TITLE OF THE INVENTION

METHOD AND APPARATUS FOR PROTECTING DIGITAL DATA BY DOUBLE RE-ENCRYPTION

FIELD OF THE INVENTION

The present invention relates to a system for managing digital contents, and in particular, to a system used for managing copyrights of the digital contents, which claim the copyrights, and for protecting the secrecy of the digital contents so as to develop digital contents distribution and to realize digital contents economics.

PRIOR ART

Hitherto widely spread analog contents are deteriorated in quality each time when they are stored, copied, edited and transferred, and hence, no serious problem in the copyright occurs during these operations. However, the digital contents are not deteriorated in quality after repeatedly stored, copied, edited and transferred, and the control of the copyright is an important issue.

Digital data such as digital video data, digital audio data, etc. is mostly supplied to users on pay basis by broadcasting, by a DVD, etc. In such a case, the data is encrypted and supplied to exclude the viewing without paying a fee. The encrypted and supplied digital data is decrypted by using a crypt key, which is supplied to the user by certain means, and the data is viewed. Because the quality of the decrypted digital data is not deteriorated even when it is stored, copied or transferred, if the data is stored, copied or transferred by the user, secondary viewing free of charge may occur. Re-use of the decrypted digital data contents is against the benefit of the data contents provider. In this respect, relating systems and equipments have been developed to prohibit re-using, i.e., secondary utilization such as storage, copying or transferring the digital data content.

However, the prohibition of the secondary utilization comes less attractive for the users in using the digital data contents and it is now recognized that this may hinder the propagation of the use of the digital data contents. In this respect, it is now proposed to prevent illegitimate use by re-encrypting the decrypted digital data content so that the use of the digital data content is more attractive for the users.

When the digital data, which is stored in a medium and is given or lent to a user or which is transferred to the user, is used for secondary utilization such as storing, copying or transferring it, it is impossible for the copyright owner to protect him(her)self the copyright of the digital data, which is at hand of the users. Therefore, it is required to protect the copyright automatically and forcibly by a certain method.

Under such circumstances, the present inventor has made various proposals with the purpose of protecting the digital content copyrights.

In Japanese Patent Laid-Open Publications 46419/1994 (GB-2269302; USSN 08/098,415) and 141004/1994 (USP5,794,115; USP5,901,339), the present inventor has proposed a system for managing copyrights by obtaining a permit key from a key control center via a public telephone line, and also, an apparatus for such a purpose in Japanese Patent Laid-Open Publication 132916/1994 (GB-2272822; USSN 08/135,634).

Also, in Japanese Patent Laid-Open Publications 271865/1995 (EP0677949A2; USSN 08/416,037) and 185448/1996 (EP0704785A2; USSN 08/536,747), a system for copyright management of the digital contents has been proposed.

In these systems and apparatus, those who wish to view an encrypted program requests viewing to a management center via a communication line using

a communication device. Upon receipt of the request of viewing, the management center transmits a permit key and charges and collects a fee.

Upon receipt of the permit key, the requestor transmits the permit key to a receiving device by on-line or off-line means. When the permit key is received, the receiving device decrypts the encrypted program by using the permit key.

The system described in Japanese Patent Laid-Open Publication 271865/1995 (EP0677949A2; USSN 08/416,037), uses a program for managing the copyright and copyright information, in addition to a key for the use permission, to manage the copyright of the digital contents in displaying (including process to sound), storing, copying, editing and transferring the digital contents, including real-time transmission of digital video contents, in a database system. The program for copyright management watches and manages in a manner that the digital content is not used outside the permission or user's requests.

Japanese Patent Laid-Open Publication 271865/1995 (EP0677949A2; USSN 08/416,037) describes that the digital content is supplied from a database in the encrypted state and is decrypted by the copyright management program only when it is displayed or edited, and is again in the encrypted state when it is stored, copied or transferred. Further, it describes that the copyright management program itself is encrypted and is decrypted by using a permit key, and the decrypted copyright management program performs decryption and encryption of the copyrighted data, and that, when utilization other than storing and displaying the data is performed, copyright information including information of a person who has performed the utilization is added to the original copyright information and stored as a history.

Japanese Patent Laid-Open Publication 287014/1996 (USP5,867,579; EP0715241A2) has proposed an apparatus for decryption/re-encryption having a

configuration of a board, a PCMCIA card, an IC card or an IC for the copyright management and a crypt key escrow system. This application also describes the copyright management method applying to a video conference system and an electronic commerce system. USP5,805,706, also describes an apparatus for decryption/re-encryption having a configuration of an IC.

Japanese Patent Laid-Open Publication 272745/1996 (USP5,646,999; EP0709760)has proposed a system, in which a copyright of original data of edited data by using a plurality of data and the copyright of edited data are protected by confirming validity of the use request according to a digital signature on an edit program by combining a secret-key cryptosystem and a public-key cryptosystem.

Japanese Patent Laid-Open Publication 288940/1996 (USP5,740,246; EP0719045A2)has proposed various forms for applying the copyright management system to a database system, a video-on-demand (VOD) system or an electronic commerce system.

Japanese Patent Laid-Open Publication 329011/1996 (USP5,848,158; EP0746126A2)has proposed a system, in which copyrights of original data and new data are protected by using a third crypt key and a copyright label in case of using and editing a plurality of data.

As it can be understood from the data copyright management systems and the data copyright management apparatus proposed by the present inventor as described above, the management of data copyrights can be accomplished by encryption/decryption/re-encryption and limiting the usage by the copyright management program. The cryptography technique and limitation of the usage can be realized by using a computer.

In a case where secret information is exchanged via a network, the information is encrypted for preventing piracy.

It is described in USPs5,504,818 and USP5,515,441 that the information piracy during transmission is prevented by encryption. Using a plurality of keys in such a case is described in USPs5,504,816, 5,353,351, 5,475,757 and 5,381,480, and performing re-encryption is described in USP5,479,514.

The protection of the copyright in the secondary utilization of the digital data by the copyright management program can be realized by re-encryption/re-decryption of the decrypted digital data and by managing and performing the re-encryption/re-decryption by using the copyright management program.

It is needless to say that as the means for carrying out re-encryption/re-decryption there are the cases where a software is used and where a hardware is used.

Here, the operation to obtain encrypted data C from non-encrypted data M by using a key K is expressed as:

$$C=E(M, K),$$

and to obtain decrypted data M from encrypted data C by using the key K is expressed as:

$$M=D(C, K).$$

When re-encryption/re-decryption of the decrypted data M is repeated, re-encryption is expressed as:

$$\forall i: Ci=E(D(Ci-1, Ki-1), Ki),$$

where i is a positive integer, and re-decryption is expressed as:

$$\exists: M=D(E(Ci-1, Ki-1), Ki).$$

Referring to Fig. 1, description will be given on an arrangement of a set-top box (STB) conventionally proposed and on a method for protecting the digital data performed in the set-top box.

The description is not given here on peripheral circuits not directly related to encryption/decryption, e.g., an amplifier unit and a compression/decompression unit.

In Fig. 1, reference numeral 1 represents the digital data supplied by broadcasting means such as digital terrestrial wave broadcasting, digital CATV broadcasting, digital satellite broadcasting, etc., by network means such as Internet, or by a digital storage medium such as a DVD, a CD, etc. The data is encrypted by using a first changeable key K1 to prevent illegitimate use:

$$C1=E(M, K1)$$

and is supplied to a set-top box 2.

When the encrypted digital data C1 is supplied to the set-top box 2, the encrypted digital data C1 is decrypted at a decryption unit 3 by using the first changeable key K1 obtained from a key center via the same route as or via a different route from that of the encrypted digital data C1:

$$M=D(C1, K1)$$

and data M thus decrypted is outputted to a display unit 4 or the like.

In a case where the decrypted data M is stored in a medium such as a digital video disk (DVD) RAM or a hard disk, etc., or it is transferred outside via a network, the decrypted data M is re-encrypted at an encryption unit 6 of an unchangeable key encryption/decryption unit 5 by using an unchangeable key K0:

$$\forall 0: C0=E(M, K0)$$
$$=E(D(C1, K1), K0)$$

and re-encrypted data C0 is stored in or transferred to an external device 8.

In a case where the re-encrypted data C0 is used again, the re-encrypted data C0 read from a storage medium of the external device 8 or transferred via the network is re-decrypted by using the unchangeable key K0 at a decryption unit 7 of the unchangeable key encryption/decryption unit 5:

$$\exists : M = D(C0, K0)$$
$$= D(E(D(C1, K1), K0)$$

and the decrypted data M is outputted to the display unit 4 or the like.

In this case, in order to ensure security, it may be arranged in such a manner that the re-encrypted data C0 in the storage medium is erased when the re-encrypted data C0 is read from the storage medium via a route shown by a broken line in the figure and that the data re-encrypted again by using the unchangeable key K0 is re-stored.

In USP5,805,706, an integrated circuit for performing re-encryption/re-decryption is described.

In the set-top box as arranged above, it is easy to handle because re-encryption/re-decryption is automatically carried out by the hardware by using the unchangeable key K0, and it is effective for forcible re-encryption/re-decryption of the digital data, which must be protected.

However, as the unchangeable key K0 is placed in the device, and there is possibility that the unchangeable key K0 may be known to others, it may become impossible to protect the digital data thereafter.

SUMMARY OF THE INVENTION

To solve the above problem, present invention provides a method and an apparatus for double re-encrypting the data by using a changeable key in addition to re-encrypting by using an unchangeable key.

In use of the unchangeable key and the changeable key, there are cases where the changeable key is used first and the unchangeable key is then used, and

where the unchangeable key is used first and the changeable key is then used.

The key used first when re-encrypting is used finally when decrypting, and accordingly, even if data, which is subsequently re-encrypted, is cryptanalyzed, security is highly ensured. Therefore, in a case where a changeable key is used first and next, an unchangeable key is used for re-encryption, the possibility that the changeable key is known to others is very low even when the unchangeable key has been known to the others.

In the aspects of the embodiments, there are the cases executed by a software and by a hardware, and further, by a combination of the software and the hardware. In case of the hardware, a hardware using the unchangeable key developed for digital video can be used.

In a case executed by the software, in order to ensure the security of the program and the key used, encryption/decryption is performed in a region under a kernel which the users cannot handle. More concretely, encryption/decryption is performed at a filter driver, a device driver, i.e., a disk driver/network driver, and a real-time OS using HAL in an I/O manager. There are two filter drivers with a file system driver interposed between them, and either one of the filter drivers may be used, or both may be used.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows a general arrangement of a conventionally proposed set-top box;

Fig. 2 shows a general arrangement of a first embodiment of the present invention applied to a set-top box;

Fig. 3 shows a general arrangement of a second embodiment of the present invention applied to a set-top box;

Fig. 4 shows a general arrangement of a third embodiment applied to an

apparatus using a personal computer;

Fig. 5 shows a general arrangement of a fourth embodiment applied to an apparatus using a personal computer;

Fig. 6 is a drawing to give detailed explanation for the fourth embodiment; and

Fig. 7 shows a general arrangement of a fifth embodiment applied to an apparatus using a personal computer.

Fig. 8 shows a general arrangement of a sixth embodiment set-top box, which is a variation of the first embodiment;

Fig. 9 shows a general arrangement of a seventh embodiment set-top, which is a variation of the sixth embodiment;

Fig. 10 shows a general arrangement of an eighth embodiment using a personal computer;

Fig. 11 illustrates a detailed description on the eighth embodiment;

Fig. 12 illustrates an embodiment of a copyright management apparatus;

Fig. 13 illustrates another embodiment of the copyright management apparatus; and

Fig. 14 illustrates still another embodiment of the copyright management apparatus.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The following describes embodiments of the present invention.

Referring to Fig. 2, description will be given on an arrangement of a set-top box (STB) of a first embodiment of the present invention, and a method for protecting the digital data in the set-top box.

