Description

The present invention relates to a system for determining the authenticity of software in an information processing apparatus. More specifically, the present invention relates to a system for determining whether software contained in an external memory, for example, ROM cartridge, floppy disk or the like is authorized for use with a main processor unit.

Conventionally, such information processing apparatuses are known wherein an external memory is loaded into a main unit and the main unit executes a predetermined operation following software contained in this external memory. The assignee of the present invention also manufactures and sells the home video game apparatus "NINTENDO Entertainment System" (Trade Mark) which is one example of such an information processing apparatus. In this type of apparatus a ROM cartridge (external memory) is loaded into the main unit, the main unit is connected to a television, and thereby various games can be enjoyed on the screen of the television. A large number of software programs (ROM cartridges) which can be utilized with such information processing apparatus are commercially available. However, such authentic software programs are subject to being imitated and counterfeited.

The present invention is directed towards solving the technical problem of determining whether an external memory which is employed with a main processor unit contains an authentic software program.

The preamble of claim 1 is based on the disclosure of an article by L Letham et al entitled "Software Security is provided by an EPROM that performs an authentication handshake" from Phoenix Conference on Computers and Communications, 1985 Conference Proceedings, Scottsdale, Arizona, 20th - 22nd March 1985, pages 122-126, IEEE, New York, US. The system disclosed in that article uses keyed-access EPROMs as the authenticating devices in the main unit and the cartridge.

The system EPROM and the cartridge EPROM each in turn generate a pseudo random number, encrypt it with a pre-loaded secret key and in turn compare the encrypted number with the same number as encrypted by the other EPROM. The handshake is only completed if the first encrypted numbers match. Until the above described authentication handshake has been completed satisfactorily, the main processor or CPU can only access a limited code area of each EPROM. A control means then releases access to the remainder of the address locations in the EPROM. It will be noted that the CPU must be fully functional throughout the handshake proceeding in order to control the operations on, and the exchange of, data between the EPROMs in the cartridge and main unit. In order for the handshake to be completed successfully, it is necessary that the EPROMS both contain the same stored key. This requires matched pairs of EPROMs to be sold to the consumer before the system can be implemented and requires the keys to be protected from discovery.

A number of other systems have been proposed whereby a CPU interrogates an authenticating device in an external memory in order to determine the authenticity of the external memory. See for example EP-A-0 080 244. Such systems and the system proposed in the Phoenix Conference paper referred to above require operation of the CPU in order to control the authentication operation.

The present invention is characterised by the features set out in the characterising clause of claim 1.

By using processor devices as the authenticating devices, it is no longer necessary for the main processor to be functional during the authentication operation. Therefore, it is possible for the main processor to remain reset until authentication is complete.

Authentication can, in a preferred embodiment, be conducted while the information processing apparatus is operating in order to provide even greater security. Other advantages of the system as provided by the features of the dependent claims will be apparent from the following description of preferred embodiments.

The invention also provides, in claim 12, an external memory unit for connection to a main data processor unit to form an information processing apparatus, said external memory unit comprising a program memory means storing a software program that is to be executed by the main data processor unit, and a microprocessor device having a memory and a CPU which is arranged to execute a predetermined verification program stored in said memory when said memory unit is connected to the main data processor unit and while said main data processor unit is held in a reset state, in order to verify that said software program stored in said program memory means is authorised for use in the main data processor unit.

Some video game machines employing external memory and employing a system in accordance with the invention for determining the authenticity of the software used, will now be described, by way of example only, with reference to the accompanying diagrammatic drawings, in which:

Fig. 1 is a perspective view showing one embodiment of a video game machine;

Fig. 2 is a block diagram showing a circuit configuration of this embodiment;

Fig.3 is a block diagram showing a circuit configuration of a lock device;

Fig. 4 is a timing chart for explaining the operation of the device shown in Fig. 3;

Fig. 5 is a flow chart for explaining an outline of the operation of the machine;

Figs. 6A and 6B together show a flow chart for explaining the operation of the machine in further detail;

Figs. 7A and 7B together show a flow chart similar to Fig. 6 for explaining a modified operation of the machine;

Fig. 8 is a perspective view showing another embodiment of a video game machine;

Fig. 9 is an illustrative view showing one example of a floppy disk used in the machine of Fig. 8; and

Fig. 10 is an illustrative view showing one example of a reading apparatus for use in the machine.

Fig. 1 is a perspective view showing one example of a game machine. The system of the present invention is described herein as it is applied to the game machine. However, it is noted that the present invention is applicable to a variety of types of information processing apparatus such as computers, word processors, banking systems or the like which employ an external memory, for example, a cartridge, floppy disk, card or the like.

A game machine 10 comprises a main unit 12, and user controllers 14a and 14b which are connected to this main unit 12. A cartridge 16 is further loaded into the main unit 12 as an external memory. As described in detail later, the cartridge 16 includes a ROM storing a program written for the game machine. The main unit 12 develops a video signal required for the game in response to signals from the controllers 14a and 14b following a program in the ROM of cartridge 16, and sends this video signal to a television 18. The operator watches the picture on the screen of the television 18, operates the controllers 14a and 14b as required, and thereby executes the game programmed in the ROM cartridge 16.

As shown in Fig. 2, a connector 20 is installed in the game machine main unit 12, and this connector 20 is engaged with a connector 22 of the cartridge 16, and thereby the main unit 12 is connected electrically to the ROM contained in cartridge 16.

A game microprocessor 24, for example, the integrated circuit "Z80A" manufactured by Zilog, is mounted on a printed circuit board (not shown) of the main unit 12, and the above-described controllers 14a and 14b and television 18 are connected to this microprocessor 24 through an interface 26.

A PPU (picture processing unit) 28, a semiconductor device 30 (lock) for determining the authenticity of the external ROM cartridge 16, and a clock oscillator 32 are further included in the main unit 12. The PPU 28 is composed, for example of an integrated circuit "2C03" manufactured by Nintendo Co. Ltd, the applicants, outputting a video information signal processed by the game microprocessor 24 as a television signal for the television 18.

The semiconductor device 30 is in this embodiment a 4-bit microprocessor, for example, the integrated circuit "10NES" manufactured by Nintendo. Another semiconductor device 34 for determining authenticity is mounted on a printed circuit board (not shown) of the cartridge 16. A reset switch 36 is connected to the reset terminal of the semiconductor device 30 (lock). A reset capacitor 38 is further connected to the reset terminal in parallel with the reset switch 36. The reset capacitor 38 is charged when a power switch 40 (Fig. 1) is turned on, thereby performing a so-called initial reset (power-on-clear) which keeps the semiconductor device 30 in the reset state for a predetermined time.

A ROM 42 for storing the game program (software) and a ROM 44 for generating data defining characters for the video game are mounted on the printed circuit board of the cartridge 16. This printed circuit board of the cartridge 16 is connected electrically to the printed circuit board of the main unit 12 through the two connectors 20 and 22 as described above.

A clock signal CL from the clock oscillator 32 is applied to semiconductor device 30 (lock) and also to the semiconductor device 34 (key) through connectors 20 and 22.

As shown in Fig. 2, a predetermined terminal of the semiconductor device 30 is grounded, while a predetermined terminal of the semiconductor device 34 is connected to a power source Vcc. Thereby, these two semiconductor devices 30 and 34 are differently conditioned to assume the role of a key or a lock, respectively.

