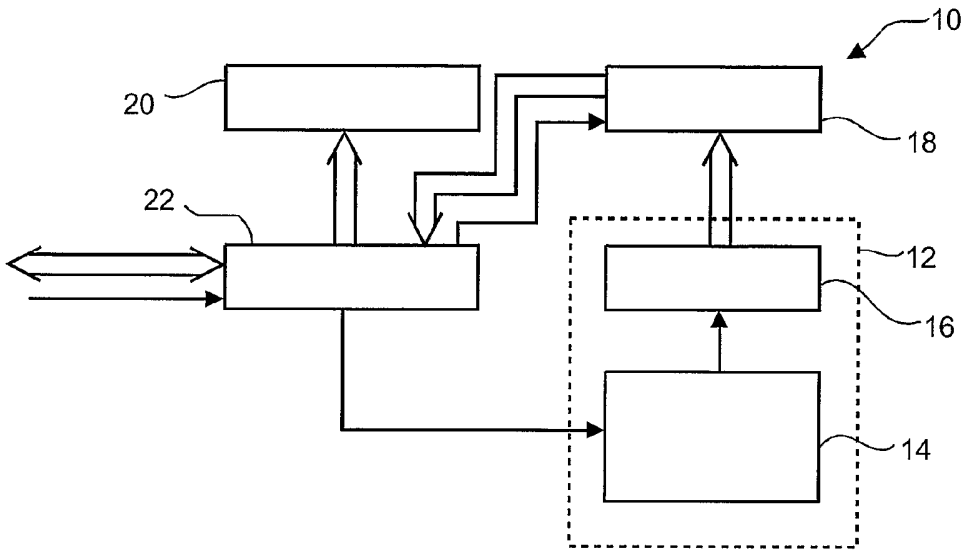
(74) Agent: **DUIJVESTIJN, Adrianus, J.**; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SECURE NUMBER GENERATOR AND CONTENT DISTRIBUTION NETWORK EMPLOYING THE SAME



(57) Abstract: A secure number generator (10, SNG 1... 10) is disclosed, comprising a random function unit (12) and a non-volatile memory (18, 20) connected to said random function unit. The random function unit (12) implements an unstable, measurable random quantity (14), such that a repeated measurement of the random quantity results in different random values. The random function unit (12) is adapted to ascertain a current random value of the random quantity (14), to transform the current random value into a digital random code, and to write said digital random code to a first section (18) of said non-volatile memory. Further, a content distribution network employing the secure number generator is disclosed.

WO 2004/114122 A2

Declaration under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Secure number generator and content distribution network employing the same

The present invention relates to a secure number generator, to a method for creating a unique identifier code of a solid state device, and to a content distribution system comprising at least one content source and a plurality of clients adapted to communicate with the content source or with each other or both for downloading or uploading one or more content items.

The proliferation of audio content distribution and Pay-TV over data networks is driving the need for solutions to the problem of securing the content distribution. In parallel, the growth of Internet and Intranets has highlighted the need for secure network access control.

There are secure protocols that use encryption and authentication by secret key information contained for example in devices like key cards (Smartcards etc). Secure protocols assume that participants are able to maintain the key information secret. This assumption has proven incorrect in many cases. EPROM memory provided on a Smartcard and containing secret key information can be examined to extract the key bits. The security concept of key card identification can for instance be by-passed after successful extraction by cloning a key card using the extracted key.

Recently, new concepts have been developed to make such key information in solid-state devices like key cards more secure. WO98/22914 and US 5,434,917 describe the use of a random distribution of metallic particles embedded into a key card.

US 5,434, 917 describes the use of the response of the metallic particles to an external magnetic or electromagnetic scanning procedure of the key card as an input to a secure public-key signature algorithm. This algorithm is located in an external device and evaluates a key code. The0000 key code is then written to a memory on the key card.

For identification or authentication purposes, the card is inserted into a reader that scans the particle distribution using the response of the particle distribution to a magnetic field generated by the reader. The resulting output of the scanning procedure and identification data of the card's owner in the memory of the key card are evaluated by the

reader according to a public-key algorithm and compared to the stored key code in order to ensure its validity. This solution has the disadvantage a card reader compatible with this system needs to be supplied with complicated and expensive scanning and evaluation facilities in order to be able to check the validity of a key card. If a key code gets compromised, the key card must be destroyed and a new card must be issued to the user.

The document B. Gassend, D. Clarke, M. van Dijk, S. Devadas: "Controlled Physical Unknown Functions: Applications to Secure Smartcards and Certified Execution", http://www.lcs.mit.edu/ publications/ pubs/ pdf/ MIT-LCS-TR-845.pdf (hereinafter "Gassend et al."), describes the use of so called controlled "physical unknown functions" (PUF) as an integral part of an IC. This document steps away from storing a key in a memory. Instead of reading from a memory, a PUF is evaluated whenever the key is requested.

A PUF, also called random physical function herein, is essentially a random function based on a physical quantity that is easy to evaluate, but hard to characterize. An example of a PUF given by Gassend et al. will be described in the following: The evaluated physical quantity in this example is the delay time of a signal travelling between two given points of an Integrated Circuit (IC). This delay time is influenced by gates and wires the signal has to pass. Further, this delay is known to have random variations due to variations in dies from the same wafer, and from wafer to wafer. Such variations are caused during manufacture, for instance, due to process parameters such as temperature and ambient pressure that are subject to local variations and variations in time. Therefore, an internal measurement of the delay of electrical signals in an IC provides one value of a random function that depends, in an uncontrollable manner, on processing parameters. The delay value is unknown to anybody, including the manufacturer of the IC. It is not possible for the manufacturer to produce two identical ICs using this PUF. Therefore, a system integrating the PUF cannot be cloned.

A drawback in the use of PUFs such as the one just described lies in an often-incurred instability of the physical quantity that is measured. For instance, the internal delay during signal propagation in an IC is depends environmental parameters at the time of the measurement. Beside parameters such as ambient temperature and pressure, e.g., also the supply voltage influences the evaluated signal delay. Therefore, a difference of the supply voltage during subsequent evaluations of the PUF will result in a different output of the random function. As a consequence of the instability of the PUF, it cannot be used for reliably supplying the same key code at different points in time.