In the set-top box of this embodiment, similarly to the case of the conventional set-top box example as shown in Fig. 1, description is not given on peripheral circuits not directly related to encryption/decryption, e.g., an amplifier unit, a compression/decompression unit and an interface unit for the outside.

The difference of the present embodiment from the conventionally proposed set-top box shown in Fig. 1 is that a changeable key encryption/decryption unit 19 for performing encryption/decryption by using a second changeable key K2 is inserted between an unchangeable key encryption/decryption unit 15 for performing encryption/decryption by using the unchangeable key K0 and a decryption unit 13.

In Fig. 2, reference numeral 11 represents digital data supplied by broadcasting means such as digital terrestrial wave broadcasting, digital CATV broadcasting, digital satellite broadcasting, etc., by network means such as Internet, or by digital storage medium such as a DVD, a CD, etc. The digital data is encrypted by using a first changeable key K1 to prevent illegitimate use:

$$C1=E(M, K1)$$

and is supplied to a set-top box 12.

When the encrypted digital data C1 is supplied to the set-top box 12, the encrypted digital data C1 is decrypted at the decryption unit 13 by using the first changeable key K1 obtained from a key center via the same route as or via a route different from that of the encrypted digital data C1:

$$M=D(C1, K1)$$

and the decrypted data M is outputted to a display unit 14 or the like.

In a case where the decrypted data M, for which the copyright is claimed, is stored in an external device 18, i.e., in a medium of a digital video disk (DVD) RAM or a hard disk, or in a case where the data is transferred to the outside via a network, the decrypted data M is re-encrypted by using a second changeable key K2 at an encryption unit 20 of the changeable key encryption/decryption unit 19:

$$\forall 2: C2=E(M, K2)$$
$$=E(D(C1, K1), K2),$$

further, the re-encrypted data C2 is double re-encrypted by using an unchangeable

key K0 at an encryption unit 16 of the unchangeable key encryption/decryption unit 15:

$$\forall 2\text{-}0: C2\text{-}0 = E(C2, K0)$$
$$= E(E(D(C1, K1), K2), K0),$$

and the data is stored in the external device 18 or transferred as double re-encrypted data C2-0.

In a case where the double re-encrypted data C2-0 is used again, the re-encrypted data C2-0 read from the storage medium of the external device 18 or transferred via a network is re-decrypted at a decryption unit 17 of the unchangeable key encryption/decryption unit 15 by using the unchangeable key K0:

$$\exists 2: C2 = E(C2\text{-}0, K0)$$
$$= D(E(E(D(C1, K1), K2), K0),$$

further, the re-decrypted data C2 is decrypted by using the second changeable key K2 at a decryption unit 21 of the changeable key encryption/decryption unit 19:

$$\exists: M = D(C2, K2)$$
$$= D(E(D(C1, K1), K2),$$

and the decrypted data M is outputted to the display unit 14 or the like.

In this case, in order to ensure the security, it may be arranged in such a manner that, when the re-encrypted data C2-0 is read from the storage medium via a route shown by a broken line in the figure, the re-encrypted data C2-0 in the storage medium is deleted and the data re-encrypted by using the changeable key K2 and the unchangeable key K0 is re-stored.

As described above, because the re-encryption using the second changeable key K2 is performed before the re-encryption using the unchangeable key, even when the unchangeable key K0 has been known to others, as the data is also encrypted by using the second changeable key K2, it is very difficult to

cryptanalyze the encrypted data by further finding out the second changeable key K2.

Also, the second changeable key K2 is first used for re-encryption, and it is again used for re-decryption after the unchangeable key K0 is used for double re-encryption and re-decryption. Accordingly, the security of the second changeable key K2 is highly ensured, and because it is used first, it strongly governs the encrypted data at the most effective manner.

In the description of the above embodiment, the encryption unit 20 and the decryption unit 21 are contained in the changeable key encryption/decryption unit 19 and the encryption unit 16 and the encryption unit 17 are contained in the unchangeable key encryption/decryption unit 15, while it is needless to say that these units 16, 17, 20 and 21 may be separately provided.

The operation as above can be easily implemented by providing a computer arrangement having a CPU and a system-bus in the set-top box 12.

Now, referring to Fig. 3, description will be given on another arrangement of the set-top box, which is a second embodiment of the present invention, and also, on a method for protecting the digital data carried out in this set-top box.

In this second embodiment set-top box, similarly to the conventional set-top box example shown in Fig. 1, description is not given on peripheral circuits not directly related to encryption/decryption, e.g., an amplifier unit and a compression/decompression unit.

The difference of the second embodiment set-top box from the first embodiment set-top box shown in Fig. 2 is that the position is replaced with each other between the unchangeable key encryption/decryption unit 35 for

encryption/decryption using the unchangeable key K0 and the changeable key encryption/decryption unit 39 for encryption/decryption using the second changeable key K2.

This unchangeable key encryption/decryption unit 35 for encryption/decryption using the unchangeable key K0 is connected to a decryption unit 33 and a display 34, and an external changeable key encryption/decryption unit 39 for encryption/decryption using the second changeable key K2 is connected to an external device 38. The second changeable key K2 may be supplied from the outside or may be generated in the set-top box.

In Fig. 3, reference numeral 31 represents digital data supplied by broadcasting means such as digital terrestrial wave broadcasting, digital CATV broadcasting, digital satellite broadcasting, etc., by network means such as Internet, or by a digital storage medium such as a DVD, a CD, etc. The data is encrypted by using a first changeable key K1 to prevent illegitimate use:

$$C1=E(M, K1)$$

and is supplied to a set-top box 32.

When the encrypted digital data C1 is supplied to the set-top box 32, the encrypted digital data C1 is decrypted at the decryption unit 33 by using the first changeable key K1 obtained via the same route as or via a route different from that of the encrypted digital data C1:

$$M=D(C1, K1)$$

and the decrypted data M is outputted to a display unit 34 or the like.

In a case where the decrypted data M, which states the copyright, is stored in an external device 38, i.e., in a medium such as a digital video disk (DVD) RAM or a hard disk, etc., or is transferred to the outside via a network, the re-encrypted data C2 is re-encrypted by using the unchangeable key K0 at the

encryption unit 36 of the unchangeable key encryption/decryption unit 35:

$$\forall 0: C0 = E(M, K0)$$
$$= E(D(C1, K1), K0),$$

further, the decrypted data M is double re-encrypted at an encryption unit 40 of the changeable key encryption/decryption unit 39 by using the second changeable key K2:

$$\forall 0\text{-}2: C0\text{-}2 = E(C0, K2)$$
$$= E(E(D(C1, K1), K0), K2),$$

and double re-encrypted data C0-2 is stored in the external device 38 or transferred.

In a case where the double re-encrypted data C0-2 is used again, the re-encrypted data C0-2 read from the storage medium of the external device 38 or transferred via a network is re-decrypted by using the external changeable key K2 at the re-decryption unit 41 of the external changeable key encryption/decryption unit 39:

$$\exists: 0: C0 = E(C0\text{-}2, K2)$$
$$= D(E(E(D(C1, K1), K0), K2),$$

further, the re-decrypted data C0 is again re-decrypted by using the unchangeable key K0 at a decryption unit 37 of the unchangeable key encryption/decryption unit 35:

$$\exists: M = D(C0, K0)$$
$$= D(E(D(C1, K1), K0)$$

and the decrypted data M is outputted to the display unit 34 or the like.

In this case, in order to ensure the security, it may be arranged in such a manner that, when the re-encrypted data C2-0 is read from the storage medium via a route shown by a broken line in the figure, the double re-encrypted data C0-2 in the storage medium is erased and the data re-encrypted by using the unchangeable key K0 and the external changeable key K2 is re-stored.

As described above, because the re-encryption is performed using the second changeable key K2 before the re-encryption using the unchangeable key K0, even when the unchangeable key K0 has been known to others, as the data is also encrypted by using the second changeable key K0, it is very difficult to cryptanalyze the encrypted data by further finding out the second changeable key K0 K2.

In this arrangement, the changeable key encryption/decryption unit 39 is simply added to the unchangeable key encryption/decryption unit 35 of the conventionally proposed set-top box shown in Fig. 1, and accordingly, the set-top box can be easily designed.

In the description of this embodiment, the encryption unit 36 and the decryption unit 37 are contained in the unchangeable key encryption/decryption unit 35 and the encryption unit 40 and the encryption unit 41 are contained in the changeable key encryption/decryption unit 39, while it is needless to say that these units 36, 37, 40 and 41 may be separately provided.

The operation as above can be easily implemented by providing a computer arrangement having a CPU and a system-bus in the set-top box 32.

Digital data contents are handled not only in the set-top box but also in a computer such as a personal computer.

Referring to Fig. 4 through Fig. 7, description will be given on embodiments of the present invention applied to an apparatus using a personal computer.

Unlike the set-top box where all components are constituted of hardware and are operated only by the hardware, a personal computer is an apparatus, which is

operated by controlling the hardware incorporated in the apparatus using software.

In order to efficiently operate the computer, an operating system (OS) is used, which manages the overall operation of the computer.

A conventional type operating system used in the personal computer comprises a kernel for providing basic services such as memory management, task management, interrupting and communication between processes, and an operating system service providing other services.

On the other hand, with the changes on the computer side situations, for example, the function improvement of a microprocessor and price decreasing of a RAM used as a main memory, and also with the increase of performance ability of computers requested by users, the improvement of the functions of the operation system to manage the overall computer operation has been required. Then, the scale of the operating system has become comparatively larger than before.

Since such an enlarged operating system occupies itself larger space in the hard disk where it is to be stored, the space to store application programs or data needed by the user is liable to be rather limited, and that may lead to inconvenience for the user to use the computer.

To cope with such situations, in the newest operating system, it is often designed in such a manner that an environmental subsystem for performing emulation of the other operating system and graphics, and a core subsystem such as a security subsystem are removed from the kernel as the subsystem part, which depends on the user. And operating system is constituted as basic parts consist a micro-kernel such as a HAL (hardware abstraction layer) to absorb differences of hardware, a scheduling function, an interrupt function, an I/O management function, etc., and a system service API (application programming interface) is interposed

between the subsystem and the micro-kernel.

By the arrangement as above, expandability of the operating system required for the change or addition of functions is improved, and portability of the operating system corresponding to the intended purpose can be made much easier.

By the distributed arrangement of elements of the micro-kernel to a plurality of network computers, it is now possible to easily realize the distributed operating system.

Computers are used in computer peripheral units, various types of control units, communication devices, etc., in addition to personal computers typically represented by the desk-top type or notebook type personal computers. In such cases, unlike the operating system for a general-purpose personal computer, in which importance is put on man-machine interface, a real-time operating system is adopted, in which importance is placed on speedy execution, an operating system especially for embedding suitable for each of these units and devices.

As a matter of course, the cost for development is increased when developing an operating system specially for each of embedded different devices. For this reason, it is recently proposed to use a general-purpose operating system in the personal computer also for the embedded type real-time operating system. By arranging a program specific for embedded type in a subsystem combined with a micro-kernel, it is now practiced to obtain embedded type real-time operating system.

Major functions of the operating system include task management such as scheduling or interrupt processing.

The task management has mainly two different types in the operating system: single task type, which only performs one task processing at the same time, and multi-task type for performing a plurality of task processings at the same

time. The multi-task type is divided to multi-task type where changeover of the task depends upon the task to be processed, and multi-task type not dependent upon the task to be processed.

Among these, the single task type allocates one process to an MPU so that the MPU is not free until the process is completed. Non-preemptive multi-task type allows the MPU to be allocated a plurality of processes by time division, so that process is not executed unless the process in execution gives the control back to the operating system. Preemptive multi-task type interrupts the process in execution at a certain time interval, so that the control is forcibly transferred to the other process.

Therefore, real-time multi-tasking can be achieved only by the preemptive type.

The task management in the computer is carried out according to the process, which is a unit having system resources such as a memory, a file, etc., and the process is managed according to a thread, which is a unit to allocate CPU time with divided processes. In this case, the system resources are shared by all threads in the same process. This means that there are more than one thread to share the system resources in one process.