In order that the two semiconductor devices 30 and 34 exchange data with each other, the respectively corresponding terminals I, O and R are connected to each other through the connectors 20 and 22. Also, as described above, the common clock signal CL is applied to these two semiconductor devices 30 and 34 from the clock oscillator 32. Accordingly, the two semiconductor devices 30 and 34 are operated so that the respective periods and phases of operation are synchronized completely with each other.

Further detailed description is now made of the semiconductor device 30 with reference to Fig. 3. The semiconductor device 34 in the cartridge 16

has the same construction as device 30 and therefore corresponding reference numerals are shown in brackets to avoid duplicate description.

As described above, the semiconductor devices 30 and 34 determine in cooperation with each other whether the cartridge 16 is authentic. The functions of these two semiconductor devices 30 and 34 can be compared to the relationship between a lock and key. Accordingly, in the following description, the semiconductor device 30 is called a lock device and the semiconductor device 34 is called a key device.

With reference to Fig. 3, the lock device 30 is composed, for example, of a 4-bit microprocessor, comprising a CPU 30a as a data processing means and a ROM 30b and RAM 30c as semiconductor memories. The ROM 30b stores an operating program for the CPU 30a, and two arithmetic routines are contained in this operating program. Thus a plurality of formulas and random number data for arithmetic computation according to such formulas are contained in one operating program. The operating program also includes a program routine for comparing the computation result of the arithmetic routines in the lock device 30 with the result computed by the key device 34 and vice versa, and a routine for determining whether the results agree. The CPU 30a of lock device 30 functions as a determining means when these comparison and determination program routines are executed.

Furthermore, a control program routine for controlling reset or release of reset of the main unit 12 based on the results of the comparison and determination routines is contained in the operating program.

An accumulator 30d is connected to the CPU 30a. A register 30e is connected to the ROM 30b. This register 30e is for temporarily storing the program data accessed from the ROM 30b. Furthermore, a frequency divider 30f for receiving the clock signal CL from the clock oscillator 32 (Fig. 2) and dividing the frequency thereof is installed in the lock device 30, and the ratio of frequency division of the frequency divider 30f is set, for example, to $\frac{1}{4}$. The CPU 30a executes sequential program steps in response to signals of respective phases $\phi 1$, $\phi 2$, $\phi 3$ and $\phi 4$ from the frequency divider 30f.

The CPU 30a, the accumulator 30d and the register 30e are connected by a data bus 30g. This data bus 30g is connected to an I/O port 30h. Data is outputted from the I/O port 30h to the key device 34, and data from the key device 34 is received through the I/O port 30h. Furthermore, two reset signals RESET 1 and RESET 2 are outputted from the I/O port 30h. The reset signal RESET 1 is applied to the key device 34 to reset it. The reset signal RESET2 is applied to the game microprocessor 24 and the PPU 28 which are contained in the main unit 12 to reset them. In order to release the reset states of the key device 34 and the main unit 12, these reset signals RESET1 and RESET2 have only to assume the opposite (inverse) state.

Next, a brief description is made of the operation of the frequency divider 30f with reference to Fig. 4. As described above, the frequency divider 30f divides the frequency of the clock signal CL from the clock oscillator 34 by 4. Accordingly, four signals $\phi 1$, $\phi 2$, $\phi 3$ and $\phi 4$ each having a respective, different phase are obtained from the frequency divider 30f. These signals $\phi 1$ - $\phi 4$ are applied to the CPU 30a. The CPU 30a performs operations in sequence in synchronism with these four signals $\phi 1$ - $\phi 4$. For example, data from the I/O port 30h is read in synchronism with the signal $\phi 1$, and predetermined arithmetic operations (data processing) are performed in response to the signals $\phi 2$ and $\phi 3$. Then, data from the I/O port 30h is outputted by the final signal $\phi 4$.

Meanwhile, these signals $\phi 1$ - $\phi 4$ are applied also to the key device 34, and accordingly, the lock device 30 and the key device 34 are operated in complete synchronism with each other. Specifically, the lock device 30 and the key device 34 have the same number of steps in their operating programs and have the same architecture, including the same hardware and the same clock signal, and therefore respective machine cycles coincide completely.

Next, a brief description is made of the operation of the embodiment with reference to Fig. 5. A more detailed description of the operation is made later with reference to Fig. 6.

First, the cartridge 16 is loaded into the main unit 12, and the power switch 40 (Fig. 1) of the main unit 12 is turned on to start the operation (step S1). In the following step S2, the lock device 30 outputs the reset signal RESET2 and resets the game microprocessor 24, and the PPU 28 comprised in the main unit 12, holding this state. No game can be played when the main unit 12 is reset.

Next, in step S3, the lock device 30 is synchronized with the key device 34. A method of synchronization thereof is described with reference to Fig. 4. The machine cycle of the lock device 30 is set so that the reset signal RESET1 applied to the key device 34 from the lock device 30 is outputted between signal $\phi 4$ of a certain period of the clock signal CL and the signal $\phi 1$ of the next period. Consequently the signal $\phi 1$ is first inputted without fail to the key device 34. Consequently, the key device 34 can start operation from the same machine cycle $\phi 1$ as that of the lock device 30. Thus, in step S3 the lock-device 30 is synchronized with the key device 34, and thereafter the respective

devices 30 and 34 execute predetermined operations in complete synchronization.

Next, in step S4, predetermined arithmetic operations are performed respectively by the lock device 30 and the key device 34. At this time, the arithmetic operation performed by the lock device 30 and the arithmetic operation performed by the key device 34 are the same. Accordingly, if the cartridge 16 is authentic, the results of the two arithmetic operations performed in this step S4 will be the same.

In step S5, the above-described results of the operations are transferred mutually between the lock device 30 and the key device 34. Then, in step S6, the lock device 30 and the key device 34 compare these two arithmetic operation results respectively. If it is determined in step S7 that these two results coincide, then, in step S8, the lock device 30 releases the reset signals RESET1 and RESET2, releasing the reset states of the key device 34 and the main unit 12.

Conversely, if, in step S7, it is determined that the results do not coincide, then, in step S9, the lock device 30 continues to output the reset signals RESET1 and RESET2, and, accordingly, the reset states of the key device 34 and the main unit 12 are continued. The operator cannot play the game in this reset state.

Next, further detailed description on the operation is made with reference to Fig. 6. With reference to Fig. 6, if the cartridge 16 is loaded into the main unit 12 and the power switch 40 (Fig. 1) of the main unit 12 is turned on or the reset switch 36 is turned on, the resetting operation of the lock device 30 is performed, and this lock device 30 starts its operating sequence at step S10.

In the following step S11, the lock device 30 determines whether it functions as the lock or as the key. As explained with reference to Fig. 2, this determination is performed by detecting whether the predetermined terminal is grounded or connected to the power source Vcc. In this case, the lock device 30 is determined to function as the lock, but in the case where the determination indicates a key function, for example, due to wiring error, malfunction or the like, an unstable state takes place and no operations are performed at all.

In step S11, when "YES" is determined, in step S12, the lock device 30 outputs the reset signal RESET2 so that the main unit 12 cannot execute the game program, and the reset state of the main unit 12 is continued. The game microprocessor 24 and the PPU 28 (Fig. 2) are forced to the reset state and disabled until the reset is released in the later-described step S21. In this step S12, the reset signal RESET1 is also outputted to reset the key device 34.