Gassend et al. provide a system that excludes an influence of instability on the key generation from the output of the PUF by introducing an additional evaluation algorithm linked to the PUF. The evaluation algorithm performs a division of different measured delay values, such as signal delay times along different paths, and uses the result of the division for generation of a stable key code. Whenever the key is read, the PUF is evaluated by internal delay measurements, the ratio of the measured delay values is determined by the calculation unit, and the determined relative delay value is provided for generation of the requested key.

However, this solution cannot be generalized to other PUFs. The division algorithm cancels out known influences of parameters on the evaluation of this particular PUF. That means: an evaluation algorithm that provides a stable output can only be provided in a case where the physical quantity underlying the used PUF is understood well enough in order to design an algorithm cancelling out all relevant parameters that cause instability of the PUF. This restriction excludes a large number of PUF from the use in a secure number generator.

In addition, the solution of Gassend et al. requires additional circuitry for implementing the readout and the evaluation algorithm. This results in a rather large size of an IC comprising the secure number generator of Gassend et al.

A further drawback lies in the fact that the range of random numbers covered by the described PUF is rather small. Delay times on different chips of the same type lie in only a small range of values due to the identical design of the integrated circuits. That implies that the random nature of the key codes provided is hard to control.

Finally, the fact that the unique number provided by the controlled PUF of Gassend et al. cannot be accessed implies that the random nature of the stored key code cannot be checked. This opens up a possibility for the manufacturer to fake the implementation of the PUF by simply programming a chosen key code into the device. Of course, this key code is not secure because multiple clones of a key card with such a fake PUF can be manufactured.

It is therefore an object of the present invention to provide a secure number generator that is simple and effective and easy to implement in solid-state devices.

According to a first aspect of the invention, a secure number generator is provided, comprising a random function unit and a non-volatile memory connected to said random function unit,

- wherein the random function unit implements an unstable, measurable random quantity, such that a repeated measurement of the random quantity results in different random values, and
- wherein the random function unit is adapted to measure a current random value of the random quantity, to transform the current random value into a digital random code, and to write said digital random code to a first section of said non-volatile memory.

The secure number generator of the present invention has a random function unit that implements an unstable measurable random quantity. The instability of the random quantity is such that a repeated measurement of the random quantity results in different random values. In other words, the result of a measurement of the random quantity is not reproducible when the measurement is repeated. An example of such a random quantity is the signal delay in an integrated circuit as described earlier. It is important that in this example according to the invention the random quantity must be unstable. That means, in contrast to Gassend et al. there is no control instance that cancels out the instability of the random quantity. Further examples of such random quantities will be presented below in the context of the description of preferred embodiments.

The random function unit of the secure number generator of the invention provides at its output a digital random code as the result of a transformation of the measured random value of the random quantity. The transformation is such that the digital random code provided by the random function preserves the irreproducible nature of the measured random value. Given a sufficient code length the binary random code can easily made globally unique without control by any external instance. In a preferred embodiment the random function unit is adapted to provide a digital random code that is simply the binary translation of the measured random value. However, other types of transformation of the measured random value into a digital random code are considered equally useful. The transformation should be as simple as possible in order to save space when implementing the transformation algorithm on chip, without, of course, destroying the random nature of the digital code and the irreproducibility of the random code.

Providing an irreproducible random code as an output is a further important difference of the secure number generator of the present invention to the known number generator of Gassend et al. Their secure number generator delivers a reproducible random code because dedicated circuitry is provided that determines a constant random value in the form of a signal delay ratio, before creating the binary code.

The random function unit is adapted to write the digital random code to a first section of a non-volatile memory. The non-volatile memory is stable and persistent. A preferred example is an MRAM register. The memory is a part of the secure number generator.

There is only an internal writing access to the memory. The memory is in a preferred embodiment protected against external attacks by an integrity control unit integrated into the secure number generator. The integrity control unit is adapted to check if any one of the bits stored in the non-volatile memory has been changed. In one embodiment the integrity control unit comprises a write controller and a read controller for the non-volatile memory. The write controller is adapted to generate from the digital random code provided by the random function unit output data that comprises the digital random code and at least one checking bit allocated to at least one code bit of the digital random code. The respective checking bit(s) has (have) a value that is complementary to that of the respective code bit(s). A checking bit is stored in a storage cell allocated to the storage cell storing the respective allocated code bit, preferably in a neighboring storage cell. This way, the read controller of the secure number generator can detect tampering attempts to the memory. The read controller compares the values of a respective code bit/checking bit pair. If the values are not complementary, i.e., if they are identical, either the code bit or the checking bit must have been changed. That implies the integrity of the random code stored in the non-volatile memory is lost. The digital random code can then be renewed internally, for instance by triggering the random function unit to create a new random code with a corresponding control signal that is provided by the read control unit.

The secure number generator has several advantages of over prior art devices. The use of a random function unit with an unstable random quantity saves space in an integrated circuit. The prior art solution of Gassend et al. shows that stability requires additional circuitry, which costs space. The stability of the binary random code is guaranteed in the secure number generator of the invention by storing the number in a non-volatile memory such as NVRAM. The binary code provided by the secure number generator is therefore not dependent on temperature or noise as in a solution where the random quantity must be evaluated every time the binary code is requested. Furthermore, it is easy to check the secure number generator of the present invention on the correctness of the implementation of the random quantity. This can be done by simply performing repeated measurements of the quantity and verifying the random nature of the provided output. In

addition, it is possible to activate the secure number generator whenever it suits best. The time of activation is under control.

The manufacturer of the secure number generator has no influence on the number. The manufacturer of a chip comprising the secure number generator of the invention need not even participate in the activation of the secure number. Therefore, with the secure number generator of the invention there is no possibility to clone the generated secure number .

A key may become compromised. Most prior art systems revoke the whole device in this case because they cannot securely renew the keys. The present invention, however, allows securely renewing a key without revocation of the device holding it. The fact that the random function unit does not generate the same binary random code twice implies that the binary random code stored in the memory can be reinitialised simply by letting the random function unit provide a new binary random code. There is no need for an issuing agent of a key card containing the secure number generator of the invention to supply a new number from the outside, or even a new key card. The renewal of the key can only be performed internally upon reception of a reset signal from outside, as will be described below in the context of a preferred embodiment. This allows a revocation authority to renew the key if necessary in a very secure way compared to known key renewal methods.

In one embodiment measures are taken that the random function can only be read once, for instance during manufacture, or first use of a solid-state device comprising the secure number generator. Such measures can comprise a hardware or software control of the secure number generator. For instance, the electrical connection between the random function unit and the non-volatile memory can be destroyed after storing the random digital code to the memory. As an alternative, a control feature can be added that implements a "write-once" access to the memory.