Each task to be processed by the multi-task type has priority spectrum, which is generally divided to 32 steps. The normal task performing no interrupt is classified to dynamic classes, which are divided to 0 - 15 steps, and the task performing interrupt is classified to real-time classes to be divided to 16 - 31 steps.

Interrupt processing is executed using interrupt enable time (normally 10 milliseconds) called as a "time slice" as a unit. Ordinary interrupt is executed at 10-millisecond time slice.

Under such circumstances, a time slice has been recently proposed, in which interrupt enable time called as a "real-time slice" is 100 microseconds. If this real-time slice is used, it is possible to execute interrupt with priority to the conventional interrupt of 10 milliseconds.

In a third embodiment shown in Fig. 4, changeable key encryption/decryption processing by a software and the management of a crypt key in the computer are carried out by a real-time OS in HAL.

In Fig. 4, reference numeral 51 represents an operating system in a computer; 56 a display unit for displaying output from the computer; 57 an unchangeable key encryption/decryption unit; and 58 a data storage medium such as a digital versatile disk (DVD) RAM or a hard disk, or a data transfer system such as a network.

The operating system 51 comprises an operating system service 52 and a system service API 53, which are a user region, and a kernel 54 and a HAL 55, which are a non-user region. The system service API 53 is arranged between the operating system service 52 and the kernel 54 and serves to mediate between the operating system service 52 and the kernel 54. The HAL 55 is arranged at the lowermost layer of the operating system 50 and serves to absorb differences between in the hardware for the software.

The operating system service 52 comprises an application 59, a subsystem 60 and a security subsystem 61. The kernel 54 comprises a plurality of micro-kernels 62 and 64 and a kernel 63. Micro-kernel 62 has task management functions such as scheduling, interrupt, etc., and the micro-kernel 64 has I/O management function.

The micro-kernel 64 having I/O management function comprises an I/O manager 65, device drivers such as a disk driver 67 and a network driver 68, which

are managed by the I/O manager, and a filter driver 66 which is inserted when necessary between the I/O manager 65 and the device drivers such as the disk driver 67 and the network driver 68.

The changeable key encryption/decryption processing in the computer is executed by a software. In case of the third embodiment, the changeable key encryption/decryption processing is carried out by the aforementioned real-time OS (RTOS) with priority to other tasks at the HAL 55 in the operating system 51.

Similarly to the first embodiment shown in Fig. 2, digital data supplied by broadcasting means such as digital terrestrial wave broadcasting, digital CATV broadcasting, digital satellite broadcasting, etc., by network means such as Internet, or by a digital storage medium such as a DVD, a CD, etc. is encrypted using a first changeable key K1 to prevent illegitimate use:

$$C1=E(M, K1)$$

and is supplied. The supplied encrypted digital data C1 is decrypted by the operating system service 52 by using the first changeable key K1 provided from the key center via the same route as or via a route different from that of the encrypted digital data C1:

$$M=D(C1, K1)$$

and the decrypted data M is outputted to the display unit 56 or the like.

In a case where the decrypted data M, which claims its copyright, is stored in a medium such as a digital versatile disk (DVD) RAM or a hard disk, or where it is transferred to the outside via a network, the decrypted data M is mandatorily re-encrypted at HAL 55 by using a second changeable key K2:

$$\forall 2: C2=E(M, K2)$$
$$=E(D(C1, K1), K2).$$

Further, the re-encrypted data C2 is double re-encrypted at the unchangeable key

encryption/decryption unit 57 by using an unchangeable key K0:

$$\forall 2\text{-}0: C2\text{-}0 = E(C2, K0)$$
$$= E(E(D(C1, K1), K2), K0),$$

and the double re-encrypted data C2-0 is stored in an external device or transferred. The changeable key K2 may be provided from the outside or may be generated in a set-top box.

When the double re-encrypted data C2-0 is utilized, the re-encrypted data C2-0 read from the storage medium or transferred via the network is re-decrypted using the unchangeable key K0 at the unchangeable key encryption/decryption unit 57:

$$\exists 2: C2 = E(C2\text{-}0, K0)$$
$$= D(E(E(D(C1, K1), K2), K0).$$

Further, the re-decrypted data C2 is decrypted using the second changeable key K2 at the HAL 55 having the changeable key encryption/decryption function:

$$\exists : M = D(C2, K2)$$
$$= D(E(D(C1, K1), K2),$$

and the decrypted data M thus obtained is outputted to the display unit 56 or the like.

The real-time OS is executed in priority to every other task. In the third embodiment, the real-time OS is implemented at the HAL, being a contact point with the hardware in the operating system. Accordingly, the re-encryption of the digital data is performed in a reliable manner, and it is impossible for the decrypted data M as it is to be stored into the external device or to be transferred. Also, re-encryption is performed using the second changeable key K2 before the re-encryption using the unchangeable key K0. As a result, even if the unchangeable key K0 is known, it is very difficult to cryptanalyze the encrypted data by finding out the second changeable key K2, as the data is also encrypted by

the second changeable key K2.

Because the second changeable key K2 is used first and is then used after the unchangeable key K0 has been used, the key security can be ensured. Because the second changeable key K2 is used first, it strongly governs the encrypted data.

The above operations can be easily implemented by arranging the unchangeable key encryption/decryption unit 57 as a sub-computer structure having a CPU and a system-bus.

In a fourth embodiment shown in Fig. 5, the changeable key encryption/decryption by a software in the computer is carried out at a filter driver 66 placed in the I/O management micro-kernel 64 in the kernel 54.

Fig. 6 shows an arrangement of the I/O management micro-kernel 64 with the filter driver 66 placed in it.

In the I/O management micro-kernel with no filter driver placed in it, a file system driver 69, an intermediate driver 70 and a device driver 71 are arranged from upper hierarchy to lower hierarchy. When necessary, a filter driver 66A or a filter driver 66B is placed above the file system driver 69 or between the intermediate driver 70 and the device driver 71.

Because it can be designed to have these filter drivers 66A and 66B perform re-encryption/re-decryption and management of the key, the filter drivers 66A or 66B is designed to carry out the re-encryption/re-decryption processing and the key management in this embodiment.

The filter driver is arranged, not in the operating system service unit 52 which the user can handle, but in the kernel 54 which the user cannot handle. On

the other hand, it is generally practiced to make the specification change to fit for the computer using the operating system. In particular, it is not very rare to change the I/O manager therein.

Utilizing the above, the modules having the function of re-encryption/re-decryption processing and the key management are placed in the I/O manager as the filter driver 66A or the filter driver 66B in the fourth embodiment.

Similarly to the first embodiment shown in Fig. 2, digital data supplied by broadcasting means such as digital terrestrial wave broadcasting, digital CATV broadcasting, digital satellite broadcasting, etc., by network means such as Internet, or by digital storage medium such as a DVD, a CD, etc. is encrypted using a first changeable key K1 to prevent illegitimate use:

$$C1=E(M, K1)$$

and it is supplied. The encrypted and supplied digital data C1 is decrypted by the operating system service unit 52 using the first changeable key K1 provided from the key center via the same route as or via a route different from that of the encrypted digital data C1:

$$M=D(C1, K1)$$

and the decrypted data M is outputted to the display unit 56 and the like.

In a case where the decrypted data M, which states its copyright, is stored in a medium such as a digital versatile disk (DVD) RAM or a hard disk, or in a case where it is transferred to the outside via a network, the decrypted data M is mandatorily re-encrypted at the filter driver 66A or 66B using the external changeable key K2:

$$\forall 2: C2=E(M, K2) = E(D(C1, K1), K2).$$

Further, the re-encrypted data C2 is double re-encrypted at the internal

unchangeable key encryption/decryption unit 57, using an unchangeable key K0:

$$\forall 2\text{-}0: C2\text{-}0 = E\ (C2, K0)$$
$$= E\ (E\ (D\ (C1, K1), K2), K0),$$

and double re-encrypted data C2-0 is stored into the external device or transferred. The changeable key K2 may be provided from the outside or may be generated in a set-top box.

When the double re-encrypted data C2-0 is utilized again, the re-encrypted data C2-0 read from the storage medium or transferred via the network is re-decrypted using the unchangeable key K0 at the internal unchangeable key encryption/decryption unit 57:

$$\exists 2: C2 = E\ (C2\text{-}0, K0)$$
$$= D\ (E\ (E\ (D\ (C1, K1), K2), K0).$$

Further, the re-decrypted data C2 is decrypted at the filter driver 66A or 66B, using the second changeable key K2:

$$\exists : M = D\ (C2, K2)$$
$$= D\ (E\ (D\ (C1, K1), K2)$$

and the decrypted data M thus obtained is outputted to the display unit 56 or the like.

The filter driver can be easily placed into the kernel of the operation system in a part of the I/O manager. In so doing, the function of the re-encryption/re-decryption processing and the key management can be easily incorporated in the operation system. Also, since re-encryption is performed using the second changeable key K2 before the re-encryption using the unchangeable key K0, even if the unchangeable key K0 is known to others, it is very difficult to cryptanalyze the encrypted data by finding out the second changeable key K0 because the data is also encrypted by the second changeable key K0.

Further, because the second changeable key K0 is used first, and is then, used after the unchangeable key K0 is used, the key security can be highly ensured. Also, because the second changeable key K2 is used first, it strongly governs the encrypted data.

The above operations can be easily implemented by arranging the unchangeable key encryption/decryption unit 57 as a sub-computer structure having a CPU and a system-bus.

In a fifth embodiment shown in Fig. 7, the changeable key encryption/decryption and the key management by a software in a computer are carried out at the disk driver 57 and the network driver 68 contained in the I/O management micro-kernel 64 in the operating system 51.

As already explained in connexion with Fig. 6, the file system driver 69, the intermediate driver 70, and the device driver 71 are arranged from upper hierarchy to lower hierarchy in the I/O management micro-kernel. The changeable key encryption/decryption processing and the key management can be carried out also in the device driver 71 positioned at the lowermost layer.

Similarly to the first embodiment shown in Fig. 2, the digital data supplied by broadcasting means such as digital terrestrial wave broadcasting, digital CATV broadcasting, digital satellite broadcasting, etc., by network means such as Internet, or by digital storage medium such as a DVD, a CD, etc. is encrypted using the first changeable key K1 to prevent illegitimate use:

$$C1=E\ (M, K1)$$

and it is supplied. The encrypted and supplied digital data C1 is decrypted by the operating system service unit 52 using the first changeable key K1 provided from the key center via the same route as or a route different from that of the encrypted digital data C1:

$$M=D(C1, K1)$$

and the decrypted data M is outputted to the display unit 56 or the like.

In a case where the decrypted data M, which states its copyright, is stored in a medium such as a digital versatile disk (DVD) RAM or a hard disk, or in a case where it is transferred to the outside via a network, the decrypted data M is mandatorily re-encrypted at the device driver 71, i.e., the disk driver 67 and the network driver 68, using the second changeable key K2:

$$\forall 2: C2=E(M, K2)$$
$$=E(D(C1, K1), K2).$$

Further, the re-encrypted data C2 is double re-encrypted at the unchangeable key encryption/decryption unit 57 using the unchangeable key K0 placed in the unchangeable key encryption/decryption unit 57:

$$\forall 2\text{-}0: C2\text{-}0=E(C2, K0)$$
$$=E(E(D(C1, K1), K2), K0),$$

and double re-encrypted data C2-0 is stored in the external device or transferred. The changeable key K2 may be provided from the outside or may be generated in a set-top box.

When the double re-encrypted data C2-0 is utilized again, the re-encrypted data C2-0 read from the storage medium or transferred via a network is re-decrypted using the unchangeable key K0 at the internal unchangeable key encryption/decryption unit 57:

$$\exists 2: C2=E(C2\text{-}0, K0)$$
$$=D(E(E(D(C1, K1), K2), K0).$$

Further, the re-decrypted data C2 is decrypted at the device driver 71, i.e., the disk driver 67 and the network driver 68, using the changeable key K2:

$$\exists: M=D(C2, K2)$$
$$=D(E(D(C1, K1), K2)$$

and the decrypted data M thus obtained is outputted to the display unit 56 or the like.

