

[DESCRIPTION]

[TITLE OF INVENTION]

INFORMATION PROCESSING DEVICE, METHOD FOR CONTROLLING
INFORMATION PROCESSING DEVICE, AND PROGRAM

5 [Technical Field]

[0001]

The present invention relates to an information processing device, a method for
controlling an information processing device, and program.

[Background Art]

10 [0002]

In various information processing devices such as a car navigation system or a
game console, there is a need to use functions of the information processing devices
immediately after startup operations (power-on operations) thereof are performed.

[0003]

15 Patent Document 1 discloses a technique in which the high-speed startup of an
information processing device is realized by storing data indicating a storage state of a
volatile memory immediately before power is turned off, a register value of a peripheral
device, and a register value of a processor in a non-volatile memory, and reproducing a
state before power-off using the data stored in the non-volatile memory when power is
20 turned on again.

[Citation List]

[Patent Literature]

[0004]

[Patent Document 1]

25 Japanese Unexamined Patent Application, First Publication No. 2015-156205

[Summary of Invention]

[Technical Problem]

[0005]

Since data stored in a non-volatile memory (a snapshot image of a volatile
5 memory) for the purpose of performing high-speed startup is normally not encoded, the
data is at risk of being easily stolen by a third party. As a countermeasure, encoding a
snapshot image of a volatile memory and then storing it in a non-volatile memory can be
considered.

However, in such a case, it is necessary to decode an encoded snapshot image
10 when power is turned on again, and then to load the decoded snapshot image into a
volatile memory or the like. In this case, it takes a processing time to decode a snapshot
image, which results in the possibility of decreasing the effect of high-speed startup.

[0006]

In view of the above problem, the present invention provides an information
15 processing device, a method for controlling an information processing device, and a
program that make it possible to enable high-speed startup and to enhance security
performance.

[Solution to Problem]

[0007]

20 According to a first aspect of the present invention, there is provided an
information processing device (1) including: a decoding circuit (12b), provided on a data
bus (DB) for connecting a main memory (101) and an external storage device (11), which
is capable of switching between enabling and disabling a process for decoding
information that is transmitted through the data bus; and a readout processing unit (1002)
25 that is configured to read out information written in the external storage device in the

main memory. In addition, the readout processing unit is configured to enable the decoding process of the decoding circuit in a case where a snapshot image of the main memory is read out as the information written in the external storage device.

In this manner, when the snapshot image is read out into the main memory immediately after power-on, the encoded snapshot image is decoded at a high speed by the decoding circuit configured as hardware in a process in which the snapshot image is transmitted on the data bus from the external storage device toward the main memory. Therefore, it is possible to read out the encoded snapshot image without decreasing the effect of high-speed startup.

10 [0008]

In addition, according to a second aspect of the present invention includes: an encoding circuit (12a), provided on the data bus, which is capable of switching between enabling and disabling a process for encoding the information that is transmitted through the data bus; and a writing processing unit that writes information stored in the main memory in the external storage device. In addition, the writing processing unit is configured to enable the encoding process of the encoding circuit in a case where a snapshot image of the main memory is written as the information stored in the main memory.

In this manner, when a snapshot image is written in the external storage device immediately before power-off, a plaintext snapshot image is encoded at a high speed by the encoding circuit 12a configured as hardware in a process in which the snapshot image is transmitted on the data bus DB from the main memory-side device 10 toward the external storage device 11. Therefore, it is possible to speed up encoding of a snapshot image to be written in the external storage device 11 during power-off.

25 [0009]

In addition, according to a third aspect of the present invention, the decoding circuit includes a logical arithmetic operation element (121b) that is configured to perform the decoding process, and a selection element (120b) capable of selecting whether the information that is transmitted through the data bus passes through the logical arithmetic operation element in accordance with a control signal that is input.

In this manner, it is possible to realize a decoding circuit capable of switching between enabling and disabling a decoding process, as hardware, with an extremely simple configuration.

[0010]

In addition, according to a fourth aspect of the present invention, the above-described information processing device further includes a data recording memory for decoding (13) in which data for decoding is recorded. In addition, the decoding circuit performs the process for decoding the information that is transmitted through the data bus on the basis of the data for decoding read out from the data recording memory for decoding.