In the next step S13, the lock device 30 releases the reset state of the key device 34, and synchronizes the two devices 30 and 34 with each other as in the above-described step S3 (Fig. 5). Thereby, the two devices 30 and 34 are synchronized with each other, and thereafter the respective devices execute sequential program steps in complete synchronism.

When the reset state of the key device 34 is released in step S13, the key device 34 determines whether it functions as the lock or as the key in the next step S11'. The determination in this step S11' can be made by detecting whether the predetermined terminal of the key device 34 is grounded or connected to the power source Vcc as in the above-described step S11. If "NO" is determined in this step S11', an unstable state takes place and no operations are performed at all.

When "YES" is determined in step S11', operations in the following steps S14' and the steps thereafter are executed.

In the lock device 30, operations in steps S14 and thereafter are executed after the step S13 is executed. Accordingly, in the lock device 30 and the key device 34, the very same operations are performed in synchronism, that is, in coincidence as a function of time.

First, the lock device 30 and the key device 34 output data representing random numbers from the respective program ROMs 30b and 34b (Fig. 3) in step S14 and in step S14'. Output of these random number data is performed using the very same random function. Also the conditions determining operation of the random function are the same for the two devices 30 and 34. Accordingly, when the cartridge is authentic, the random number data generated in the key device 34 should be the same.

Next, in steps S15 and S15', the lock device 30 and the key device 34 exchange data with each other, and read the random number data generated by the counterpart, respectively. Then, in steps S16 and S16', the devices 30 and 34 perform the predetermined data processing or arithmetic operations based on the random number data inputted from the counterpart. The arithmetic operations formula used for the first arithmetic operation in these steps S16 and S16' is the same in the two devices 30 and 34, and therefore the results of these operations become the same when the inputted random number data are the same. Then, in steps S17 ad S17', the lock device 30 and the key device 34 output the results of the arithmetic operations to the counterpart, respectively. Responsively, in steps S18 and S18', the two devices 30 and 34 mutually receive the results of the arithmetic operation outputted from the counterpart. In this case, the lock device 30 and the key device 34 perform

the same operation at the same timing. Accordingly, in this embodiment, both coincidence of the results of arithmetic operations and coincidence of time that results are received are taken into account to determine authenticity of the cartridge.

Next, in step S19, the lock device 30 compares the result of its arithmetic operation against the result of the operation produced by the key device 34, determining whether or not they coincide. As a result of this comparison, if "NO" is determined in step S20, the lock device 30 in step S22 holds the reset state of each circuit in the main unit 12, namely, the game microprocessor 24 and the PPU 28. Thereby, the main unit 12 is prevented from executing the game program.

Meanwhile, an alarm may be generated in response to a determination of non-coincidence instead of maintaining a hold of the reset states, or the processing may return to the initial state, namely, the step S11.

As a result of the comparison in step S19, if "YES" is determined in step S20, the lock device 30 releases the reset states of these circuits, namely, the game microprocessor 24 and the PPU 28 in the next step S21.

Subsequently, in step S23, the lock device 30 generates two, a first and a second, random number data based on a predetermined random function. Then, in step S24, the lock device 30 selects the kind of arithmetic operation formula using the second of the random number data, and sets the first and the second random number data as the values to be substituted into the arithmetic operation formula. More specifically, in this embodiment, n (positive integer) kinds of arithmetic operation formulas are set in advance in the arithmetic operation program in the ROM 30b (Fig. 3), and from among them, an arithmetic operation formula is selected in response to the second random number data. Subsequently, in step S25, the selected arithmetic operation wherein the first and the second random number data are substituted is executed based on the selected arithmetic operation formula.

Operations in these steps S19 - S25 are also performed in the same manner at the same timing in the key device 34. Then, the same random function for generating the first and the second random number data as that used for the lock device 30 is also used in the case of the key device 34. Also, conditions for the random function for generating the first and the second random number data are the same for the lock device 30 and the key device 34 as described above. Accordingly, if the cartridge 16 is authentic, the same arithmetic operation formula is selected for the two devices 30 and 34, and the results of these arithmetic operations should be the same.

Next, in step S26, the lock device 30 passes the results of the arithmetic operation performed in step S25 to the key device 34, and also receives the results of the arithmetic operation performed by the key device 34. A similar operation is performed in the key device 34. Next, in steps S27 and S28, the lock device 30 compares and checks the results of its arithmetic operation against the results of the arithmetic operation received from the key device 34 and determines whether or not they agree, i.e. coincide with each other.

If the cartridge 16 loaded into the main unit 12 is not authentic, the results of the arithmetic operations will not coincide, and therefore, in this case, the lock device 30, in step S29, outputs the reset signal RESET 2, to force the game microprocessor 24, and the PPU 28 of the main unit 12 into the reset state to stop their operations.

In the alternative, when the lock device 30 determines that the result of its arithmetic operation and the result of the arithmetic operation received from the key device 34 coincide with each other, processing returns again to step S24, and thereafter the operations in steps S24 - S28 are repeated. In other words, in this embodiment, as long as the main unit 12 is operating, the second arithmetic operation program routine in steps S24 - S28 is executed repeatedly, and when a non-coincidence of the results of the arithmetic operations occurs even once, step S29 is executed and the main unit 12 is stopped.

In addition, the same operations as those in steps S26 - S29 are performed in the key device 34. However, the key device 34 has no effect on resetting and releasing each circuit of the main unit 12. This is because no reset signal is outputted to the main unit 12 from the key device 34.

As for the operation of the key device 34 corresponding to step S29, since a chip-select terminal is normally installed in the ROMs 42 and 44 (Fig. 2), this chip-select terminal may be disabled. When the chip-select terminal is disabled, the game microprocessor 24 and the PPU 28 of the main unit 12 cannot access those ROMs 42 and 44, and therefore continuation of the game operation becomes impossible.

Determination of authenticity of the external memory cartridge can be made not only by checking the results of the first arithmetic operations in step S16 and step S16', but also in the above-described embodiment, by performing the second arithmetic operations and checking of the results thereof in steps S24 - S28 repeatedly as long as the main unit 12 is operating, and therefore the determination of authenticity of the cartridge 16 can be made nearly certain. Accordingly, in the case where a cartridge containing ROMs that are non-authentic copies of the ROMs 42 and 44 in the

cartridge 16 or a cartridge containing ROMs storing similar programs is used, the software protection system cannot be defeated unless the same hardware as provided in the key device 34 is employed. Also, by using devices such as custom ICs or the like which are difficult to obtain normally, such a protection can be made more complete.

Thus, the protection of programs (software) contained in the cartridge 16 can be made complete by installing the key device 34 for determining authenticity of the cartridge 16 and determining how it cooperates with the lock device 30 of the main unit 12, and accordingly any copied or forged cartridge, that is, a cartridge other than an authentic one is blocked from operating in unit 12.

Fig. 7 is a flow chart showing a modified example of Fig. 6. Nearly the same hardware as the embodiment of Fig. 6 is employed also in this embodiment, and for this Fig. 7 embodiment, though not illustrated, a counter is formed in the RAM 30c of the lock device 30 and the RAM 34c of the key device 34 (Fig. 3), respectively. Then, by utilizing this counter, the second arithmetic operation is repeated a predetermined number of times set by this counter.