A preferred embodiment of the secure number generator of the invention comprises a control unit connected with the random function unit. The control unit is adapted to trigger the random function unit to ascertain and write a new digital random code to the memory. The control unit may further be adapted to provide this signal under certain predetermined conditions. One example of such a condition is the first detection of a reception of a read request asking for an output of the digital random code from the first section of the memory to an external client. Another example of such a condition is the reception of a signal indicating detection of a loss of integrity of the digital random code. A loss of integrity is for instance a change of one or several bits of the code. In this example,

the control unit receives this signal from an integrity control adapted to unit that is preferably integrated into the secure number generator.

Another form of this embodiment allows the reception of a "reset" request signal from an external source. The implementation of the handling of such an external signals may be an alternative or an addition to the handling of internal signals described in the last paragraph. In this embodiment the secure number generator is adapted to receive from an external source a signal indicating that the memory shall be initialised or rewritten with a new random code. Such an external source can be a unit that is provided on the same chip, for instance a timing unit that detects and signals that the time of validity of the previously stored code has run out. An external source may also be an external device adapted to create the signal and provide it to the secure number generator through an electrical contact on the chip comprising the secure number generator. For instance, an operator of a smartcard system may send a reset command to a set-top box that is used to read the card. The set-top box will then reset the card. Another example is a user interface of a device holding the secure number generator that allows the user to enter a command to reset the secure number.

A further embodiment of the secure number generator has a second section in the memory separate from the first section. The second section can be used for storing manufacturer identification. The memory has an input connected with said second section and not said first section. This way, it can be assured that the manufacturer is not able to overwrite the binary random code stored in the first section. The implementation of the connection between the input and only the second section of the memory can be physical, e.g., by circuit paths connecting the input only with the second section. This embodiment requires two inputs to the memory, one for the random code, one for external identification data. As an alternative, the present embodiment may take the form of two separate memory registers integrated into the secure number generator. Another alternative is to provide only one memory with only one input connected with both the first and second section physically, and to implement an additional control feature that detects any external data input and writes this external data input to the second section.

The non-volatile memory is preferably an MRAM register. MRAM memory technology provides a stable, temperature-resistant memory.

The secure number generator contains a random function. A possible candidate for a random function to be used with the secure number generator of the invention is any random function that implements an unstable, measurable random quantity, such that a

repeated measurement of the random quantity results in different random values. The most important feature of the random function used with the secure number generator of the invention is that the number created is not predictable. The random function is in alternative embodiments deterministic or non-deterministic.

Four examples of a suitable random function are given in the following:

a) A maximum length sequence (MLS) coupled to a free-running ring-oscillator. Maximum length-sequences are well known in the art. For instance, an MLS can be implemented using a shift register with exclusive-OR feedback from more than two taps of the register. A MLS alone provides a pseudo-random sequence of bits that is repeated after a predetermined number of bits, depending on the length of the shift register. A highly unpredictable binary value can be generated by reading the bit-sequence of the MLS after an unpredictable number of clock ticks. For instance this can be done by connecting the shift clock input of the MLS to a free running ring oscillator of poorly predictable frequency, and reading the MLS value after a period that is determined by some independent other means, e.g. a fixed system time interval.

b) A non-linear electrical circuit exhibiting chaotic behaviour. It is well known in the art that non-linear circuits can be designed to exhibit chaotic behaviour in an output signal. For instance, a diode may be the source of a chaotic behaviour in a non-linear circuit.

c) An electrical circuit reading physical noise, such as the thermal noise generated by thermal agitation of electrons in a conductor, background noise in the radio static electromagnetic spectrum

d) Another example of a random function implementing a suitable physical quantity is an array of MRAM cells that have an uncertain cell state. Below a certain cell size an MRAM cell does not take on a defined cell state. A measurement of the cell state results in a value that varies randomly from measurement to measurement. Therefore, each cell of the array will provide a random bit resulting in a random bit sequence that is obtained when reading from the whole MRAM array.

The secure number generator can be used in any application, which makes use of secure random numbers, such as in an encryption device, in a random number generator that provides third parties with random numbers for their particular purposes, such as a lottery, etc. The secure number generator of the invention is preferably integrated into an IC. The preferred use of the secure number generator is to provide a secure identification key of the IC, and to renew the identification key under predefined conditions such as when a key has been compromised by an unauthorized manipulation.

Accordingly, a second aspect of the invention concerns a method for creating a unique key allocated to a solid-state device, comprising the steps of

- providing a solid state device comprising an implementation of an unstable, measurable random quantity, such that a repeated measurement of the random quantity results in different random values,
- measuring a current random value of the random quantity,
- transforming the current random value into a digital random code, and
- writing said digital random code to a first section of a non-volatile memory that is integrated into the solid-state device,

wherein the solid-state device performs the measuring, transforming and writing steps.

The method of this aspect of the invention provides a secure way of creating an identifier for a solid-state device, which can be an IC, or any device comprising the IC. The advantages of the method are the same as those described for the secure number generator of the first aspect of the invention. The key may be used as an identifier of the solid-state device, or for encrypting data exported or written by the solid-state device to a memory, or for both.

Different preferred embodiments of the method of the invention comprise performing the method during manufacture of the solid-state device or during first use of the device. The method may also be performed after the first use of the device, for instance, at the time when the solid-state device is required to provide or use the key for the first time. Other preferred embodiments of the method of the invention correspond to the additional features of the preferred embodiments of the secure number generator of the first aspect of the invention. One embodiment comprises triggering the random function unit to ascertain and write a new digital random code to said memory. Another embodiment comprises receiving a signal from an external source indicating that the memory shall be rewritten with a new digital random code. A further embodiment comprises programming a second section of the memory with a second digital code. Advantages of these embodiments have described above in connection with the corresponding embodiments of the secure number generator.

By way of example, the present invention can be used in the field of digital rights management (DRM) in connection with content distribution over data networks. Most known DRM systems use a multitude of identifiers to track the nature and origin of content items and to describe and classify it. Some of the identifiers are embedded into the content item or the multiplex containing the content, some are only associated with the content item. The identifiers used currently are embedded by central instances such as an original source of

the content, and many instances of content items with identical identifiers exist. These identifiers cannot be used to pin point specific hardware that may be compromised. Pin pointing offending hardware would be useful if it becomes possible to revoke specific hardware as proposed for emerging DRM systems. Current systems do not provide for a means to securely add tags locally to signify the state of the content item or of the local source.