In this manner, the decoding circuit can perform decoding at a high speed using data for decoding which is read out directly from a dedicated memory (a data recording memory for decoding).

[0011]

In addition, according to a fifth aspect of the present invention, the data for decoding is information recorded in the main memory in an initial state immediately after power-on.

In this manner, it is possible to achieve encoding of a snapshot image on the basis of the information (PUF information) recorded in the main memory from the initial state. Thereby, it is possible to further enhance security performance of the information

processing device 1.

[0012]

In addition, according to a sixth aspect of the present invention, there is provided a method for controlling an information processing device including a decoding circuit, provided on a data bus for connecting a main memory and an external storage device, which is capable of switching between enabling and disabling a process for decoding information that is transmitted through the data bus includes a readout step of reading out information written in the external storage device into the main memory. In addition, the decoding process of the decoding circuit is enabled in the readout step in a case where a snapshot image of the main memory is read out as the information written in the external storage device.

[0013]

In addition, according to a seventh aspect of the present invention, there is provided a program causing an information processing device including a decoding circuit that is provided on a data bus for connecting a main memory and an external storage device and is capable of switching between enabling and disabling a process for decoding information that is transmitted through the data bus to function as a readout processing unit that is configured to read out information written in the external storage device into the main memory. In addition, the readout processing unit is configured to enable the decoding process of the decoding circuit in a case where a snapshot image of the main memory is read out as the information written in the external storage device.

[Advantageous Effects of Invention]

[0014]

According to the information processing device, the method for controlling an information processing device, and the program, it is possible to enable high-speed

startup and to enhance security performance.

[Brief Description of Drawings]

[0015]

Fig. 1 is a diagram schematically showing a hardware configuration of an
5 information processing device according to a first embodiment.

Fig. 2 is a diagram showing a functional configuration of a CPU according to
the first embodiment.

Fig. 3 is a diagram showing a functional configuration of the information
processing device according to the first embodiment and a flow of various types of
10 information.

Fig. 4 is a diagram showing a first process flow of the information processing
device according to the first embodiment.

Fig. 5 is a diagram showing operations relating to the first process flow of the
information processing device according to the first embodiment.

15 Fig. 6 is a diagram showing a second process flow of the information processing
device according to the first embodiment.

Fig. 7 is a diagram showing operations relating to the second process flow of the
information processing device according to the first embodiment in detail.

20 Fig. 8 is a diagram showing operations relating to the second process flow of the
information processing device according to the first embodiment in detail.

Fig. 9 is a diagram showing a functional configuration of a CPU according to a
second embodiment.

Fig. 10 is a diagram showing a second process flow of an information
processing device according to the second embodiment.

25 [Description of Embodiments]

[0016]

<First embodiment>

Hereinafter, an information processing device according to a first embodiment will be described in detail with reference to Figs. 1 to 8.

5 [0017]

(Hardware configuration of information processing device)

Fig. 1 is a diagram schematically showing a hardware configuration of an information processing device according to a first embodiment.

As shown in Fig. 1, an information processing device 1 includes a CPU 100, a
10 main memory 101, an external storage device 11, an encoding circuit 12a, a decoding circuit 12b, and a random number recording memory (a data recording memory for decoding) 13. In addition, the CPU 100, the main memory 101, and the external storage device 11 are connected to each other through a data bus DB.

[0018]

15 The CPU 100 is a processor that takes charge of an operation of the entire information processing device 1, and exhibits various functions by subsequently executing commands in accordance with a program prepared in advance. The CPU 100 executes an arithmetic operation process while accessing data and various types of commands which are read out into the main memory 101 on the basis of a program.

20 The main memory 101 is a volatile memory for enabling high-speed access from the CPU 100 and is also referred to as a main storage device. The main memory 101 is, for example, a dynamic random access memory (DRAM).

The external storage device 11 is a high-capacity non-volatile memory and is also referred to as an auxiliary storage device. The external storage device 11 is, for
25 example, a hard disk drive (HDD), a solid state drive (SSD), or the like.