The operations in steps S110 - S120 and S111' - 119' of this Fig. 7 embodiment are the same as those in steps S10 - S20 and S11' - S19' (in Fig. 6), and therefore duplicate description is omitted here.

If a coincidence of the results of the first arithmetic operations is determined in step S120, in the Fig. 7 embodiment, the counter formed in the RAM 30c of the lock device 30 is reset in step S121. The second arithmetic operation is executed in the following steps S123 - S128 as described for steps S23 - S28 in Fig. 6. Then, if a coincidence of the results of the two arithmetic operations is determined in step S128, the lock device 30 increments the counter (not illustrated) formed in the RAM 30c in the next step S130. Then, in the next step S131, determination is made of whether or not the value of the counter is the predetermined value. If the counted value of the counter has not reached the predetermined value, the lock device 30 repeats steps S123-S130.

Then, if "YES" is determined in step S131, that is, if the second arithmetic operation has been repeated by the predetermined number of times, the lock device 30 releases the reset state of the game microprocessor 24 and the PPU 28 of the main unit 12 in step S132 as in step S21 in Fig. 6.

In addition, in the embodiment of Fig. 7, the second arithmetic operation is performed a predetermined number of times in steps S123 - S131, but the number of times may be one.

If the results of the first arithmetic operations in steps S114 - S116 coincide, the main unit 12 is enabled immediately, and thereafter the second arithmetic operation as shown in steps S132 - S131 is repeated. When "NO" is determined in step S128 during the repetition, the main unit 12 is disabled, and if non-coincidence does not occur by repeating the second arithmetic operation, thereafter the main unit 12 may remain enabled until the power switch 40 (Fig. 1) of the main unit 12 is turned off.

Furthermore, steps S22 and S29 in Fig. 6 and steps S122 and S129 in Fig. 7, may be modified as follows. Black screen data for wholly blackening the screen of the television 18 and title data for displaying a game title are stored in advance in the ROM 42 of the cartridge 16. Then, in the above-described step S22 or S29 and step S122 or S129, a pulse-reset signal is outputted from the lock device 30, and thereby the black screen and the title screen are displayed repeatedly in an alternating fashion. Thereby the operator is informed that the cartridge 16 is not authentic.

The ROM cartridge 16 is used for an external memory in the above-described embodiment. However a magnetic memory for example, floppy disk, magnetic card or an optical memory, for example, optical disk or the like may be used in place of cartridge 16 as the external memory.

Fig. 8 is a perspective view showing another type of game machine. This embodiment employs a floppy disk for an external memory. In the configuration of the Fig. 1 embodiment, the floppy disk cannot be employed without modification, and therefore in the Fig. 8 embodiment, an adapter 46 is used which has the same shape as that of the cartridge 16 (Fig. 1) and which is attachable and detachable to the main unit 12. A disk reader 48 is connected to this adapter 46. Then, a floppy disk 50 is loaded into this reader 48. Accordingly, the program (software) written in advance to the floppy disk 50 is read by the reader 48, and is sent to the main unit 12 through the adapter 46.

As shown in Fig. 9, the floppy disk 50 comprises a case 52 and a disc-shaped magnetic sheet 54 supported rotatably in the case 52. The key device 34 and an electrode 56 for connecting the key device 34 are formed in the case 52.

As shown in Fig. 9, inside the reader 48 receiving such a floppy disk 50, a disk drive 58 is accommodated and also a contact 60 connected to an electrode 56 is installed. Accordingly, the key device 34 installed in the case 52 of the floppy disk 50 is connected to the lock device 30 of the main unit 12 through the electrode 56 and the contact 60.

In the embodiment of Fig. 8, operation is executed following the program as shown in Fig. 6 or 7 by cooperation of the lock device 30 (Fig. 2) comprised in the main unit 12 and the key device

34 installed in the case of the floppy disk 50, and thereby determination is made whether or not the floppy disk 50 is authentic.

Meanwhile, the lock device 30 (Fig. 2) may be installed in the reader 48, not in the main unit 12. In this case, the reset signal will be given to the main unit 12 from the reader 48.

Furthermore, in the case where a memory means is comprised in the apparatus itself which is connected to the adapter 46, for example, in the case where a sound source apparatus comprising a synthesizer ROM or the like is connected, the key device 34 is installed in the adapter 46, and the operation in Fig. 6 or Fig. 7 may be executed by this key device 34 and the lock device 30 built into the main unit 12.

In addition, in the above-described embodiment, microprocessors are employed for the lock device 30 and the key device 34. However, for these devices 30 and 34, simpler digital arithmetic operation devices may be employed, and furthermore analog processors may be employed which perform analog processing in place of digital processing. Also, a digital circuit may be employed in either of the lock device 30 and the key device 34 and an analog circuit in the other device.

In the case where an analog circuit is employed, various configurations can be utilized other than the above-described analog processor. For example, determination of the authenticity of the external memory (software) may be performed by a coincidence of frequencies of the clock signal CL converted by both the lock device and the key device following the same program. Furthermore, pulse signals are outputted from the lock device 30 and the key device 34, and the duty ratio of the pulse signals is converted following a predetermined program, and thereby authenticity can be determined by a coincidence of the duty ratios. Or, for example, determination may be made by a coincidence of levels of integrations of the same saw-tooth waves, and further differentials may be used. Or authenticity of the external memory can be determined by determining a coincidence of the results of analog processes performed by the two devices.

Claims

1. A system for determining the authenticity of software in an information processing apparatus, the system comprising a main unit (12), an external memory (16) in which said software is stored, a main processor (28) in said main unit (12), connector means (20,22) for removably connecting the external memory (16) to said main unit (12) to allow execution of the software by the main processor (28), a first authenticating device (34) associated with said external memory (16), a second authenticating device (30) in said main unit (12), said devices each having an associated memory (34b,30b) and being cooperable to determine, under the control of determining means (30), the authenticity of the software, and control means (30) operable in response to said authenticity determination,

   characterised in that said first and second authenticating devices (34,30) comprise first and second CPU's (34a,30a) respectively, said first CPU (34a) being arranged to execute a first predetermined authenticating program stored in its associated memory (34b) and said second CPU being arranged to execute a second pre-determined authenticating program stored in its associated memory (30b); and in that said control means (30) keeps the main processor (28) reset during the execution of said authenticating programs and does not release the main processor unless the execution of said first authenticating program by said first CPU (34a) exhibits a predetermined relationship to the execution of said second authenticating program by said second CPU (30a).

2. A system as claimed in claim 1, characterised in that said first and second authenticating devices (34,30) have substantially identical CPU's (34a,30a).

3. A system as claimed in claim 1, characterised in that said first and second authenticating devices (34,30) each comprise a substantially identical analog processing device, and said control means (30) comprises said determining means (30), for determining whether the results of execution of said authenticating programs by said analog processing devices are the same, and thereby exhibit said predetermined relationship.

4. A system as claimed in claim 1 or claim 2, wherein said CPU's (34a,30a) are programmed to send a RESET signal to said main processor (28) on connecting said external memory (16) to said main unit (12).

5. A system as claimed in claim 1 or claim 2 or claim 4, wherein said first and second authenticating programs include the same arithmetic operation routine, and said determining means (30) is arranged to determine whether or not the results of executing said arithmetic operation routine by said first and second CPU's (34a,30a) coincide in time and value.