Accordingly, in a third aspect the invention concerns a content distribution network, comprising at least one content source and a plurality of clients. The clients and the content server are adapted to communicate with each other for downloading or uploading one or more content items. The content source comprises a plurality of content items having content data. The content source and at least one content client are provided with a secure number generator according to the first aspect of the invention. The content source and at least one content client is adapted to add a digital random code stored in its respective secure number generator to a copy of the content item during or after downloading, before or during uploading, or during or after manipulating the content data of the copy of the content item.

The present aspect of the invention proposes to enable the secure adding of certain identifiers in the form of a digital random code by the device or application that imports (i.e., downloads), exports (i.e., uploads) or manipulates content data of a content item. For the transmission of data from a content source to a client the terms import and download are used with the same meaning herein. For the transmission of data from a client to a content source the terms export or upload are used herein with the same meaning. A client imports or downloads a copy of a content item from a content source. The terms download and upload shall not imply a determination of who initiates the data transmission. The client or the content source may initiate downloading. The initiation of an download process by a client is a request form well known from Internet usage. Initiation of an download by the content source is known from software update procedures, for instance within corporate content distribution networks. Also uploading content items may be initiated by either the content source or the client.

A content item provided by a content source need not be the original. It can be a copy of an original, or a second copy, and so on. One of the main advantages of the content distribution network of the invention is that it allows tracking the history of the individual copy. If the content item is a copy of an original item, it contains at least one identifier of the hardware the data has been imported from, and an identifier of the content source where it is presently stored. It is therefore possible to track the content history. Based an that history the

original content provider may not only track illegal use, but also award benefits to the owners or users and distributors of the featured ID's.

A further advantage of the proposed content distribution network is that the content data carry information about nature and state of source device, medium or DRM. If for instance a copy of an original is allowed but a copy of a copy not then embedding a source identifier could provide a receiving device with information about the legality of making a copy.

It is quite clear that a client cannot add its identifier to a copy of a content item before the downloading procedure has started. Therefore, the invention comprises adding the identifier during or after downloading. Correspondingly, the content source can add its identifier to a copy of a content item only before or during uploading the copy. Manipulating content data in the sense of the invention is any change of the content data, except for adding the random digital key stored in the secure number generator to the content data. Manipulating includes for instance rendering, encryption, or compression of at least a part of the content data.

The content distribution network of the present invention has at least one content source. The content source is in one embodiment a server connected to a database. The database comprises content items. A content item in the context of the present invention is a data file comprising coded information that can be reproduced for instance using an optical or acoustical reproduction technique or by a combination of optical and acoustical reproduction techniques. Typical examples of content items are data files encoding sound, music, a movie, a text document, a picture, a game, etc. or comprising an executable file, or a combination of the aforementioned. The content source of this embodiment is adapted to receive requests for transmission of one or several content items from clients comprised by the content distribution network and to transmit the content items to the requesting client, or another client, or to a number of clients at the same time, depending on the destination address for the content item given in the request.

Content items are in one embodiment of the content distribution network of the invention provided by more than one content source. For instance, several content sources are implemented in different countries to provide the same or different content items to clients. In one form of this embodiment of the content distribution network of the invention a client may be a content source at the same time, and vice versa. In this embodiment, a client and a content source are preferably implemented by respective software modules that may or may not be based on known applications such as an FTP server/client or an Internet browser.

The functionality of downloading or uploading or manipulating a content item is known from many applications. The feature of adding a secure identifier stored in the non-volatile memory of the secure number generator to a copy of a content item during or after downloading, before or during uploading, or during or after manipulating the content data of the copy of the content item is in one embodiment implemented as an additional software module extending the functionalities of one or more preexisting applications.

A hardware comprising both a client and a content source implementation is adapted to play both roles. In an alternative embodiment a certain solid-state device (hardware) can take only one role within the content distribution network, either content source or client. In different embodiments the clients take the form of solid state devices like an MP3 player, a personal digital assistant, a mobile phone, a computer, a CD or DVD player and/or burner, a digital video recorder, and the like. Communication between content source and client can be established by any known communication technique, cable-bound or wireless, optical or electrical, also by transportation of storage media storing a content item.

In one embodiment a DRM unit is provided communicating with the content source or the content client or both and adapted to allocate rights to perform defined actions with an individual copy of a content item to an individual hardware. A right can take the form of a string that encodes authorized uses for a content item. For instance a right may indicate that a certain song only plays if the medium storing the song is in a player with a specified identification number.

The possible roles a hardware may play are in a further embodiment controlled, preferably by a digital rights management unit connected to the content distribution network. The DRM unit allocates rights to individual solid-state devices comprised by the content distribution network. This may take the form of providing a combined client and content source implementation on a solid state device with the information that performing the content source implementation on the solid state device is prohibited, preferably with means in addition for prohibiting an attempt to perform the content source implementation.

In a preferred embodiment of the content distribution network of the invention, every content source and every client of the content distribution network of the invention is provided with a secure number generator of the invention. In this embodiment, tracking the distribution means that a content provider is able to read the distribution history of an individual copy of a content item from the content data. A content provider is, e.g., a publisher of the content, such as a record company. Every time a client imports an individual

copy of a content item content item, the content data is extended with a secure identifier. This way it is possible to pin point a device that provided an illegal copy of a content item. As a consequence, the secure number of the device may be revoked by the DRM unit, which will prohibit the further distribution of the copy from that hardware.

In another embodiment, not all clients have a secure number generator. For instance, it may be considered unnecessary to provide trusted clients such as clients under immediate control of a content provider with the embedding feature.

In a preferred embodiment the content source or the client or both are adapted to add to the digital random code at least one second digital code containing the following information item:

- that a content item has been imported or
- a device type of the importing client or
- a device type of the content source
- a type of an application or server implemented on the client or the content source
- an authorised type of use of the content item allocated to the client or
- an identifier of the content source or the client the content has been uploaded from or
- a combination of the previous information items.

The device type is, e.g., a disc type, a Sapphire-compliant CE player, a Digital Media X (DMX) player, an electronic content upload server. Including the device can be relevant if there are rules for manipulation of content items that restrict the right for manipulation to certain device types.

Information items specifying authorised usage are, e.g., an information element indicating an authorisation of a specific client to render the content data, and an information element indicating an authorisation to only read the content data.