For the device driver, it is generally practiced to make the specification change to fit for the computer using the operating system or when the corresponding device has been modified.

As the function of the re-encryption/re-decryption processing and the key management is incorporated into such the device driver, it allows to easily incorporate the function into the kernel of the operating system. Also, since re-encryption is performed using the second changeable key K2 before the re-encryption using the unchangeable key K0, even if the unchangeable key K0 is known to others, it is very difficult to cryptanalyze the encrypted data by finding out the second changeable key K2 because the data is also encrypted using the second changeable key K2.

There is a possibility if the second changeable key K2 may be known to others, while it is repeatedly used. In such a case, it is preferably designed in such a manner that the second changeable key K2 used for encryption is abandoned and it is again generated when necessary for decryption, as described in Japanese Patent Laid-Open Publication 185448/1996 (EP0704885A2, USSN 08/536,749). If it is necessary to have the key for decryption, it should be obtained from the key center again.

For the security purpose, K1, K2 and K0 may be based on different crypt algorithm.

These operations can be easily implemented by arranging the unchangeable key encryption/decryption unit 57 as a sub-computer structure having a CPU and a system-bus.

In the embodiments described above, the second changeable key K2 and the unchangeable key K0 are used in addition to the first changeable key K1. In the embodiments described below, a third changeable key K3 is used additionally so that more reliable copyright management of digital contents is provided.

Referring to Fig. 8, description will be given on an arrangement of a set-top box in a sixth embodiment of the present invention, which is a variation of the first embodiment, and also on a method for protecting digital data carried out in the set-top box.

In the set-top box of this embodiment, similarly to the first embodiment set-top box, no description is given on peripheral circuits not directly related to encryption/decryption, e.g., an amplifier unit and a compression/decompression unit.

The set-top box of the sixth embodiment has a difference from that of the first embodiment in distinguishing between a case where the decrypted data M is stored in a storage medium 81 such as a hard disk, which is incorporated into or dedicated to the set-top box, and another case where the decrypted data M is stored in a removable medium, e.g., a DVD-RAM, in an external 82 or is transferred to the outside via a network.

The internal unchangeable key encryption/decryption unit 15 and further a changeable key encryption unit 80 are provided. In a case where the decrypted copyrighted data is stored, for example, in a hard disk as a storage medium 81, which is incorporated into or dedicated to the set-top box, it is double re-encrypted using an internal unchangeable key K0. On the other hand, in a case where it is stored in a removable medium, i.e., a DVD-RAM, or is transferred to the outside via the network, it is double re-encrypted, not by the internal unchangeable key K0 but by a third changeable key K3.

In Fig. 8, reference numeral 11 represents digital data, which is supplied by broadcasting means such as digital terrestrial wave broadcasting, digital CATV broadcasting, digital satellite broadcasting, etc., by network means such as Internet, or by a digital storage medium such as a DVD, a CD, etc. The digital data is encrypted using a first changeable key K1 to prevent illegitimate use:

$$C1=E(M, K1)$$

and encrypted digital data C1 is supplied to a set-top box 12.

When the encrypted digital data C1 is supplied to the set top box 12, the encrypted digital data C1 is decrypted at a decryption unit 13 using a first changeable key K1 obtained from a key center:

$$M=D(C1, K1)$$

and the decrypted data M is outputted to a display unit 14 or the like.

In a case where the decrypted copyrighted data M is stored in a storage medium 81 such as a hard disk, which is incorporated into or is dedicated to the set-top box 12, or in a removable medium such as a DVD-RAM, or where it is transferred outside via a network, the decrypted data M is re-encrypted at an encryption unit 20 of a changeable key encryption/decryption unit 19 using a second changeable key K2, which is obtained from the key center or generated in the set-top box 12:

$$\forall 2: C2=E(M, K2)$$
$$=E(D(C1, K1), K2).$$

In a case where the re-encrypted data C2 is stored in a hard disk of the storage medium 81 incorporated into or dedicated to the set-top box 12, the re-encrypted data C2 is double re-encrypted at an encryption unit 16 of an internal unchangeable key encryption/decryption unit 15 using an unchangeable crypt key

K0 placed in the internal unchangeable key encryption/decryption unit 15:

$\forall$ 2-0: C2-0=E (C2, K0)

=E (E (D (C1, K1), K2), K0)

and the double re-encrypted data C2-0 is stored in the storage medium 81 or the like.

When the double re-encrypted data C2-0 stored in the storage medium 81 is utilized, the re-encrypted data C2-0 read from the storage medium 81 is decrypted using the unchangeable crypt key K0 placed in a decryption unit 17 of the internal unchangeable key encryption/decryption unit 15:

$\exists$ 2: C2=D (C2-0, K0)

=D (E (E (D (C1, K1), K2), K0)

=E (E (D (C1, K1), K2),

further, the re-decrypted data C2 is decrypted using the changeable key K2 at a decryption unit 21 of the changeable key encryption/decryption unit 19:

$\exists$: M=D (C2, K2)

=D (E (D (C1, K1), K2)

and the decrypted data M is outputted to the display unit 14 or the like.

In this case, in order to ensure security, when the re-encrypted data C2-0 is read from the storage medium 81 via a path shown by a broken line in the figure, it may be designed in a manner that the re-encrypted data C2-0 in the storage medium 81 is erased at that time, and that the data re-encrypted using the changeable key K2 and the internal unchangeable key K0 is stored again.

In a case where the re-encrypted data C2 is stored in a DVD-RAM of a removable medium, or it is transferred outside via a network at the externals 82, the re-encrypted data C2 is double re-encrypted using a third changeable key K3, which is obtained from the key center or generated in the set-top box 12, at a

changeable key encryption unit 80:

$$\forall\ 2\text{-}3:\ C2\text{-}3=E\ (C2,\ K3)$$
$$=E\ (E\ (M,\ K2),\ K3).$$

When the double re-encrypted data C2-3 sent to the externals 82 is utilized, the double re-encrypted data C2-3 is decrypted using the third changeable key K3 stored at a decryption unit 84 of a changeable key encryption/decryption unit 83:

$$\exists\ 2:\ C2=D\ (C2\text{-}3,\ K3)$$
$$=D\ (E\ (M,\ K2),\ K3),\ K3)$$
$$=E\ (M,\ K2),$$

further, the re-encrypted data C2 thus obtained is decrypted using the second changeable key K2 at a decryption unit 85 of the changeable key encryption/decryption unit 83:

$$\exists:\ M=D\ (C2,\ K2)$$
$$=D\ (E\ (M,\ K2),\ K2)$$

and the decrypted data M thus obtained is outputted to a display unit 86 or the like.

These operations can be easily achieved by providing a sub-computer arrangement having a CPU and a system-bus in the set-top box 12.

Referring to Fig. 9, description will be given on an arrangement of a set-top box of a seventh embodiment, which is a variation of the sixth embodiment, and also on a method for protecting digital data carried out in the set-top box.

In the set-top box of this embodiment again, similarly to the sixth embodiment set-top box, no description is given on peripheral circuits not directly related to encryption/description, e.g., an amplifier unit and a compression/decompression unit.

The seventh embodiment set-top box has difference from that of the sixth embodiment that the inserted positions are exchanged between the unchangeable

key encryption/decryption unit 15 for performing encryption/decryption using the unchangeable key K0 and the changeable key encryption/decryption unit 19 for performing encryption/decryption using the second changeable key K2, and that there is further provided a changeable key encryption unit 87 for performing encryption/decryption using the second changeable key K2 for the case where the data is stored in a DVD-RAM of a removable medium or is transferred outside via a network at the externals 82.

The digital data 11, which is supplied by broadcasting means such as digital terrestrial wave broadcasting, digital CATV broadcasting, digital satellite broadcasting, etc., by network means such as Internet, or by a digital storage medium such as a DVD, a CD, etc., is encrypted using a first changeable key K1 in order to prevent illegitimate use:

$$C1=E\ (M, K1)$$

and encrypted digital data C1 is supplied to the set-top box 12.

When the encrypted digital data C1 is supplied to the set-top box 12, the encrypted digital data C1 is decrypted at the decryption unit 13 using the first changeable key K1 obtained from the key center:

$$M=D\ (C1, K1)$$

and the decrypted data M thus obtained is outputted to the display unit 14 or the like.

In a case where the copyrighted and decrypted data M is stored in the storage medium 81 such as a hard disk incorporated into or dedicated to the set-top box 12, the decrypted data M is re-encrypted to re-encrypted data C0 using the unchangeable crypt key K0 at the internal unchangeable key encryption/decryption unit 15:

$$\forall\ 0:\ C0=E\ (M, K0)$$

$$=E\ (D\ (C1,\ K1),\ K0).$$

The re-encrypted data C0 is double re-encrypted at the encryption unit 20 of the changeable key encryption/decryption unit 19 using the second changeable key K2 obtained from the key center or generated in the set-top box 12:

$$\forall\ 0\text{-}2:\ C0\text{-}2=E\ (C0,\ K2)$$
$$=E\ (E\ (M,\ K0),\ K2)$$

and the double re-encrypted data C0-2 is stored in the storage medium 81 or the like.

When the double re-encrypted data C0-2 stored in the storage medium 81 is utilized, the double re-encrypted data C0-2 read from the storage medium 81 is re-decrypted at the decryption unit 21 of the changeable key encryption/ decryption unit 19 using the second changeable key K2:

$$\exists\ 0:\ C0=D\ (C0\text{-}2,\ K2)$$
$$=D\ (E\ (C0,\ K2),\ K2),$$

further, the re-decrypted data C0 is re-decrypted again using the unchangeable key K0 at the decryption unit 17 of the unchangeable key encryption/decryption unit 15:

$$\exists:M=D\ (C0,\ K0)$$
$$=D\ (E\ (M,\ K0),\ K0)$$

and the decrypted data M thus obtained is outputted to the display unit 14 or the like.

In this case, in order to ensure security, when the re-encrypted data C0-2 is read from the storage medium 81 via a route shown by a broken line in the figure, it may be designed in a manner that the re-encrypted data C0-2 in the storage medium 81 is erased at that time, and that the data re-encrypted using the second changeable key K2 and the unchangeable key K0 is stored again.

In a case where the decrypted data M is stored in a DVD-RAM of a removable medium or is transferred outside via a network at the externals 82, the decrypted data M is re-encrypted to re-encrypted data C3 using a third changeable key K3 obtained from the key center or generated in the set-top box 12 at the changeable key encryption unit 80:

$$\forall\, 3\text{: } C3=E\,(M, K3)$$
$$=E\,(D\,(C1, K1), K3).$$

The re-encrypted data C3 is encrypted to double re-encrypted data C3-2 at the changeable key encryption unit 87 using the second changeable key K2 obtained from the key center or generated at the set-top box 12:

$$\forall\, 3\text{-}2\text{: } C3\text{-}2=E\,(C3, K2)$$
$$=E\,(E\,(D\,(C1, K1), K3), K2)$$

and the double re-encrypted data C3-2 is stored in the DVD-RAM or is transferred via a network in the externals 82.

When the double re-encrypted data C3-2 sent to the externals 82 is utilized, the double re-encrypted data C3-2 is decrypted using the third changeable key K3 at the decryption unit 84 of the changeable key encryption/decryption unit 83:

$$\exists\, 3\text{: } C3=D\,(C3\text{-}2, K2)$$
$$=D\,(E\,(C3, K2), K2),$$

further, the double re-encrypted data C2 thus obtained is decrypted using the third changeable key K3 at the decryption unit 85 of the changeable key encryption/decryption unit 83:

$$\exists\text{: } M=D\,(C3, K3)$$
$$=D\,(E\,(M, K3), K3)$$

and the decrypted data M thus obtained is outputted to the display unit 86 or the like.