34 installed in the case of the floppy disk 50, and thereby determination is made whether or not the floppy disk 50 is authentic.

Meanwhile, the lock device 30 (Fig. 2) may be installed in the reader 48, not in the main unit 12. In this case, the reset signal will be given to the main unit 12 from the reader 48.

Furthermore, in the case where a memory means is comprised in the apparatus itself which is connected to the adapter 46, for example, in the case where a sound source apparatus comprising a synthesizer ROM or the like is connected, the key device 34 is installed in the adapter 46, and the operation in Fig. 6 or Fig. 7 may be executed by this key device 34 and the lock device 30 built into the main unit 12.

In addition, in the above-described embodiment, microprocessors are employed for the lock device 30 and the key device 34. However, for these devices 30 and 34, simpler digital arithmetic operation devices may be employed, and furthermore analog processors may be employed which perform analog processing in place of digital processing. Also, a digital circuit may be employed in either of the lock device 30 and the key device 34 and an analog circuit in the other device.

In the case where an analog circuit is employed, various configurations can be utilized other than the above-described analog processor. For example, determination of the authenticity of the external memory (software) may be performed by a coincidence of frequencies of the clock signal CL converted by both the lock device and the key device following the same program. Furthermore, pulse signals are outputted from the lock device 30 and the key device 34, and the duty ratio of the pulse signals is converted following a predetermined program, and thereby authenticity can be determined by a coincidence of the duty ratios. Or, for example, determination may be made by a coincidence of levels of integrations of the same saw-tooth waves, and further differentials may be used. Or authenticity of the external memory can be determined by determining a coincidence of the results of analog processes performed by the two devices.

Claims

1. A system for determining the authenticity of software in an information processing apparatus, the system comprising a main unit (12), an external memory (16) in which said software is stored, a main processor (28) in said main unit (12), connector means (20,22) for removably connecting the external memory (16) to said main unit (12) to allow execution of the software by the main processor (28), a first authenticating device (34) associated with said external memory (16), a second authenticating device (30) in said main unit (12), said devices each having an associated memory (34b,30b) and being cooperable to determine, under the control of determining means (30), the authenticity of the software, and control means (30) operable in response to said authenticity determination,

   characterised in that said first and second authenticating devices (34,30) comprise first and second CPU's (34a,30a) respectively, said first CPU (34a) being arranged to execute a first predetermined authenticating program stored in its associated memory (34b) and said second CPU being arranged to execute a second pre-determined authenticating program stored in its associated memory (30b); and in that said control means (30) keeps the main processor (28) reset during the execution of said authenticating programs and does not release the main processor unless the execution of said first authenticating program by said first CPU (34a) exhibits a predetermined relationship to the execution of said second authenticating program by said second CPU (30a).

2. A system as claimed in claim 1, characterised in that said first and second authenticating devices (34,30) have substantially identical CPU's (34a,30a).

3. A system as claimed in claim 1, characterised in that said first and second authenticating devices (34,30) each comprise a substantially identical analog processing device, and said control means (30) comprises said determining means (30), for determining whether the results of execution of said authenticating programs by said analog processing devices are the same, and thereby exhibit said predetermined relationship.

4. A system as claimed in claim 1 or claim 2, wherein said CPU's (34a,30a) are programmed to send a RESET signal to said main processor (28) on connecting said external memory (16) to said main unit (12).

5. A system as claimed in claim 1 or claim 2 or claim 4, wherein said first and second authenticating programs include the same arithmetic operation routine, and said determining means (30) is arranged to determine whether or not the results of executing said arithmetic operation routine by said first and second CPU's (34a,30a) coincide in time and value.

* C L M S *

6. A system as claimed in any preceding claim wherein said CPU's (34a,30a) are programmed:

a) to synchronise themselves whilst the main processor (28) is in a reset state, then

b) to execute their stored authenticating programs in synchronism, then

c) to exchange data and compare the results of executing said programs in the respective CPU's before releasing the main processor from its reset state.

7. A system as claimed in claim 5 or claim 6, wherein a clock means (32) is arranged to send the same clock signal (CL) to said first and second CPU's (34a,30a) via said connector means (20,22) to synchronise the execution of said authenticating programs by said CPU's.

8. A system as claimed in claim 7 wherein said second authenticating device (30) constitutes said determining means (30), and said clock means (32) are permanently connected to said second CPU (30a).

9. A system as claimed in any one of claims 5 to 8, characterised in that said first and second authenticating programs each comprise at least first and second processing routines, and said determining means (30) comprises means for determining coincidence of the results of the execution of said first and second routines.

10. A system as claimed in claim 9, characterised in that said CPU's (34a,30a) are arranged to repeat the execution of said second routine in accordance with said authenticating program, and said determining means (30) comprises means for determining whether or not the results of executing said second routine coincide every time said second routine is repeated.

11. A system as claimed in claim 10, characterised in that it further comprises means for counting the number of times that the execution of the second routine has been repeated by said first and second CPU's (34a,30a).

12. An external memory unit (16) for connection to a main data processor unit (12) to form an information processing apparatus, said external memory unit (16) comprising a program memory means (42) storing a software program that is to be executed by the main data processor unit (12), and a microprocessor device (34) having a memory (34b) and a CPU (34a) which is arranged to execute a predetermined verification program stored in said memory (34b) when said memory unit (16) is connected to the main data processor unit (12) and while said main data processor unit (12) is held in a reset state, in order to verify that said software program stored in said program memory means (42) is authorised for use in the main data processor unit (12).

13. An external memory unit (16) as claimed in claim 12 for storing a video game program to be executed by said main data processor unit (12) said software program being a video game program and said memory unit (16) further comprising character memory means (44) having stored data defining video game-related characters, and connector means (22) coupled to said program memory means (42), said character memory means (44) and said CPU (34a) and arranged to connect said external memory unit (16) to said main data processor unit (12), said microprocessor device (34) including:

input means (34h) for receiving data, when connected in use to said main data processing unit (12) via said connector means,

output means (34h) for transferring data related to the results of the execution of said verification program, when connected in use to said main data processing unit (12), via said connector means (22), and

synchronizing input means (34b) for receiving, in use, a synchronization signal, via said connector means (22),

said CPU (34a) being programmed to receive, in response to said synchronisation signal, a value generated by said main data processing unit (12), to perform predetermined arithmetic operations on said value, and to transfer results of said arithmetic operations to said output means (34h).

14. An external memory unit (16) according to claim 13, wherein said CPU (34a) is arranged to receive further values via said input means (34h) from said main data processing unit (12) and is programmed to compare said results with said further values.

15. An external memory unit (16) according to claim 14, wherein said CPU (34a) is programmed to be responsive to the detection of coincidence between said results and said further values to perform at least a further arithmetic operation.

16. An external memory (16) unit according to claim 15, wherein said CPU (34a) is programmed to output the result of said further

* C L M S *

arithmetic operation.

17. An external memory unit (16) according to claim 15 or claim 16, wherein said CPU (34a) is programmed to perform repetitively further arithmetic operations.

18. An external memory unit (16) according to claim 17, wherein said CPU (34a) is arranged in use to execute further arithmetic operations during video game program execution.