In a further embodiment of the content distribution system, the content source or the content clients or both are adapted to add the digital random code by performing at least one of the following steps:

- watermarking the content item with the digital random code
- storing the identifier to a predefined location inside a multiplex containing the content
- storing the identifier in a header or a tail of a file containing the content

- storing the identifier in a separate file allocated to the content, such as in an (optionally encrypted) rights string as stored by the DRM unit.

A combination of the previous is for instance embedding the identifier (or a set of identifiers or additional coded information items) in a file header, tail or a separate file and embedding a message digest type of signature (hash) in the content stream with a watermark. This way a receiving application will know from the content stream that more information should be present and, if present, can check the validity of the information present. Another example of a combination is to embed a strong watermark indicating the presence of identifiers on another location. This way the disadvantage that watermarking cannot be used to accumulate a number of IDs in a content item can be avoided while using the advantages of watermarking in combination with hardware tracking according to the invention. Further, if a strong watermark is used, also the payload mark can be a fragile watermark as manipulations that invalidate the information in the watermark are always unauthorised manipulations.

It is noted that the content may be in compressed form, be it in as a part of a multiplex or not.

In a further embodiment the content source or the content clients or both are adapted to encrypt the content data using their respective digital random code. The predefined location inside the multiplex can be encrypted (for protection) or not (to ensure accessibility).

The content distribution system of the invention comprises in one embodiment a revocation authority adapted to communicate with the clients and to communicate a revocation to a specific client, wherein the clients are adapted to trigger their respective secure number generator to create a new digital random code upon receiving the revocation. The revocation authority is preferably the DRM unit mentioned earlier. The communication of the revocation may take the form of a predefined signal, a revocation file.

In a further embodiment the hardware of the device containing the secure number generator may be revoked by a corresponding predefined communication, e.g., a revocation file or signal. Reception of this communication triggers the erasure of the secure number registers and a shut down of the secure number generator, or of the device holding the secure number generator.

Further features and advantages of the invention are described below with reference to the figures.

Fig. 1 is a simplified block diagram showing a preferred embodiment of the secure number generator of the invention.

Fig. 2 is a flow diagram showing a preferred embodiment of the method of the invention

Fig. 3 is a schematic diagram showing a content distribution network of the invention

Fig. 4 shows the structure of a database of the content distribution network of the invention and the content items stored therein.

Fig. 1 is a simplified block diagram showing a preferred embodiment of the secure number generator 10. The secure number generator has a random function unit 12 comprising a random circuit 14. Random circuit 14 implements a non-linear electrical circuit exhibiting chaotic behaviour. The output of random circuit 14 is connected to a random function controller 16 also comprised by random function unit 12. Random function controller 16 is connected with a first MRAM register 18. The secure number generator further has a second MRAM register 20 connected with a control unit 22. Control unit 22 has an interface for receiving control data and user data from external sources and for providing the code stored in MRAM registers 18 and 20 as an output, as indicated in Fig. 1 by a single-lined arrow (control data) and a double-lined arrow (user data). User data can only be forwarded to MRAM register 20. There is no connection between control unit 22 and MRAM register 18 that allows a write operation of the user data received from an external source. This ensures that the MRAM register 18 cannot be overwritten with a code other than a new random code generated by random function unit 12.

The secure number generator 10 is a circuit module (IP) that can be implemented in connection with other modules in an integrated circuit (IC). All other modules of such an IC are external sources of signal or user data.

In operation, the operation of the random circuit 14 is triggered by a control signal provided by control unit 22. Control unit 22 sends an initial trigger signal to random circuit 14 when power is supplied to the random generator 10 for the first time. Later on, control unit 14 triggers the random circuit whenever the latter receives a control message from an external source indicating that a new random code is to be generated.

Upon reception of a trigger signal random circuit 14 provides a voltage value of the electrical circuit that exhibits chaotic behaviour at its output. Random function controller 16 reads the voltage value and transforms it into a digital random code. Depending on the desired length of the digital random code, these steps are repeated until the predefined number of random code bits has been determined. The generated digital random code is written to MRAM register 18.

The control unit 22 writes incoming user data received at its interface to second MRAM register 20. MRAM register 20 can for instance be used to extend the digital random code in first MRAM register 18 by an identifier specifying, e.g., the manufacturer of the IC containing the secure number generator. The combination of the codes in MRAM registers 18 and 20 forms a globally unique secure identifier, if, of course, a large enough length of the digital random code in MRAM register 18 is chosen. As an alternative, MRAM register 20 holds a globally unique number already. Then the code length of the secure number in MRAM register 18 is not an issue for the uniqueness of the complete number.

The secure number generator is in an alternative embodiment extended to generate and store several different digital random codes. The MRAM register 18 has a corresponding number of memory cells. Controller 16 is adapted to manage the allocation of different memory sections of MRAM register 18 to the different identifiers and to write a specified identifier to a corresponding section. In addition, the control unit 22 is adapted to manage requests to read or to renew a specific identifier. This embodiment is useful for instance in a content distribution system which prescribes a content client to use of different identifiers for downloading and uploading content items.

Another alternative embodiment has a basic random code in MRAM register 18 and several code annexes indicating different content uses in different sections of MRAM register 20. A combination of the basic random code with a specific annex is provided as the output by control unit 22, given a corresponding content use.

Fig. 2 shows a flow diagram of an embodiment of the method of the invention. In a step S10 a current random value of an unstable physical random quantity is measured. In a step S12 the measured value is transformed into a digital random code. As an example, an analog-digital converter can be used to perform step S12. The measured value forms the analog input, the digital random code forms the output. In a following step S14 the digital random code is written to an MRAM register. Of course, an MRAM register is mentioned here as an example. Any other type of non-volatile memory is equally suitable. With step S14 one cycle of operation of the method of the invention is finished. The present embodiment of

the method has a step S16 of watching for a trigger signal to restart code generation. If such a trigger signal is received, code generation is started again with step S10.

Fig. 3 is a schematic diagram showing an embodiment of a content distribution network according to the invention. The content distribution network comprises content servers forming content sources. Content servers are represented in Fig. 3 by boxes with double outlines, such as the content server 32. Content server 32 is connected with a database 34 that stores content items. Examples of content servers are an internet server or a retail stop based jukebox.

The content distribution network also comprises clients. Clients are represented by boxes with single outlines, such as clients 36 through 46. Client 46 is connected with a local database 48. In addition, there is a combined server/client device 50 with a database 52.