In the above embodiment, the third changeable key K3 is used at the changeable key encryption unit 80 and the second changeable key K2 is used at the changeable key encryption unit 87, while this may be performed in reverse order.

Also, it may be designed in a manner that the encryption unit 20 of the changeable key encryption/decryption unit 19 serves the function of the changeable key encryption unit 87.

While description has been given on the above in the case where the encryption unit 16 and the decryption unit 17 are contained in the unchangeable key encryption/decryption unit 15 and the encryption unit 20 and the decryption unit 21 are contained in the changeable key encryption/decryption unit 19, it is needless to say that these units 16, 17, 20 and 21 may be separately provided.

These operations can be easily achieved by providing a sub-computer arrangement having a CPU and a system-bus in the set-top box 12.

Description will be given on a variation, which is applied to an embodiment using a personal computer.

This eighth embodiment shown in Fig. 10 is a variation of the fourth embodiment shown in Fig. 5. In the embodiment, detailed description common to the fourth embodiment arrangement is not given here.

The eighth embodiment has a difference from the fourth embodiment in distinguishing between the cases where the decrypted data M is stored in a storage medium 81 such as a hard disk incorporated into or dedicated to the computer, and where it is stored in a removable medium 92 such as a DVD-RAM or is transferred outside via a network 93.

For this purpose, changeable key encryption units 90 and 91 are provided as a hardware 88, in addition to the unchangeable key encryption/decryption unit 89.

In a case where the copyrighted and decrypted data is stored in the hard disk 81 of the storage medium incorporated into or dedicated to the computer, it is double re-encrypted and decrypted using the unchangeable key K0 at the encryption/decryption unit 91 via a disk driver 67. In a case where the data is stored in the DVD-RAM 89 of the removable medium, it is double re-encrypted and decrypted using the third changeable key K3 at the encryption/ decryption unit 90 via the disk driver 67. In a case where the data is transferred outside via the network 93, it is double re-encrypted and decrypted using the third changeable key K3 at the changeable key encryption/decryption unit 91 via a network driver 68.

Similarly to the first embodiment shown in Fig. 2, the digital data supplied by broadcasting means such as digital terrestrial broadcasting, digital CATV broadcasting, digital satellite broadcasting, etc., by network means such as Internet, or by a digital storage medium such as a DVD, a CD, etc. is encrypted using a first changeable key K1 to prevent illegitimate use:

$$C1=E(M, K1)$$

and is supplied. The encrypted digital data C1 thus supplied is decrypted at the operating system service 52 using the first changeable key K1 provided from the key center via the same route as or a route different from that of the encrypted digital data C1:

$$M=D(C1, K1)$$

and the decrypted data M is outputted to the display unit 56 or the like.

In cases where the decrypted data M is stored in the storage medium 81 incorporated into or dedicated to the computer, such as a hard disk, where it is stored in a medium such as the DVD-RAM, and where it is transferred outside via a network, the decrypted data M is re-encrypted at a filter driver 66 using the second changeable key K2 obtained from the key center or generated in the operating system service 52:

$\forall$ 2: C2=E (M, K2)

=E (D (C1, K1), K2).

Further, when the re-encrypted data C2 is stored in a computer-incorporated or -dedicated storage medium 81, the re-encrypted data C2 is double re-encrypted using an unchangeable key K0 at the encryption/decryption unit 89 in the hardware 88:

$\forall$ 2-0:C2-0=E (C2, K0) =E (E (D (C1, K1), K2), K0)

and double re-encrypted data C2-0 is stored in the hard disk 81 or the like.

In a case where the double re-encrypted data C2-0 stored in the storage medium 81 is utilized, the re-encrypted data C2-0 read from the storage medium 81 is re-decrypted using the unchangeable key K0 at the encryption/decryption unit 89 in the hardware 88:

$\exists$ 2: C2=E (C2-0, K0) =D (E (E (D (C1, K1), K2), K0),

further, the re-decrypted data C2 is decrypted using the second changeable key K2 at the filter driver 66 having encryption/ decryption function:

$\exists$: M=D (C2, K2) =D (E (D (C1, K1), K2),

and the decrypted data M is outputted by the operating system of the computer to the display unit 56 or the like to be utilized.

When the re-encrypted data C2 is stored in a DVD-RAM of the removable medium, the re-encrypted data C2 is double re-encrypted using the second changeable key K2 at the changeable key encryption/decryption unit 90 of the hardware:

$\forall$ 2-3: C2-3=E (C2, K3) =E (E (D (C1, K1), K2), K3)

and double re-encrypted data C2-3 is stored in the removable medium, the DVD-RAM.

In a case where the double re-encrypted data C2-3 stored in the removable medium 92 is utilized, the re-encrypted data C2-3 read from the removable medium 92 is re-decrypted using the third changeable key K3 obtained from the key center or generated in the operating system service 52 at the encryption/decryption unit 90 in the hardware:

$\exists$ 2: C2=E (C2-3, K3 =D (E (E (D (C1, K1), K2), K3),

further, the re-decrypted data C2 is decrypted using the second changeable key K2 at the filter driver 66 having encryption/ decryption function:

$\exists$: M=D (C2, K2) =D (E (D (C1, K1), k2)

and the decrypted data M is outputted by the operating system of the computer to the display unit 56 or the like to be utilized.

When the re-encrypted data C2 is transferred outside via the network 93, the re-encrypted data C2 is double re-encrypted using the second changeable key K2 at the encryption/decryption unit 91:

$\forall$ 2-3: C2-3=E (C2, K3) =E (E (D (C1, K1), K2), K3)

and double re-encrypted data C2-3 is transferred outside via the network 93.

In a case where the double re-encrypted data C2-3 transferred from the outside via the network 88 is utilized, the encrypted data C2-3 is re-decrypted using the third changeable key K3 at the encryption/decryption unit 91:

$\exists$ 2: C2=E (C2-3, K3) =D (E (E (D (C1, K1), K2) K3),

further, the re-decrypted data C2 is decrypted using the second changeable key K2 at the filter driver 66 having encryption/ decryption function:

$\exists$:M=D (C2, K2) =D (E (D (C1, K1), K2)

and the decrypted data M is outputted by the operating system of the computer to the display unit 56 or the like to be utilized.

In the above embodiment, in order to facilitate the explanation, it has been

described that the encryption/decryption units 90 and 91 are separate, while it is needless to say that these units may be a single unit.

The encryption/decryption as described above is managed by a real-time OS (RTOS) as already explained, with priority to the other tasks at HAL 55 in the operating system 51.

These operations can be easily achieved by designing the hardware 88 as the sub-computer arrangement having a CPU and a system-bus.

Fig. 11 shows a concrete arrangement of the encryption/ decryption using I/O management micro-kernel 64 having the filter driver 66 which serves the changeable key encryption/decryption processing of the eighth embodiment.

In the I/O management micro-kernel 64, a file system driver 69, an intermediate driver 70, and device drivers, i.e., a disk driver 67 and a network driver 68, are arranged from upper hierarchy to lower hierarchy. When necessary, a filter driver 66A or a filter driver 66B for performing changeable key encryption/decryption is inserted above the file system driver 69 or between the intermediate driver 70 and the device driver.

Because these filter drivers 66A and 66B can perform re-encryption/re-decryption, it is designed to have the filter driver 66A or 66B carry out the re-encryption/re-decryption processing and the management of crypt keys in this embodiment.

In cases where the copyrighted and decrypted data M is stored in a storage medium such as a hard disk, incorporated therein or dedicated thereto, where it is stored in a removable medium such as a DVD-RAM or where it is transferred outside via a network, the decrypted data M is re-encrypted at the filter driver 66A or 66B using the second changeable key K2 obtained from the key center or

generated in the I/O management micro-kernel 64:

$\forall$ 2: C2=E (M, K2) =E (D (C1, K1), K2).

Further, in a case where the re-encrypted data C2 is stored in a computer-incorporated or -dedicated storage medium 81, the re-encrypted data C2 is double re-encrypted using the unchangeable key K0 at the encryption/decryption unit 89 in the hardware 88:

$\forall$ 2-0: C2-0=E (C2, K0) =E (E (D (C1, K1), K2), K0)

and double re-encrypted data C2-0 is stored in the hard disk 81 or the like.

When the double re-encrypted data C2-0 stored in the storage medium 81 is utilized, the re-encrypted data C2-0 read from the storage medium 81 is re-decrypted using the unchangeable key K0 at the encryption/decrypted unit 89 in the hardware 88:

$\exists$ 2: C2=E (C2-0, K0) =D (E (E (D (C1, K1), K2), K0),

further, the re-decrypted data C2 is decrypted using the second changeable key K2 at the filter driver 66 having encryption/decryption function:

$\exists$: M=D (C2, K2) =D (E (D (C1, K1), K2)

and the decrypted data M is outputted by the operating system of the computer to the display unit 56 or the like to be utilized.

Also, in a case where the re-encrypted data C2 is stored in the removable medium such as a DVD-RAM, the re-encrypted data C2 is double re-encrypted using the third changeable key k3 obtained from the key center or generated in the I/O management micro-kernel 64, at the encryption/decryption unit 90 in the hardware 88:

$\forall$ 2-3: C2-3=E (C2, K3) =E (E (D (C1, K1), K2), K3)

and double re-encrypted data C2-3 is stored in a removable medium such as the DVD-RAM.

When the double re-encrypted data C2-3 stored in the removable medium 92 is utilized, the re-encrypted data C2-3 read from the removable medium 92 is re-decrypted using the third changeable key K3 at the encryption/decryption unit 90 in the hardware 88:

$\exists$ 2: C2=E (C2-3, K3) =D (E (E (D (C1, K1), K2), K3),

further, the re-decrypted data C2 is decrypted using the second changeable key K2 at the filter driver 66 having encryption/decryption function:

$\exists$: M=D (C2, K2) =D (E (D (C1, K1), K2)

and the decrypted data M is outputted by the operating system of the computer to the display unit 56 or the like to be utilized.

Also, in a case where the re-encrypted data C2 is transferred outside via the network 93, the re-encrypted data C2 is double re-encrypted using the second changeable key K2 at the encryption/decryption unit 91:

$\forall$ 2-3: C2-3=E (C2, K3) =E (E (D (C1, K1), K2), K3)

and double re-encrypted data C2-3 is transferred outside via the network 93.

When the double re-encrypted data C2-3 transferred from the outside via the network 93 is utilized, the re-encrypted data C2-3 is re-decrypted using the third changeable key K3 at the encryption/decryption unit 91:

$\exists$ 2: C2=E (C2-3, K3) =D (E (E (D (C1, K1), K2), K3),

further, the re-decrypted data C2 is decrypted using the second changeable key K2 at the filter driver 66 having encryption/decryption function:

$\exists$: M=D (C2, K2) =D (E (D (C1, K1), K2)

and the decrypted data M is outputted by the operating system of the computer to the display unit 56 or the like to be utilized.

It is generally practiced that the specification of the device driver is changed

to fit for the computer using the operating system or according to the corresponding device modified.

By providing the device driver with the function for the re-encryption/re-decryption processing and the management of a key, it allows to easily incorporate the function into the kernel of the operation system. Also, by re-encrypting the data using the second changeable key K2 before it is re-encrypted using the unchangeable key K0, it is very difficult to cryptanalyze the encrypted data, even if the unchangeable key is known to others, by finding out the second changeable key K2 because the data is also encrypted using the second changeable key K2.

Further, because the second changeable key K2 is used first and then, is used after the unchangeable key K0 is used, high security of the key is ensured. Because the second changeable key K2 is used first, it also strongly governs the encrypted data.

When the second changeable key K2 is repeatedly used, there is a possibility if it may be known to others. In such a case, it is preferably designed in such a manner that the second changeable key K2 used for encryption is abandoned and it is again obtained from the key center or generated, when necessary for decryption, as described in Japanese Patent Laid-Open Publication 185448/1996 (EP0704885A2, USSN 08/536,749).