19. An external memory unit (16) in accordance with claim 13, wherein said microprocessor device (34) includes clock signal input means (34f) coupled to said connector means (22) for receiving, in use, clock signals (CL) from said main data processor unit (12).

20. An external memory unit (16) according to claim 19, wherein said microprocessor device (34) includes means (34f) responsive to said clock signals (CL) for generating a plurality of timing signals each of which initiates the performance of a predetermined processing operation.

21. An external memory unit (16) according to claim 20, wherein said microprocessor device (34) is responsive to said plurality of timing signals to receive data from said main data processor unit (12) in response to a first timing signal, to perform predetermined arithmetic operations in response to a second timing signal and to transfer data to said main processor unit (12) in response to a third timing signal.

22. An external memory unit (16) as claimed in claim 12 which is a video game cartridge.

Patentansprüche

1. System zum Feststellen der Echtheit von Software in einer Informationsverarbeitungsanlage, wobei das System aufweist:
eine Haupteinheit (12), einen externen Speicher (16), in welchem die Software gespeichert ist, einen Hauptprozessor (28) in der Haupteinheit (12), Verbindungsmittel (20, 22) zum lösbaren Verbinden des externen Speichers (16) mit der Haupteinheit (12), um die Ausführung der Software durch den Hauptprozessor (28) zu ermöglichen, eine erste Echtheitfeststellungsvorrichtung (34), die mit dem externen Speicher (16) verbunden ist, eine zweite Echtheitfeststellungsvorrichtung (30) in der Haupteinheit (12), wobei die Vorrichtungen jeweils einen zugeordneten Speicher (34b, 30b) haben und zusammenwirken können, um unter der Steuerung der Feststellungsmittel (30) die Echtheit der Software festzustellen, und Steuermittel (30), die in Reaktion auf die Echtheitfeststellung betreibbar sind, dadurch gekennzeichnet, daß die erste und zweite Echtheitfeststellungsvorrichtung (34, 30) eine erste bzw. zweite Zentraleinheit (34a, 30a) aufweisen, wobei die erste Zentraleinheit (34a) so angeordnet ist, daß sie ein in ihrem zugeordneten Speicher (34b) gespeichertes erstes vorbestimmtes Echtheitfeststellungsprogramm ausführt, und die zweite Zentraleinheit so angeordnet ist, daß sie ein in ihrem zugeordneten Speicher (30b) gespeichertes zweites vorbestimmtes Echtheitfeststellungsprogramm ausführt, und daß die Steuermittel (30) den Hauptprozessor (28) während der Ausführung des Echtheitfeststellungsprogramms zurückgesetzt hält und den Hauptprozessor nur freigibt, wenn die Ausführung des ersten Echtheitfeststellungsprogramms durch die erste Zentraleinheit (34a) ein vorbestimmtes Verhältnis zu der Ausführung des zweiten Echtheitfeststellungsprogramms durch die zweite Zentraleinheit (30a) aufweist.

2. System nach Anspruch 1, dadurch gekennzeichnet, daß die erste und zweite Echtheitfeststellungsvorrichtung (34, 30) im wesentlichen identische Zentraleinheiten (34a, 30a) haben.

3. System nach Anspruch 1, dadurch gekennzeichnet, daß die erste und zweite Echtheitfeststellungsvorrichtung (34a, 30a) jeweils eine im wesentlichen identische analoge Verarbeitungsvorrichtung aufweisen und daß die Steuermittel (30) die Feststellungsmittel (30) aufweisen, um festzustellen, ob die Ergebnisse der Ausführung des Echtheitfeststellungsprogramms durch die analogen Verarbeitungsvorrichtungen dieselben sind und dadurch das vorbestimmte Verhältnis aufweisen.

4. System nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Zentraleinheiten (34a, 30a) so programmiert sind, daß sie ein ZURÜCKSETZEN-Signal zu dem Hauptprozessor (28) senden, wenn der externe Speicher (16) mit der Haupteinheit (1) verbunden wird.

5. System nach Anspruch 1, 2 oder 4, dadurch gekennzeichnet, daß das erste und das zweite Echtheitfeststellungsprogramm dasselbe arithmetische Betriebsprogramm aufweisen und daß die Feststellungsmittel (30) angeordnet sind, um festzustellen, ob die Ergebnisse der Ausführung des arithmetischen Betriebspro-

gramms durch die erste und zweite Zentraleinheit (34a, 30a) in Zeit und Wert übereinstimmen oder nicht.

6. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Zentraleinheiten (34a, 30a) programmiert sind:
   a) um sich selbst zu synchronisieren, während der Hauptprozessor in einem zurückgesetzten Zustand ist, dann
   b) zum synchronisierten Ausführen ihrer gespeicherten Echtheitfeststellungsprogramme, und dann
   c) zum Austauschen von Daten und Vergleichen der Ergebnisse der Programmausführungen in den jeweiligen Zentraleinheiten, bevor der Hauptprozessor aus seinem zurückgesetzten Zustand freigegeben wird.

7. System nach Anspruch 5 oder 6, dadurch gekennzeichnet, daß Taktgebermittel (32) angeordnet sind, um über die Verbindungsmittel (20, 22) dasselbe Taktsignal (CL) an die erste und zweite Zentraleinheit (34a, 30a) zu senden, um die Ausführung des Echtheitfeststellungsprogramms durch die Zentraleinheiten zu synchronisieren.

8. System nach Anspruch 7, dadurch gekennzeichnet, daß die zweite Echtheitfeststellungsvorrichtung (30) die Feststellungsmittel (30) bilden und die Taktgebermittel (32) permanent mit der zweiten Zentraleinheit (30a) verbunden sind.

9. System nach einem der Ansprüche 5 bis 8, dadurch gekennzeichnet, daß das erste und zweite Echtheitfeststellungsprogramm jeweils mindestens erste und zweite Verarbeitungsprogramme aufweisen und daß die Feststellungsmittel (30) Mittel zum Feststellen der Übereinstimmung der Ausführungsergebnisse des ersten und zweiten Programms aufweisen.

10. System nach Anspruch 9, dadurch gekennzeichnet, daß die Zentraleinheiten (34a, 30a) angeordnet sind, um die Ausführung des zweiten Programms in Übereinstimmung mit dem Echtheitfeststellungsprogramm zu wiederholen, und daß die Feststellungsmittel (30) Mittel zum Feststellen aufweisen, ob die Ergebnisse der Ausführung des zweiten Programmes bei jedem Wiederholen des zweiten Programmes identisch sind.

11. System nach Anspruch 10, dadurch gekennzeichnet, daß es weiterhin Mittel aufweist, die zählen, wie oft die Ausführung des zweiten Programmes durch die erste und zweite Zentraleinheit (34a, 30a) wiederholt wurde.

12. Externe Speichereinheit (16) zum Verbinden mit einer Hauptdatenverarbeitungseinheit (12) zur Bildung einer Informationsverarbeitungsanlage, wobei die externe Speichereinheit (16) Programmspeichermittel (42) aufweist, die ein Softwareprogramm speichern, das von der Hauptdatenverarbeitungseinheit (12) ausgeführt werden soll, und eine Mikroprozessorvorrichtung (34) mit einem Speicher (34b) und einer Zentraleinheit (34a), die zum Ausführen eines vorbestimmten in dem Speicher (34b) gespeicherten Verifikationsprogramm angeordnet sind, wenn die Speichereinheit (16) mit der Hauptdatenverarbeitungseinheit (12) verbunden ist und während die Hauptdatenverarbeitungseinheit (12) in einem zurückgesetzten Zustand gehalten ist, um zu verifizieren, daß das in den Programmspeichermitteln (42) gespeicherte Programm für eine Verwendung in der Hauptdatenverarbeitungseinheit (12) zugelassen ist.