An oval shape 54 represents the communication network through which the data exchange between content servers and clients takes place. Lines connecting the individual boxes with the oval shape 54 indicate connection of the individual clients and servers through the communication network 54.

Communication through network 54 may be performed using packet switching or circuit switching. As an alternative to a data communication through communication network 54, a direct link between a content server and a client can be established, for instance using a local network connection. This is indicated by the direct connection between content server 32 and client 36.

Content clients 42 and 44 are connected with the network through a local content proxy server 46. The local proxy server 46 takes the role of a client in communication with other content servers such as content server 32. In communication with local clients 42 and 44 it is a content server. A local content proxy server is useful for instance in larger companies working in the field of content rendering. The clients 42 and 44 may in that example represent workstations implementing content rendering software.

For communication between content servers and content client 40 a wireless communication link is used between client 40 and a base station 56 of a wireless communication network, indicated by the antennas 58 and 60 and the dashed line between client 40 and base station 56.

All content servers, databases, and clients in content distribution network 30 have a secure number generator. This is indicated by small boxes with reference numbers SNG 1 through SNG 13.

As a first example of operation of the content distribution network 30 consider client 40. For the purpose of the present example client 40 is a single chip MRAM based MP3 player. Its secure number generator SNG10 has an embedded unique identifier, referred to as identifier A in the following. Server 32 is a retail stop based jukebox having an identifier B.

Before the MP3 player 40 downloads content from jukebox 32 it sends identifier A through a secure authenticated communication channel provided by communication network 54 and the wireless network provider MP3 player has subscribed to. Jukebox 32 maintains a "black list" of identifiers that have been revoked. A reason for revocation of an identifier is for instance an illegal distribution of a content item by the corresponding device.

If the content dispenser, the jukebox, ascertains that identifier A is not on his black list it embeds identifier A into the audio data stream that is downloaded as a requested content item to the MP3 player 40. For embedding the identifier using watermarking is used. As an option the identifier of jukebox 32 can also be implemented, with an additional annex indicating that the content item was downloaded from jukebox 32.

If the jukebox determines that identifier A is compromised it will not transmit the requested content item. Instead, it will invoke revocation of the identifier A. For revocation, a revocation procedure provided by a DRM system or DRM enabeling technology is used, for instance the secure digital storage standard Sapphire.

For the purpose of another example, client/server 50 is a CE player, i.e. a pocket player based on the operation system "Windows CE". It is adapted to redistribute downloaded content items.

The present example differs from the last in the following features: If CE player 50 downloads a content item from content server 32, attached to the multiplex containing the compressed audio data there is a table of identifiers encrypted in the same key as the content. Each record in the table has two fields. The first field specifies the type of identifier, the second the identifier itself. A robust watermark in the audio stream indicates that the identifer table must be present. The original provider of the content has written its own identifier in the first record of the table.

If the file is read by CE player 50 and exported to another device, then the original recipient 50 writes its ID in the second record. As an feature that can optionally be implemented, it may also write a source type ID (disc), a device type ID (CE player) in the following records. If each subsequent device that handles the file writes its identification in

the file than a history of the copy of the content item is compiled. Based an that history the original content provider may award benefits to the owners of the featured ID's. This can be accomplished using a transaction server (not shown) that is contacted for activation of content or for paying for the content. The transaction server may retrieve the history and dispense credits based on it.

Fig. 4 shows schematically the structure of files contained in a storage medium 60 of a content source or a client. The storage medium 60 contains content files 62, 64, and 66. In addition, there is a file 68 used to store tracking data.

The structure of content file 66 when transmitted in a content stream is shown below the block representing storage medium 60. The content stream has a stream header 70, a number of data packets, and a stream tail 78. Only the first data packet 72, the last data packet 74 and an intermediate data packet 76 of the content stream are given reference numbers. The intermediate data packet 76 is chosen as an example to show the data structure of a data packet. A packet has a packet header 80, content data section 82, and a packet tail 84. The stream header 70, the stream tail 78, the packet headers 80 and the packet tails provide space for storing identifiers.

CLAIMS:

1. Secure number generator (10, SNG 1...10), comprising a random function unit (12) and a non-volatile memory (18, 20) connected to said random function unit,

- wherein the random function unit (12) implements an unstable, measurable random quantity (14), such that a repeated measurement of the random quantity results in different random values, and

- wherein the random function unit (12) is adapted to ascertain a current random value of the random quantity (14), to transform the current random value into a digital random code, and to write said digital random code to a first section (18) of said non-volatile memory.

2. The secure number generator of claim 1, comprising a control unit (22) connected with the random function unit (12) and being adapted to trigger the random function unit to ascertain and write a new digital random code to said memory (18).

3. The secure number generator of claim 2, wherein the control unit (22) is adapted to receive a signal from an external source indicating that the memory shall be rewritten with a new digital random code.

4. The secure number generator of claim 1, wherein the memory has a second section (20) separate from said first section and an input connected with said second section and not said first section, and wherein the memory is adapted to be programmed with a second digital code in said second section (20) through said input.

5. The secure number generator of claim 1, wherein the non-volatile memory (18, 20) is an MRAM register.

6. The secure number generator of claim 1, wherein the random quantity (14) is selected from the group of

- a bit sequence of a maximum length sequence coupled to a free-running ring-

oscillator,

- an output quantity of non-linear electrical circuit exhibiting chaotic behaviour,
- an output quantity of an electrical circuit reading physical noise,
- a set of bits provided by an array of MRAM cells having an uncertain cell state.

7. A solid-state device (32, 36, 38, ..., 52), comprising the secure number generator (10, SNG 1, ...SNG 10) of claim 1.

8. A watermark embedder, comprising the secure number generator of claim 1.

9. An encryption device, comprising the secure number generator of claim 1.

10. A method for creating a unique identifier code of a solid-state device, comprising the steps of

- measuring a current random value of a random quantity that is integrated into the solid state device (S10),
- transforming the current random value into a digital random code (S12), and
- writing said digital random code to a first section of a non-volatile memory that is integrated into the solid-state device (S14),

wherein said random quantity is an unstable, measurable random quantity, such that a repeated measurement of the random quantity results in different random values, and wherein the solid-state device performs the measuring, transforming and writing steps.