In order to perform re-encryption/re-decryption of digital data as above, it is necessary to add, to the digital data, information to identify that storage or transfer of the digital data is restricted. In a case where the digital data is stored or transferred without being edited, illegitimate use of the digital data can be prevented by the method and the apparatus for re-encryption/re-decryption as described above.

However, when the digital data is edited, there is a possibility that the information to identify the restriction of storage or transfer may be lost.

In such the case, it may d be designed in a manner that all of the data are re-encrypted/re-decrypted using a key specific to the device (a master key).

In so doing, even the digital data which has been edited, for example, by the "cut & paste" method, can be prevented from illegitimate use by re-encryption/re-decryption.

Also, it may be designed in a manner that the digital data without the information to identify the restriction of storage or transfer only is re-encrypted/re-decrypted by using the master key, and that the digital data provided with the information to identify the restriction of storage or transfer is re-encrypted/re-decrypted using the method and the apparatus as explained in the above embodiments.

In a case where the copyrighted and encrypted digital data is utilized in a specific device such as a set-top box, illegitimate storing, copying or transferring can be relatively easily prevented. Also, in a case where the copyrighted and encrypted digital data is utilized on a computer, the management of storing, copying or transferring the decrypted digital data can be executed by using the decryption/re-encryption apparatus described in Japanese Patent Laid-Open Publication 287014/1996 (USP5,867,579; EP0715241A2) or by using the decryption/re-encryption apparatus described in USP5,805,706.

However, the digital data decrypted for the purpose of displaying or printing is present on the bus of the computer, and it is possible to store, copy or transfer the decrypted digital data via a device connected to the bus. In the following,

description will be given on a copyright management apparatus, which solves this problem.

Fig. 12 shows a structural example of a copyright management apparatus, in which a first changeable key and a second changeable key are used.

Also, this copyright management apparatus can be realized configured in a sub-board, a PCMCIA card, an IC card or an IC package for the purpose of security.

In Fig. 12, reference numeral 101 represents a CPU. A ROM 103, a RAM 104, a hard disk drive 105, a flexible disk drive 105, a CD-ROM drive 107, a modem 108, etc. are connected to a system-bus 102 connected to the CPU 101.

Reference numeral 109 represents a copyright management apparatus, which comprises a decryption/encryption unit 110, a video interface 113, an audio interface 114, and a printer interface 115.

A display unit 116, a speaker 117 and a printer 118 are connected to the video interface 113, the audio interface 114, and the printer interface 115 respectively on the outer side of the computer.

The decryption/encryption unit 110 comprises a decryption unit 111 and an encryption unit 112.

The decryption unit 111 and the encryption unit 112 of the decryption/encryption unit 110 are connected to the system-bus 102 of the computer. The video interface 113, the audio interface 114, and the printer interface 115 are connected to the decryption unit 111.

This arrangement can be easily achieved by designing the copyright management apparatus 109 as a sub-computer arrangement having a CPU and a system-bus.

In cases where the decrypted digital data M is stored in the hard disk drive 105, where it is copied at the flexible disk drive 105 or where it is transferred via the modem 108, the decrypted digital data is re-encrypted using the second changeable key K2 at the re-encryption unit 115:

$$\forall 2: C2=E(M, K2)$$
$$=E(D(C1, K1), K2),$$

the re-encrypted digital data C2 is supplied to the system-bus 102, and is stored in the hard disk drive 105, copied in the flexible disk drive 105 or transferred via the modem 108.

The encrypted digital data C1 encrypted using the first changeable key K1 is supplied to the decryption unit 111 from the system-bus 102, and is decrypted using the first changeable key K1:

$$M=D(C1, K1).$$

In a case where the decrypted digital data M is outputted to the display unit 116 or the speaker 117, it is turned to analog at the video interface 113 and the audio interface 114 in the copyright management apparatus 109 and is outputted in a predetermined signal form.

When the decrypted digital data M is outputted to the printer 118, print data is outputted via the printer interface 115.

When this copyright management apparatus 109 is used, the decrypted digital data other than the data outputted to the printer is not present outside the copyright management apparatus 109. Because the data outputted to the printer is still data, digital data of a moving picture or of audio data is not present outside the copyright management apparatus 109.

In the computer, non-encrypted digital data is also present in addition to the decrypted digital data.

In order to process the non-encrypted digital data and the decrypted data by distinguishing between them, it is necessary to provide a video interface, an audio interface and a printer interface, and this would make the system more complicated and costly. To avoid such situation, it may be designed in a manner that non-encrypted digital data is processed at the video interface 113 and the audio interface 114 in the copyright management system 109.

Fig. 13 shows another arrangement example of a copyright management apparatus, in which an unchangeable key is used in addition to the first and the second changeable keys.

This copyright management apparatus can be realized configured in a sub-board, a PCMCIA card, an IC card, or an IC package for security purpose.

In Fig. 13, reference numeral 101 represents a CPU. A ROM 103, a RAM 104, a hard disk drive 105, a flexible disk drive 105, a CD-ROM drive 107, a modem 108, etc. are connected to a system-bus 102 connected to the CPU 101.

Reference numeral 120 represents a copyright management apparatus. The copyright management apparatus 120 has, in addition to the decryption/encryption unit 110, an unchangeable key encryption unit 121, a crypt video interface 122, a crypt audio interface 123, and a crypt printer interface 124.

The decryption/encryption unit 110 has a decryption unit 111 and an encryption unit 112.

Also, an encrypted digital video display unit 125, an encrypted digital audio player 126, and an encrypted digital data printer 127, which arranged outside of the computer, are connected to the crypt video interface 122, the crypt audio interface 123, and the crypt printer interface 124.

The decryption unit 111 and the encryption unit 112 of the

decryption/encryption unit 110 are both connected to the computer system-bus 102. The unchangeable key encryption unit 121 is further connected to the decryption unit 111.

The crypt video interface 122, the crypt audio interface 123, and the crypt printer interface 124 are connected to the unchangeable key encryption unit 121.

The encrypted data display unit 125 is connected to the crypt video interface 122, the encrypted audio data player 126 is connected to the crypt audio interface 123 and the encrypted data printer 127 is connected to the crypt printer interface 124.

The above arrangement can be easily realized by designing the copyright management apparatus 120 as a sub-computer arrangement having a CPU and a system-bus.

The encrypted data display unit 125 has an unchangeable key decryption unit 128 connected to the crypt video interface 122, a D/A converter 131 connected to the unchangeable key decryption unit 128, and a display unit 116 connected to the D/A converter 131.

The encrypted audio data player 126 has an unchangeable key decryption unit 129 connected to the crypt audio interface 123, a D/A converter 132 connected to the unchangeable key decryption unit 129, and a speaker 117 connected to the D/A converter 132.

The encrypted data printer 127 has an unchangeable key decryption unit 130 connected to the crypt printer interface 124 and a printer 118 connected to the unchangeable key decryption unit 130.

It is needless to say that the encrypted data display unit 125, the encrypted audio data player 126 and the encrypted data printer 127 have other components such as an amplifier.

The encrypted digital data C1 encrypted using the first changeable key K1 is supplied to the decryption unit 111 from the system-bus 102, and it is decrypted using the first changeable key K1:

$$M=D(C1, K1).$$

When the decrypted digital data M is stored at the hard disk drive 105 or is copied at the flexible disk drive 105 or is transferred via the modem 108, it is re-encrypted using the second changeable key K2 at the re-encryption unit 115:

$$\forall\ 2: C2=E(M, K2)$$
$$=E(D(C1, K1), K2),$$

the re-encrypted digital data C2 is supplied to the system-bus 102, and it is stored at the hard disk drive 105, copied at the flexible disk drive 105, or transferred via the modem 108.

When the decrypted digital data M is outputted to the encrypted data display unit 125, the encrypted audio data player 126 or the encrypted data printer 127, it is re-encrypted using the unchangeable key K0 at the unchangeable key encryption unit 121 in the copyright management apparatus 120:

$$\forall\ 0: C0=E(M, K0)$$
$$=E(D(C1, K1), K0).$$

The re-encrypted digital data C0 is arranged to be provided to the encrypted data display unit 125, the encrypted audio data player 126 and the encrypted data printer 127 at the crypt video interface 122, the crypt audio interface 123 and the printer interface 124 respectively, and an encrypted display signal Cd0, an encrypted audio signal Ca0 and an encrypted print signal Cp0 are respectively outputted.

When the encrypted display signal Cd0 is inputted to the encrypted data display unit 125 from the crypt video interface 122, it is decrypted using the

unchangeable key K0 at the unchangeable key decryption unit 128:

Md=D (Cd0, K0),

the decrypted display signal Md is converted to a displayable analog signal at the D/A converter 131 and it is displayed on the display unit 116.

If the display unit 116 is a digital display unit, which can display the digital data as it is, the D/A converter 131 is unnecessary.

When the encrypted audio signal Ca0 is inputted to the encrypted audio data player 126 from the crypt audio interface 123, it is decrypted using the unchangeable key K0 at the unchangeable key decryption unit 129:

Ma=D (Ca0, K0),

the decrypted audio signal MA is converted to a playable analog signal at the D/A converter 132, and it is played at the speaker 116.

The encrypted print signal Cp0 inputted to the encrypted data printer 127 from the crypt printer interface 124 is decrypted using the unchangeable key K0 at the unchangeable key decryption unit 130:

Mp=D (Cp0, K0)

and the decrypted print signal Mp is printed by the printer 118.

When this copyright management apparatus 120 is used, no decrypted data is present outside the copyright management apparatus 120.

As aforementioned, non-encrypted digital data is also present in addition to the decrypted digital data in the computer.

In order to process the non-encrypted digital data and the decrypted digital data by distinguishing between them, it is necessary to provide a video interface, an audio interface and a printer interface, and this would make the system more complicated and costly. To avoid such situation, it may be designed in a manner

that the non-encrypted digital data is processed at the unchangeable key re-encryption unit 121 of the copyright management apparatus 120.

Fig. 14 shows another arrangement example of the copyright management apparatus, in which an unchangeable key encryption unit is provided to follow the video interface, the audio interface and the printer interface.

The copyright management apparatus can be realized configured in a sub-board, a PCMCIA card, an IC card or an IC package for security purpose.

In Fig. 14, reference numeral 101 represents a CPU. A ROM 103, a RAM 104, a hard disk drive 105, a flexible disk drive 105, a CD-ROM drive 107, a modem 108, etc. are connected to a system-bus 102 connected to the CPU 101.

Reference numeral 140 represents a copyright management apparatus, which comprises a decryption/re-encryption unit 110, a video interface 113, an audio interface 114, a printer interface 141, and an unchangeable key encryption unit 134.

The decryption/re-encryption unit 110 has a decryption unit 111 and an re-encryption unit 112.

The unchangeable key encryption unit 134 has an unchangeable key encryption unit for video 142, an unchangeable key encryption unit for audio 136, and an unchangeable key encryption unit for print 137. The unchangeable key encryption units for video, audio and print may be arranged in a single unit if it is available for sufficient encryption capacity.

The decryption unit 111 and the re-encryption unit 112 of the decryption/encryption unit 110 are connected to the system-bus 102 of the computer. Further, the video interface 113, the audio interface 114 and the printer interface 115 are connected to the decryption unit 111, and the unchangeable key encryption unit for video 135, the unchangeable key encryption unit for audio 136

and the unchangeable key encryption unit for print 137 are connected to these interfaces.

An encrypted digital video display unit 125, an encrypted digital audio player 126 and an encrypted digital data printer 127 arranged outside the computer are connected respectively to the unchangeable key encryption unit for video 135, the unchangeable key encryption unit for audio 163 and the unchangeable key encryption unit for print 137.

The above arrangement can be easily realized by designing the copyright management apparatus 120 as a sub-computer arrangement having a CPU and a system-bus.

The encrypted data display unit 125 has an unchangeable key decryption unit 128 connected to the unchangeable key encryption unit for video 135, a D/A converter 131 connected to the unchangeable key decryption unit 128, and a display unit 116 connected to the D/A converter 131.