13. Externe Speichereinheit (16) nach Anspruch 12 zum Speichern eines Videospiel-Programms, das von der Hauptdatenverarbeitungseinheit (12) ausgeführt werden soll, wobei das Softwareprogramm ein Videospiel-Programm ist und die Speichereinheit (16) weiterhin Zeichen-Speichermittel (44) mit gespeicherten Daten aufweist, die die zum Videospiel gehörenden Zeichen definieren, und Verbindungsmittel (22), die mit den Programmspeichermitteln (42) verbunden sind, wobei die Zeichen-Speichermittel (44) und die Zentraleinheit (34a) so angeordnet sind, daß sie die externe Speichereinheit (16) mit der Hauptdatenverarbeitungseinheit (12) verbinden, wobei die Mikroprozessorvorrichtung (34) folgendes aufweist:
Eingangsmittel (34h) zum Empfangen von Daten, wenn die Eingangsmittel (34h) bei Betrieb über die Verbindungsmittel mit der Hauptdatenverarbeitungseinheit (12) verbunden sind,
Ausgangsmittel (34h) zum Übertragen von auf die Ergebnisse der Ausführung des Verifikationsprogramms bezogene Daten, wenn die Ausgangsmittel (34h) bei Betrieb über die Verbindungsmittel (22) mit der Hauptdatenverarbeitungseinheit (12) verbunden sind, und Synchronisierungs-Eingangsmittel (34b) zum Empfangen eines Synchronisierungssignals über die Verbindungsmittel (22) bei Betrieb,
wobei die Zentraleinheit (34a) so programmiert ist, daß sie in Reaktion auf das Synchronisierungssignal einen Wert empfängt, der von der Hauptdatenverarbeitungseinheit (12) erzeugt wurde, um vorbestimmte arithmetische Opera-

tionen an dem Wert durchzuführen und um Ergebnisse der arithmetischen Operationen an die Ausgangsmittel (34h) zu übertragen.

14. Externe Speichereinheit (16) nach Anspruch 13, dadurch gekennzeichnet, daß die Zentraleinheit (34a) so angeordnet ist, daß sie weitere Werte über die Eingangsmittel (34h) von der Hauptdatenverarbeitungseinheit (12) empfängt, und daß sie so programmiert ist, daß sie die Ergebnisse mit den weiteren Werten vergleicht.

15. Externe Speichereinheit (16) nach Anspruch 14, dadurch gekennzeichnet, daß die Zentraleinheit (34a) so programmiert ist, daß sie auf die Feststellung einer Übereinstimmung zwischen den Ergebnissen und den weiteren Werten reagiert und mindestens eine weitere arithmetische Operation ausführt.

16. Externe Speichereinheit (16) nach Anspruch 15, dadurch gekennzeichnet, daß die Zentraleinheit (34a) so programmiert ist, daß sie das Ergebnis der weiteren arithmetischen Operation ausgibt.

17. Externe Speichereinheit (16) nach Anspruch 15 oder 16, dadurch gekennzeichnet, daß die Zentraleinheit (34a) so programmiert ist, daß sie wiederholt weitere arithmetische Operationen ausführt.

18. Externe Speichereinheit (16) nach Anspruch 17, dadurch gekennzeichnet, daß die Zentraleinheit (34a) bei Betrieb so angeordnet ist, daß sie weitere arithmetische Operationen während der Videospiel-Programmausführung durchführt.

19. Externe Speichereinheit (16) nach Anspruch 13, dadurch gekennzeichnet, daß die Mikroprozessorvorrichtung (34) Taktgebersignal-Eingangsmittel (34f) aufweist, die mit den Verbindungsmitteln (22) verbunden sind, um bei Betrieb Taktgebersignale (CL) von der Hauptdatenverarbeitungseinheit (12) zu empfangen.

20. Externe Speichereinheit (16) nach Anspruch 19, dadurch gekennzeichnet, daß die Mikroprozessorvorrichtung (34) Mittel (34f) aufweist, die auf die Taktgebersignale (CL) reagieren, um eine Mehrzahl von Taktsignalen zu erzeugen, von denen jedes die Ausführung einer vorbestimmten Verarbeitungsoperation auslöst.

21. Externe Speichereinheit (16) nach Anspruch 20, dadurch gekennzeichnet, daß die Mikroprozessorvorrichtung (34) auf die Mehrzahl der Taktsignale reagiert, um Daten von der Hauptdatenverarbeitungseinheit (12) in Reaktion auf ein erstes Taktsignal zu empfangen, um vorbestimmte arithmetische Operationen in Reaktion auf ein zweites Taktsignal durchzuführen und um Daten zu der Hauptverarbeitungseinheit (12) in Reaktion auf ein drittes Taktsignal zu übertragen.

22. Externe Speichereinheit (16) nach Anspruch 12, wobei diese eine Videospielcassette ist.

Revendications

1. Système pour déterminer l'authenticité d'un logiciel dans un appareil de traitement d'informations, le système comprenant une unité principale (12), une mémoire extérieure (16) dans laquelle est stocké le logiciel, un processeur principal (28) dans cette unité principale (12), des connecteurs (20,22) pour raccorder de façon amovible la mémoire extérieure (16) à l'unité principale (12) pour permettre au processeur principal (28) d'exécuter le logiciel, un premier dispositif d'authentification (34) associé à la mémoire extérieure (16), un deuxième dispositif d'authentification (30) dans l'unité principale (12), chacun de ces dispositifs ayant une mémoire associée (34b,30b) et pouvant coopérer pour déterminer, sous le contrôle des moyens de détermination (30), l'authenticité du logiciel, et des moyens de contrôle (30) pouvant être mis en oeuvre en réponse à la détermination d'authenticité,
caractérisé en ce que les premier et deuxième dispositifs d'authentification (34,30) comprennent une première et une deuxième unité de traitement centrale (UTC)(34a,30a) respectivement, la première UTC (34a) étant disposée pour exécuter un premier programme d'authentification prédéterminé stocké dans sa mémoire associée (34b) et la deuxième UTC étant disposée pour exécuter un deuxième programme d'authentification prédéterminé stocké dans sa mémoire associée (30b), et en ce que les moyens de contrôle (30) maintiennent le processeur principal (28) à l'état réinitialisé pendant l'exécution de ces programmes d'authentification et ne libèrent pas le processeur principal à moins que l'exécution du premier programme d'authentification par la première UTC (34a) présente une relation prédéterminée par rapport à l'exécution du deuxième programme d'authentification par la deuxième UTC (30a).

2. Système selon la revendication 1, caractérisé en ce que les premier et deuxième dispositifs

* C L M S *

d'authentification (34,30) ont des UTC pratiquement identiques (34a,30a).

3. Système selon la revendication 1, caractérisé en ce que les premier et deuxième dispositifs d'authentification (34,30) comprennent chacun un dispositif de traitement analogique pratiquement identique et en ce que les moyens de contrôle (30) comprennent des moyens de détermination (30) pour déterminer si les résultats de l'exécution des programmes d'authentification par ces dispositifs de traitement analogiques sont identiques et de ce fait présentent ladite relation prédéterminée.