11. A content distribution network, comprising at least one content source (32) and a plurality of clients (36, 38, 40, 42, 44) adapted to communicate with the content source (32) or with each other or both for downloading or uploading one or more content items, wherein the content source (32) comprises a plurality of content items (62, 64, 66) having content data (76, 82),

wherein the content source (32) and at least one content client is provided with a secure number generator (SNG1, ..., SNG 10) according to claim 1,

and wherein the content source (32) and at least one content client is adapted to add a digital random code stored in its respective secure number generator to a copy of the content item

(66) during or after downloading, before or during uploading, or during or after manipulating the content data (82) of the copy of the content item.

12. The content distribution system of claim 11, wherein the content source or the content clients or both are adapted to add to the digital random code at least one second digital code containing the following information item:

- that a content item has been imported or
- a device type of the importing client or
- a device type of the content source
- a type of an application or server implemented on the client or the content source
- an authorised type of use of the content item allocated to the client or
- an identifier of the content source or the client the content has been uploaded from or
- a combination of the previous information items

13. The content distribution system of claim 11, wherein the content source or the content clients or both are adapted to add the digital random code by performing one or more of the following steps:

- watermarking the content item with the digital random code
- storing the identifier to a predefined location inside a multiplex containing the content
- storing the identifier in a header or a tail of a file containing the content
- storing the identifier in a separate file allocated to the content.

14. The content distribution system of claim 11, wherein the content source or the content clients or both are adapted to encrypt the content data using their respective digital random code.

15. The content distribution system of claim 11, comprising a revocation authority adapted to communicate with the clients and to send a revocation signal to a specific client, wherein the clients are adapted to trigger their respective secure number generator to create a new digital random code upon receiving the revocation signal.

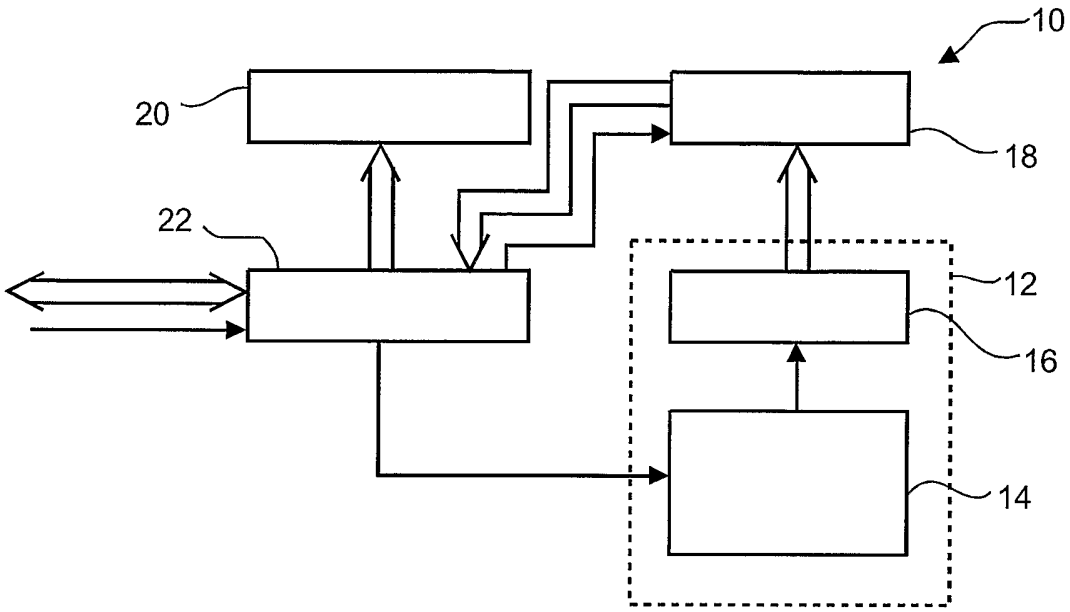

10
20
18
22
12
16
14

FIG.1

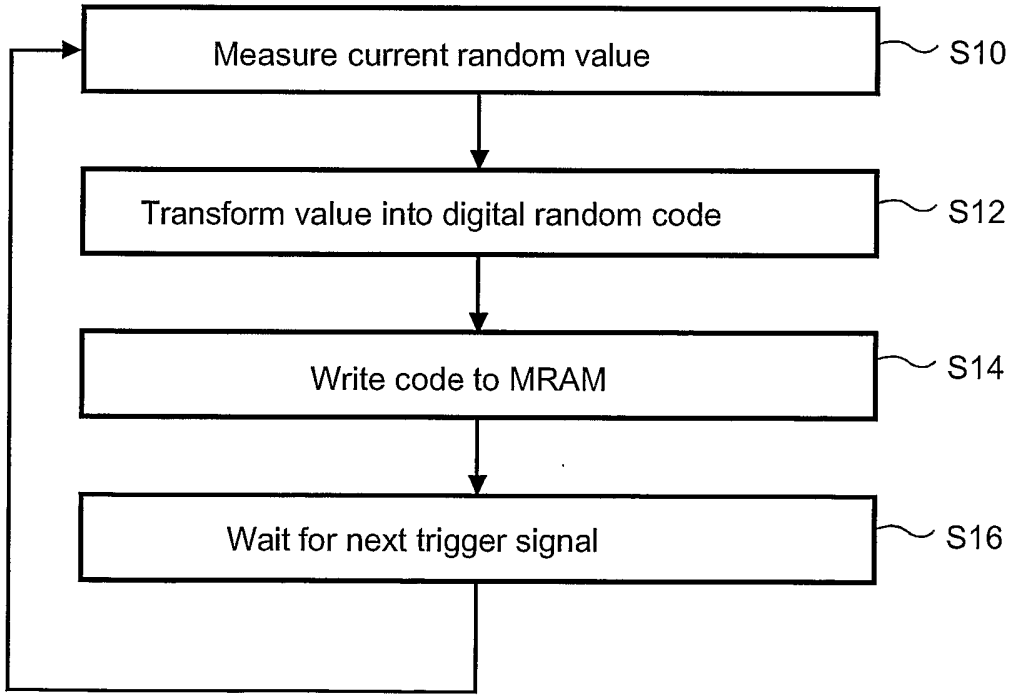

Measure current random value
S10
Transform value into digital random code
S12
Write code to MRAM
S14
Wait for next trigger signal
S16