The encrypted audio data player 126 has an unchangeable key decryption unit 129 connected to the unchangeable key encryption unit for audio 136, a D/A converter 132 connected to the unchangeable key decryption unit 129, and a speaker 117 connected to the D/A converter 132.

The encrypted data printer 127 has an unchangeable key decryption unit 130 connected to the unchangeable key encryption unit for print 137 and a printer 118 connected to the unchangeable key decryption unit 130.

It is needless to say that the encrypted data display unit 125, the encrypted audio data player 126 and the encrypted data printer 127 have other components such as an amplifier.

The encrypted digital data C1 encrypted using the first changeable key K1 is supplied to the decryption unit 111 from the system-bus 102 and it is decrypted

using the first changeable key K1:

$$M=D(C1, K1).$$

When the decrypted digital data M is stored at the hard disk drive 105 or copied at the flexible disk drive 105 or transferred via the modem 108, it is re-encrypted using the second changeable key K2 at the re-encryption unit 115:

$$\forall\ 2: C2=E(M, K2)$$
$$=E(D(C1, K1), K2),$$

the re-encrypted digital data C2 is supplied to the system-bus 102, and it is then stored at the hard disk drive 105, copied at the flexible disk drive 105 or transferred via the modem 108.

When the decrypted digital data M is outputted to the encrypted data display unit 125, the encrypted audio data player 126 or the encrypted data printer 127, the decrypted digital data M is arranged to digital data Md, Ma and Mp to be provided to the display unit 116, the speaker 117 and the printer 118 respectively at the video interface 131, the audio interface 132 and the printer interface 133 in the copyright management apparatus 120. Then, these digital data are encrypted using the unchangeable key K0 at the unchangeable key encryption unit for video 135, the unchangeable key encryption unit for audio 136 and the unchangeable key encryption unit for print 137:

$$Cd0=E(Md, K0)$$
$$Ca0=E(Ma, K0)$$
$$Cp0=E(Mp, K0)$$

and the encrypted display signal Cd0, the encrypted audio signal Ca0 and the encrypted print signal Cp0 are outputted.

The encrypted display signal Cd0 is inputted to the encrypted data display unit 125 from the unchangeable key encryption unit for video 135, and it is

decrypted using the unchangeable key K0 at the unchangeable key decryption unit 128:

Md=D (Cd0, K0).

The decrypted display signal Md is converted to a displayable analog signal at the D/A converter 131, and is displayed on the display unit 116.

If the display unit 116 is a digital display unit, which can display the digital data as it is, the D/A converter 131 is unnecessary.

The encrypted audio signal Ca0 is inputted to the encrypted audio data player 126 from the unchangeable key encryption unit 136, and it is decrypted using the unchangeable key K0 at the unchangeable key decryption unit 129:

Ma=D (Ca0, K0).

The decrypted audio signal Ma is converted to a playable analog signal at the D/A converter 132, and is played at the speaker 116.

The encrypted print signal Cp0 is inputted to the encrypted data printer 127 from the unchangeable key encryption unit 137, and it is decrypted using the unchangeable key K0:

Mp=D (Cp0, K0).

The decrypted audio signal Mp is printed by the printer 118.

When this copyright management apparatus 140 is used, no decrypted data is present outside the copyright management apparatus 120.

As aforementioned, non-encrypted digital data is also present in addition to the decrypted digital data in the computer.

In order to process the non-encrypted digital data and the decryption data by distinguishing between them, it is necessary to provide a video interface, an audio interface and a printer interface, and this would make the system more complicated

and costly. To avoid such situation, it may be designed in a manner that the non-encrypted digital data is processed at the video interface 131, the audio interface 132 and the printer interface 133 of the copyright management apparatus 140.

A secret-key cryptosystem is often used as a cryptosystem for encrypting digital data. The most popular DES (Data Encryption Standard) in the secret-key cryptosystems carries out encryption/decryption per 64-bit block unit of data. It is a typical block cipher method in the secret-key cryptosystem and has been widely adopted. Using this encryption/decryption per block processing allows to realize a more high speed encryption/decryption processing.

In doing so, a plurality of encryption units and decryption units are provided in the encryption/decryption unit. It allows these plurality of encryption units and decryption units to be, in order, allocated the encryption/decryption processings of data blocks to be carried out. And then, encryption/decryption processing results, thus obtained, are synthesized.

Further, it brings a supplemental effect that it is possible to use a respective crypt key for each data block and also to adopt a respective cryptosystem for each data block. Then, more highly securing the digital data is possible.

I claim:

1. A method for protecting decrypted digital data, to which encrypted digital data is decrypted, from illegitimate use, said method comprising the steps of:

encrypting said decrypted digital data by using a changeable key to digital data re-encrypted by the changeable key;

encrypting said digital data re-encrypted by the changeable key by using an unchangeable key in a device to digital data double re-encrypted by changeable-unchangeable keys to be stored, copied or transferred;

decrypting said copied, stored or transferred digital data double re-encrypted by changeable-unchangeable keys, by using said unchangeable key to digital data re-encrypted by the changeable key; and

decrypting said digital data re-encrypted by the changeable key, by using said changeable key to said decrypted digital data.

2. A method for protecting decrypted digital data, to which encrypted digital data is decrypted, from illegitimate use, comprising the steps of:

encrypting said decrypted digital data by using an unchangeable key in a device to digital data re-encrypted by the unchangeable key;

encrypting said digital data re-encrypted by the unchangeable key by using a changeable key to digital data double re-encrypted by changeable-unchangeable keys to be stored, copied or transferred;

decrypting said copied, stored or transferred digital data double re-encrypted by changeable-unchangeable keys, by using said changeable key to digital data re-encrypted by the changeable key; and

decrypting said digital data decrypted by the changeable key key, by using said unchangeable key to said decrypted digital data.

3. The method according to claim 1 or 2, wherein said steps of encrypting and decrypting by using said changeable key are carried out by a software.

4. The method according to claim 1 or 2, wherein said steps of encrypting and

* C L M S *

decrypting by using said changeable key are carried out by a hardware.

5. The method according to claim 1 or 2, wherein said changeable key is supplied from the outside of a device.

6. The method according to claim 1 or 2, wherein said changeable key is generated in a device.

7. The method according to claim 1 or 2, wherein said steps of encrypting and decrypting by using said unchangeable key are carried out by a software.

8. The method according to claim 1 or 2, wherein said steps of encrypting and decrypting by using said unchangeable key are carried out by a hardware.

9. The method according to claim 1 or 2, wherein said unchangeable key is already placed in said device.

10. The method according to claim 1 or 2, wherein said unchangeable key is generated in said device.

11. The method according to claim 1 or 2, wherein said unchangeable key is supplied from the outside of said device.

12. The method according to claim 9, 10 or 11, wherein said unchangeable key is specific to said device.

13. The method according to claim 9, 10 or 11, wherein said unchangeable key is not specific to said device.

14. An apparatus for protecting decrypted digital data, to which encrypted digital data is decrypted, from illegitimate use, said apparatus comprising:

a changeable key re-encryption unit for encrypting said decrypted digital data by using a changeable key to digital data re-encrypted;

an unchangeable key encryption unit for encrypting said digital data re-encrypted by the changeable key by using an unchangeable key in a device to digital data double re-encrypted by changeable-unchangeable keys to be stored, copied or transferred;

an unchangeable key decryption unit for decrypting said copied, stored or transferred digital data double re-encrypted by changeable-unchangeable keys, by



using said unchangeable key to digital data re-encrypted by the unchangeable key; and

a changeable key decryption unit for decrypting said digital data re-encrypted by the unchangeable key, by using said changeable key to said decrypted digital data.

15. An apparatus for protecting decrypted digital data, to which encrypted digital data is decrypted, from illegitimate use, said apparatus comprising:

an unchangeable key encryption unit for encrypting said decrypted digital data by using an unchangeable key in a device to digital data re-encrypted by the unchangeable key;

a changeable key encryption unit for encrypting said digital data re-encrypted by the unchangeable key by using a changeable key to digital data double re-encrypted by changeable-unchangeable keys to be stored, copied or transferred;

a changeable key decryption unit for decrypting said copied, stored or transferred digital data double re-encrypted by changeable-unchangeable keys, by using said changeable key to digital data re-encrypted by the unchangeable key; and

an unchangeable key decryption unit for decrypting said digital data re-encrypted by the unchangeable key, by using said unchangeable key to said decrypted digital data.

16. The apparatus according to claim 14 or 15, in which encrypting and decrypting by using said changeable key are carried out by a software.

17. The apparatus according to claim 14 or 15, in which encrypting and decrypting by using said changeable key are carried out by a hardware.

18. The apparatus according to claim 14 or 15, wherein said changeable key is supplied from the outside of a device.

19. The apparatus according to claim 14 or 15, wherein said changeable key is generated in a device.

20. The apparatus according to claim 14 or 15, in which encrypting and decrypting by using said unchangeable key are carried out by a software.

* C L M S *

21. The apparatus according to claim 14 or 15, in which encrypting and decrypting by using said unchangeable key are carried out by a hardware.

22. The apparatus according to claim 14 or 15, wherein said unchangeable key is already placed in said device.

23. The apparatus according to claim 14 or 15, wherein said unchangeable key is generated in said device.

24. The apparatus according to claim 14 or 15, wherein said unchangeable key is supplied from the outside of said device.

25. The apparatus according to claim 14 or 15, wherein said unchangeable key is specific to said device.

26. The apparatus according to claim 14 or 15, wherein said unchangeable key is not specific to said device.

27. A method for protecting decrypted digital data, to which digital data encrypted by a first changeable key is decrypted, from illegitimate use, said method comprising the steps of:

encrypting said decrypted digital data by using a second changeable key to digital data re-encrypted by the second changeable key;

encrypting said digital data re-encrypted by the second changeable key by using an unchangeable key in a device to digital data double re-encrypted by unchangeable-second-changeable keys to be stored;

decrypting said stored digital data double re-encrypted by unchangeable-second-changeable keys by using said unchangeable key to said digital data re-encrypted by the second changeable key;

encrypting said digital data re-encrypted by the second changeable key by using a third changeable key to digital data double re-encrypted by third-changeable-second-changeable keys to be copied or transferred;

decrypting said copied or transferred digital data double re-encrypted by third-changeable-second-changeable keys by using said third changeable key to digital data re-encrypted by the second changeable key; and

* C L M S *

decrypting said digital data re-encrypted by the second changeable key by using said second changeable key to decrypted digital data.

28. A method for protecting decrypted digital data, to which digital data encrypted by a first changeable key is decrypted, from illegitimate use, said method comprising the steps of:

encrypting said decrypted digital data by using a second changeable key to digital data re-encrypted by the second changeable key;

encrypting said digital data re-encrypted by the second changeable key by using an unchangeable key in a device to digital data double re-encrypted by unchangeable-second-changeable keys to be stored;

decrypting said stored digital data double re-encrypted by unchangeable-second-changeable keys by using said unchangeable key to said digital data re-encrypted by the second changeable key;

encrypting said digital data re-encrypted by the second changeable key by using a third changeable key to digital data double re-encrypted by third-changeable-second-changeable keys to be copied or transferred;

decrypting said copied or transferred digital data double re-encrypted by third-changeable-second-changeable keys by using said third changeable key to digital data re-encrypted by the second changeable key; and

decrypting said digital data re-encrypted by the second changeable key by using said second changeable key to decrypted digital data.