4. Système selon la revendication 1 ou la revendication 2, dans lequel les UTC (34a,30a) sont programmées pour envoyer un signal de réinitialisation au processeur principal (28) lors du raccordement de la mémoire extérieure (16) à l'unité principale (12).

5. Système selon la revendication 1 ou la revendication 2 ou la revendication 4, dans lequel les premier et deuxième programmes d'authentification comprennent le même sous-programme d'opérations arithmétiques et dans lequel les moyens de détermination (30) sont agencés pour déterminer si oui ou non les résultats de l'exécution du sous-programme d'opérations arithmétiques par les première et deuxième UTC (34a,30a) coïncident dans le temps et en valeur.

6. Système selon l'une des revendications précédentes, dans lequel les UTC (34a,30a) sont programmées :
   (a) pour se synchroniser pendant que le processeur principal (28) est à l'état réinitialisé, ensuite
   (b) pour exécuter leurs programmes d'authentification stockés en synchronisme, puis
   (c) pour échanger des données et comparer les résultats de l'exécution de ces programmes dans les UTC respectives avant de libérer le processeur principal de son état réinitialisé.

7. Système selon la revendication 5 ou la revendication 6, dans lequel une horloge (32) est agencée pour envoyer le même signal d'horloge (CL) aux première et deuxième UTC (34a,30a) par l'intermédiaire des connecteurs (20,22) pour synchroniser l'exécution des programmes d'authentification par lesdites-UTC.

8. Système selon la revendication 7, dans lequel le deuxième dispositif d'authentification (30) constitue lesdits moyens de détermination (30), et les moyens d'horloge (32) sont raccordés de façon permanente à cette deuxième UTC (30a).

9. Système selon l'une des revendications 5 à 8, caractérisé en ce que les premier et deuxième programmes d'authentification comprennent chacun au moins un premier et un deuxième sous-programme de traitement, et en ce que les moyens de détermination (30) comprennent des moyens pour déterminer la coïncidence des résultats de l'exécution de ces premier et deuxième sous-programmes.

10. Système selon la revendication 9, caractérisé en ce que les UTC (34a,30a) sont agencées pour répéter l'exécution du deuxième sous-programme en fonction du programme d'authentification, et en ce que les moyens de détermination (30) comprennent des moyens pour déterminer si oui ou non les résultats de l'exécution du deuxième sous-programme coïncident chaque fois que ce deuxième sous-programme est répété.

11. Système selon la revendication 10, caractérisé en ce qu'il comprend en outre des moyens pour compter le nombre de fois que l'exécution du deuxième sous-programme a été répété par les première et deuxième UTC (34a,30a).

12. Unité de mémoire extérieure (16) destinée à être raccordée à un processeur de données principal (12) pour former un appareil de traitement d'informations, cette unité de mémoire extérieure (16) contenant une mémoire de programme (42) stockant un programme de logiciel qui doit être exécuté par le processeur de données principal (12), et un microprocesseur (34) ayant une mémoire (34b) et une UTC (34a) qui est agencée pour exécuter un programme de vérification prédéterminé stocké dans la mémoire (34b) quand cette mémoire extérieure (16) est raccordée au processeur de données principal (12) et, pendant que ce processeur de données principal (12) est maintenu dans un état réinitialisé, pour vérifier que ce programme de logiciel stocké dans la mémoire de programme (42) est autorisé pour être utilisé dans le processeur de données principal (12).

13. Unité de mémoire extérieure (16) selon la revendication 12, pour stocker un programme de jeu vidéo à exécuter par le processeur de données principal (12), ce programme de logi-

* C L M S *

ciel étant un programme de jeu vidéo et cette unité de mémoire (16) comprenant en outre une mémoire de caractères (44) ayant stocké des données définissant des caractères associés au jeu vidéo, et un connecteur (22) couplé à la mémoire de programme (42), à la mémoire de caractères (44) et à l'UTC (34a) et agencé pour raccorder l'unité de mémoire extérieure (16) au processeur de données principal (12), ce microprocesseur (34) comprenant :

- des moyens d'entrée (34h) pour recevoir des données, lorsqu'ils sont raccordés en service à l'unité de traitement de données principal (12) par l'intermédiaire du connecteur,
- des moyens de sortie (34h) pour transférer les données associées aux résultats de l'exécution du programme de vérification, lorsqu'ils sont raccordés en service à l'unité de traitement de données principale (12) par l'intermédiaire du connecteur (22), et
- des moyens d'entrée et de synchronisation (34b) pour recevoir, en service, un signal de synchronisation par l'intermédiaire du connecteur (22),

la UTC (34a) étant programmée pour recevoir, en réponse à ce signal de synchronisation, une valeur générée par l'unité de traitement de données principale (12), pour effectuer des opérations arithmétiques prédéterminées sur cette valeur et pour transférer les résultats de ces opérations arithmétiques aux moyens de sortie (34h).

14. Unité de mémoire extérieure (16) selon la revendication 13, dans laquelle la UTC (34a) est agencée pour recevoir d'autres valeurs par l'intermédiaire des moyens d'entrée (34h) depuis l'unité de traitement de données principale (12) et est programmée pour comparer ces résultats avec ces autres valeurs.

15. Unité de mémoire extérieure (16) selon la revendication 14, dans laquelle la UTC (34a) est programmée pour répondre à la détection d'une coïncidence entre ces résultats et ces autres valeurs pour effectuer au moins une autre opération arithmétique.

16. Unité de mémoire extérieure (16) selon la revendication 15, dans laquelle la UTC (34a) est programmée pour émettre le résultat de cette autre opération arithmétique.

17. Unité de mémoire extérieure (16) selon la revendication 15 ou la revendication 16, dans laquelle la UTC (34a) est programmée pour effectuer de façon répétitive d'autres opérations arithmétiques.

18. Unité de mémoire extérieure (16) selon la revendication 17, dans laquelle la UTC (34a) est agencée pour, en service, exécuter d'autres opérations arithmétiques pendant l'exécution du programme de jeu vidéo.

19. Unité de mémoire extérieure (16) selon la revendication 13, dans laquelle le microprocesseur (34) contient des moyens d'entrée de signaux d'horloge (34f) couplés au connecteur (22) pour recevoir, en service, des signaux d'horloge (CL) du processeur de données principal (12).

20. Unité de mémoire extérieure (16) selon la revendication 19, dans laquelle le microprocesseur (34) comprend des moyens (34f) sensibles aux signaux d'horloge (CL) pour générer une multiplicité de signaux de synchronisation dont chacun déclenche la réalisation d'une opération de traitement prédéterminée.

21. Unité de mémoire extérieure (16) selon la revendication 20, dans laquelle le microprocesseur (34) est sensible à cette multiplicité de signaux de synchronisation pour recevoir des données du processeur de données principal (12) en réponse à un premier signal de synchronisation, pour effectuer des opérations arithmétiques prédéterminées en réponse à un deuxième signal de synchronisation et pour transférer les données au processeur principal (12) en réponse à un troisième signal de synchronisation.

22. Unité de mémoire extérieure (16) selon la revendication 12, qui est une cassette de jeux vidéo.

* C L M S *