FIG.2

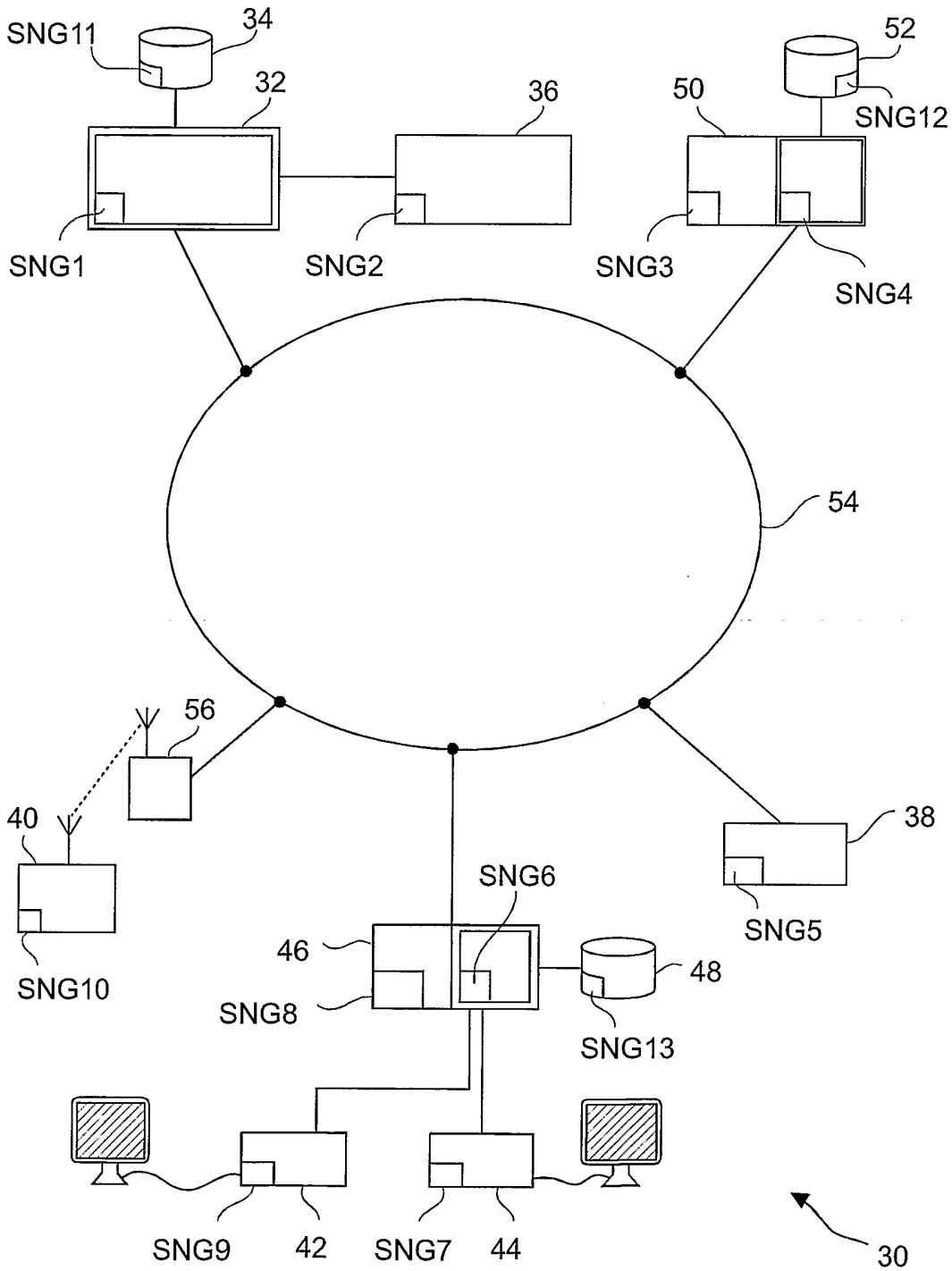

SNG11
34
32
36
52
50
SNG12
SNG1
SNG2
SNG3
SNG4
54
56
40
38
SNG6
SNG5
46
48
SNG8
SNG13
SNG10
SNG9
42
SNG7
44
30

FIG.3

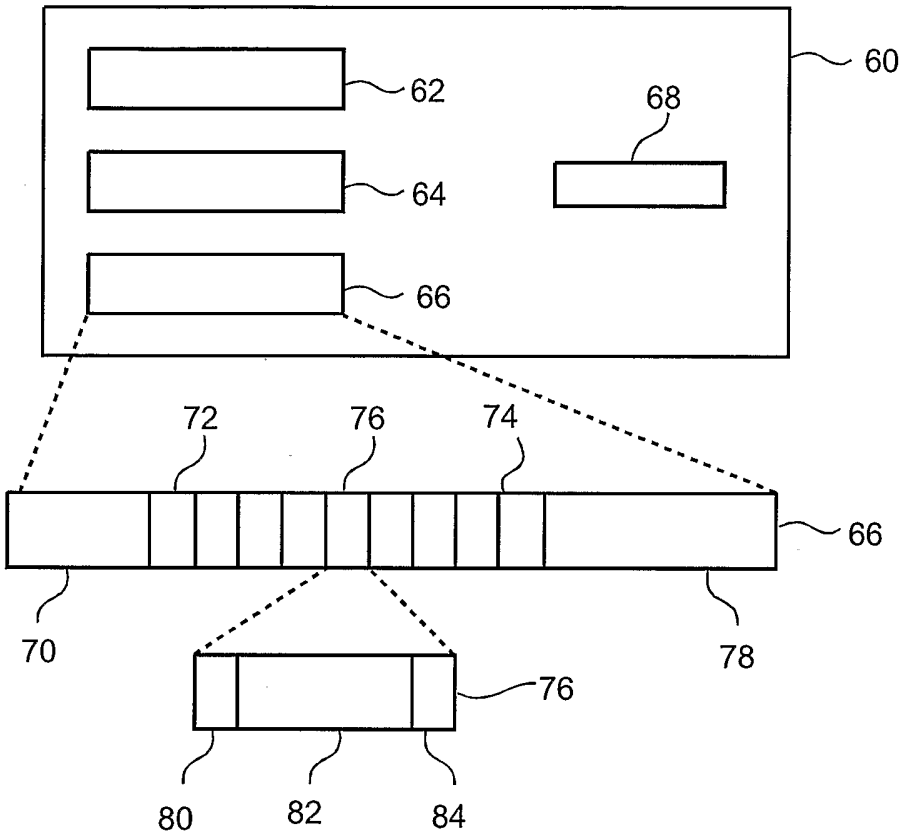


FIG.4