29. A method for protecting decrypted digital data, to which digital data encrypted by a first changeable key is decrypted, from illegitimate use, said method comprising the steps of:

encrypting said decrypted digital data by using an unchangeable key in a device to digital data re-encrypted by the unchangeable key, and encrypting said digital data re-encrypted by the unchangeable key by using a second changeable key to digital data double re-encrypted by second-changeable-unchangeable keys to be stored;



decrypting said stored digital data double re-encrypted by second-changeable-unchangeable keys by using said second changeable key to digital data re-encrypted by the unchangeable key;

decrypting said digital data re-encrypted by the unchangeable key by using said unchangeable key to decrypted digital data;

encrypting said re-encrypted digital data by using a third changeable key to digital data re-encrypted by the third changeable key, and encrypting said digital data re-encrypted by the third changeable key to digital data double re-encrypted by second-changeable-third-changeable keys to be copied or transferred;

decrypting said copied or transferred digital data double re-encrypted by second-changeable-third-changeable keys by using said second changeable key to digital data re-encrypted by the third changeable key; and

decrypting said digital data re-encrypted by the third changeable key by using said third changeable key to decrypted digital data.

30. A method for protecting decrypted digital data, to which digital data encrypted by a first changeable key is decrypted, from illegitimate use, said method comprising the steps of:

encrypting said decrypted digital data by using an unchangeable key in a device to digital data re-encrypted by the unchangeable key, and encrypting said digital data re-encrypted by the unchangeable key by using a second changeable key to digital data double re-encrypted by second-changeable-unchangeable keys to be stored;

decrypting said stored digital data double re-encrypted by second-changeable-unchangeable keys by using said second changeable key to digital data re-encrypted by the unchangeable key;

decrypting said digital data re-encrypted by the unchangeable key by using said unchangeable key to decrypted digital data;

encrypting said re-encrypted digital data by using a third changeable key to digital data re-encrypted by the third changeable key, and encrypting said digital

* C L M S *

data re-encrypted by the third changeable key to digital data double re-encrypted by second-changeable-third-changeable keys to be copied or transferred;

decrypting said copied or transferred digital data double re-encrypted by second-changeable-third-changeable keys by using said second changeable key to digital data re-encrypted by the third changeable key; and

decrypting said digital data re-encrypted by the third changeable key by using said third changeable key to decrypted digital data.

31. The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting by using said second changeable key are carried out by a software.

32. The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting by using said second changeable key are carried out by a hardware.

33. The method according to claim 27, 28, 29 or 30, wherein said second changeable key is supplied from the outside of a device.

34. The method according to claim 27, 28, 29 or 30, wherein said second changeable key is generated in a device.

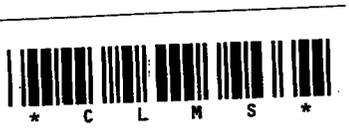
35. The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting by using said third changeable key are carried out by a software.

36. The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting by using said third changeable key are carried out by a hardware.

37. The method according to claim 27, 28, 29 or 30, wherein said third changeable key is supplied from the outside of a device.

38. The method according to claim 27, 28, 29 or 30, wherein said third changeable key is generated in a device.

39. The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting by using said unchangeable key are carried out by a



software.

40. The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting by using said unchangeable key are carried out by a hardware.

41. The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is already placed in said device.

42. The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is generated in said device.

43. The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is supplied from the outside of said device.

44. The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is specific to a device.

45. The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is not specific to a device.

46. An apparatus for protecting decrypted digital data, to which digital data encrypted by a first changeable key is decrypted, from illegitimate use, said apparatus comprising:

a second changeable key encryption unit for encrypting said decrypted digital data by using a second changeable key to digital data re-encrypted by the second changeable key;

an unchangeable key encryption unit for encrypting said digital data re-encrypted by the second changeable key by using an unchangeable key in a device to digital data double re-encrypted by unchangeable-second-changeable keys to be stored;

an unchangeable key decryption unit for decrypting said stored digital data double re-encrypted by unchangeable-second-changeable keys by using said unchangeable key to said digital data re-encrypted by the second changeable key;

a third changeable key encryption unit for encrypting said digital data re-encrypted by the second changeable key by using a third changeable key to

* C L M S *

digital data double re-encrypted by third-changeable-second-changeable keys to be copied or transferred;

a third changeable key decryption unit for decrypting said copied or transferred digital data double re-encrypted by third-changeable-second-changeable keys by using said third changeable key to digital data re-encrypted by the second changeable key; and

a second changeable key decryption unit for decrypting said digital data re-encrypted by the second changeable key by using said second changeable key to decrypted digital data.

47. An apparatus for protecting decrypted digital data, to which digital data encrypted by a first changeable key is decrypted, from illegitimate use, said apparatus comprising:

a second changeable key encryption unit for encrypting said decrypted digital data by using a second changeable key to digital data re-encrypted by the second changeable key;

an unchangeable key encryption unit for encrypting said digital data re-encrypted by the second changeable key by using an unchangeable key in a device to digital data double re-encrypted by unchangeable-second-changeable keys to be stored;

an unchangeable key decryption unit for decrypting said stored digital data double re-encrypted by unchangeable-second-changeable keys by using said unchangeable key to said digital data re-encrypted by the second changeable key;

a third changeable key encryption unit for encrypting said digital data re-encrypted by the second changeable key by using a third changeable key to digital data double re-encrypted by third-changeable-second-changeable keys to be copied or transferred;

a third changeable key decryption unit for decrypting said copied or transferred digital data double re-encrypted by third-changeable-second-changeable keys by using said third changeable key to digital data re-encrypted by the second

changeable key; and

a second changeable key decryption unit for decrypting said digital data re-encrypted by the second changeable key by using said second changeable key to decrypted digital data.

48. An apparatus for protecting decrypted digital data, to which digital data encrypted by a first changeable key is decrypted, from illegitimate use, said apparatus comprising:

an unchangeable key encryption unit for encrypting said decrypted digital data by using an unchangeable key in a device to digital data re-encrypted by the unchangeable key, and a second changeable key encryption unit for encrypting said digital data re-encrypted by the unchangeable key by using a second changeable key to digital data double re-encrypted by second-changeable-unchangeable keys to be stored;

a second changeable key decryption unit for decrypting said stored digital data double re-encrypted by second-changeable-unchangeable keys by using said second changeable key to digital data re-encrypted by the unchangeable key, and an unchangeable key decryption unit for decrypting said digital data re-encrypted by the unchangeable key by using said unchangeable key to decrypted digital data;

a third changeable key encryption unit for encrypting said re-encrypted digital data by using a third changeable key to digital data re-encrypted by the third changeable key, and a second changeable key encryption unit for encrypting said digital data re-encrypted by the third changeable key to digital data double re-encrypted by second-changeable-third-changeable keys to be copied or transferred; and

a second changeable key decryption unit for decrypting said copied or transferred digital data double re-encrypted by second-changeable-third-changeable keys by using said second changeable key to digital data re-encrypted by the third changeable key, and a third changeable key decryption unit for decrypting said digital data re-encrypted by the third changeable key by using said third changeable

key to decrypted digital data.

49. An apparatus for protecting decrypted digital data, to which digital data encrypted by a first changeable key is decrypted, from illegitimate use, said apparatus comprising:

an unchangeable key encryption unit for encrypting said decrypted digital data by using an unchangeable key in a device to digital data re-encrypted by the unchangeable key, and a second changeable key encryption unit for encrypting said digital data re-encrypted by the unchangeable key by using a second changeable key to digital data double re-encrypted by second-changeable-unchangeable keys to be stored;

a second changeable key decryption unit for decrypting said stored digital data double re-encrypted by second-changeable-unchangeable keys by using said second changeable key to digital data re-encrypted by the unchangeable key, and an unchangeable key decryption unit for decrypting said digital data re-encrypted by the unchangeable key by using said unchangeable key to decrypted digital data;

a third changeable key encryption unit for encrypting said re-encrypted digital data by using a third changeable key to digital data re-encrypted by the third changeable key, and a second changeable key encryption unit for encrypting said digital data re-encrypted by the third changeable key to digital data double re-encrypted by second-changeable-third-changeable keys to be copied or transferred; and

a second changeable key decryption unit for decrypting said copied or transferred digital data double re-encrypted by second-changeable-third-changeable keys by using said second changeable key to digital data re-encrypted by the third changeable key, and a third changeable key decryption unit for decrypting said digital data re-encrypted by the third changeable key by using said third changeable key to decrypted digital data.

50. The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting by using said second changeable key are carried out by a



software.

51. The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting by using said second changeable key are carried out by a hardware.

52. The apparatus according to claim 46, 47, 48 or 49, wherein said second changeable key is supplied from the outside of a device.

53. The apparatus according to claim 46, 47, 48 or 49, wherein said second changeable key is generated in a device.

54. The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting by using said third changeable key are carried out by a software.

55. The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting by using said third changeable key are carried out by a hardware.

56. The apparatus according to claim 46, 47, 48 or 49, wherein said third changeable key is supplied from the outside of a device.

57. The apparatus according to claim 46, 47, 48 or 49, wherein said third changeable key is generated in a device.

58. The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting by using said unchangeable key are carried out by a software.

59. The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting by using said unchangeable key are carried out by a hardware.

60. The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is already placed in the device.

61. The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is generated in the device.

62. The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable

key is supplied from the outside of the device.

63. The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is specific to said device.

64. The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is not specific to said device.

65. A method for protecting digital data from illegitimate use, said method comprising the steps of:

determining whether said digital data is subject to be protected or not;

encrypting said digital data determined being subject to be protected by using an unchangeable key in a device to digital data encrypted by the unchangeable key;

storing, copying or transferring said digital data determined being not subject to be protected and said digital data encrypted by the unchangeable key;

decrypting said stored, copied or transferred digital data encrypted by the unchangeable key by using said unchangeable key to decrypted digital data; and

utilizing said stored, copied or transferred digital data and said decrypted digital data.

66. The method according to claim 65, wherein said steps of encrypting and decrypting by using said unchangeable key are carried out by a software.

67. The method according to claim 65, wherein said steps of encrypting and decrypting by using said unchangeable key are carried out by a hardware.

68. The method according to claim 65, in which encrypting and decrypting by using said unchangeable key are controlled by identifying information which is added to said digital data.

69. The method according to claim 68, in which encrypting and decrypting are carried out by presence of said identifying information.

70. The method according to claim 68, in which encrypting and decrypting are carried out by absence of said identifying information.

71. The method according to claim 65, wherein said unchangeable key is already placed in a device.



72. The method according to claim 65, wherein said unchangeable key is generated in the device.

73. The method according to claim 65, wherein said unchangeable key is supplied from the outside of the device.

74. The method according to claim 71, 72 or 73, wherein said unchangeable key is specific to the device.

75. The method according to claim 71, 72 or 73, wherein said unchangeable key is not specific to the device.

76. An apparatus for protecting digital data from illegitimate use, said apparatus comprising:

determining means as to whether said digital data is subject to be protected or not;

means for encrypting said digital data determined being subject to be protected by using an unchangeable key in a device to digital data encrypted by the unchangeable key;

means for storing, copying or transferring said digital data determined being not subject to be protected and said digital data encrypted by the unchangeable key;

means for decrypting said stored, copied or transferred digital data encrypted by the unchangeable key by using said unchangeable key to decrypted digital data; and

means for utilizing said stored, copied or transferred digital data and said decrypted digital data.

77. The apparatus according to claim 76, wherein encrypting and decrypting by using said unchangeable key are carried out by a software.

78. The apparatus according to claim 76, wherein encrypting and decrypting by using said unchangeable key are carried out by a hardware.

79. The apparatus according to claim 76, wherein encrypting and decrypting by using said unchangeable key are controlled by identifying information which is added to said digital data.

80. The apparatus according to claim 76, wherein encrypting and decrypting are carried out by presence of said identifying information.

81. The apparatus according to claim 76, wherein encrypting and decrypting are carried out by absence of said identifying information.

82. The apparatus according to claim 76, wherein said unchangeable key is already placed in a device.

83. The apparatus according to claim 76, wherein said unchangeable key is generated in the device.

84. The apparatus according to claim 76, wherein said unchangeable key is supplied from the outside of the device.

85. The apparatus according to claim 82, 83 or 84, wherein said unchangeable key is specific to the device.

86. The apparatus according to claim 82, 83 or 84, wherein said unchangeable key is not specific to the device.