Meanwhile, an aspect in which the external storage device 11 according to the present embodiment is built into the information processing device 1 is described (see Fig. 1), but in another embodiment, an aspect in which the external storage device is externally attached to the information processing device 1 may be used.

5 In the following description, the CPU 100 and the main memory 101 are also denoted as a main memory-side device 10 collectively.

[0019]

The data bus DB is a signal line for exchanging data (such as a numerical value which is a target for arithmetic operation and the result of an arithmetic operation)
10 between the CPU 100 and the main memory 101 and between the CPU 100 and the external storage device 11.

Meanwhile, the information processing device 1 includes an address bus and a control bus (not shown in the drawing) in addition to the data bus DB. As is the case with the data bus DB, the address bus and the control bus are signal lines for connecting
15 the CPU 100, the main memory 101 and the external storage device 11 to each other. The address bus is a signal line for designating a storage place (an address) of data intended to be written and read out in the main memory 101 and the external storage device 11. In addition, the control bus is a signal line for designating whether data is read out from or written in a storage place designated in the address bus.

20 [0020]

The encoding circuit 12a is a logic circuit, provided on the data bus DB, which performs a process for encoding information transmitted through the data bus DB. The encoding circuit 12a is configured to be capable of switching between enabling and disabling an encoding process in accordance with a control signal which is separately
25 input.

The decoding circuit 12b is a logic circuit, provided on the data bus DB, which performs a process for decoding information transmitted through the data bus DB. The decoding circuit 12b is configured to be capable of switching between enabling and disabling a decoding process in accordance with a control signal which is separately
5 input.

[0021]

The random number recording memory 13 is a storage device in which random numbers generated by the CPU 100 are recorded. Here, random numbers generated by the CPU 100 serve as data for encoding used when the encoding circuit 12a performs an
10 encoding process, and serve as data for decoding used when the decoding circuit 12b performs a decoding process. In the present embodiment, the data for encoding and the data for decoding are the same random numbers.

The random number recording memory 13 according to the present embodiment is considered to be a rewritable non-volatile memory such as a flash memory.

15 [0022]

(Functional configuration of CPU)

Fig. 2 is a diagram showing a functional configuration of a CPU according to the first embodiment.

As shown in Fig. 2, the CPU 100 operates in accordance with a program
20 prepared in advance, to thereby exhibit the functions of a writing processing unit 1001, a readout processing unit 1002, and a random number generation unit 1003.

[0023]

The writing processing unit 1001 performs a process for writing information stored in the main memory 101 in the external storage device 11.

25 The readout processing unit 1002 performs a process for reading out information

written in the external storage device 11 into the main memory 101. Here, immediately after the information processing device 1 is powered on, the CPU 100 initially reads out a program for startup (boot loader) which is set in advance. Immediately after power-on, the CPU 100 operates in accordance with the program for startup (boot loader) which is read out herein, and thus functions as the readout processing unit 1002 that reads out data stored in the external storage device 11 (a snapshot image to be described later) into the main memory 101.

The random number generation unit 1003 generates random numbers, and performs a process for storing the random numbers in the random number recording memory 13.

[0024]

(Functional configuration of information processing device and flow of various types of information)

Fig. 3 is a diagram showing a functional configuration of the information processing device according to the first embodiment and a flow of various types of information.

As shown in Fig. 3, the information processing device 1 exchanges various types of information (data, an address and a control signal) between the main memory-side device 10 and the external storage device 11.

First, hardware configurations of the encoding circuit 12a and the decoding circuit 12b will be described with reference to Fig. 3.

[0025]

As shown in Fig. 3, the encoding circuit 12a is configured to include a multiplexer 120a (a selection element) and a logical arithmetic operation element 121a.

The multiplexer 120a outputs information which is input to any one of two input

ports [1] and [2] from an output port [4]. Specifically, in a case where a control signal WR_mux which is input to a selection port [3] is “L” (Low), the multiplexer 120a outputs information which is input to the input port [1] from the output port [4]. In addition, in a case where the control signal WR_mux which is input to the selection port

5 [3] is “H” (High), the multiplexer 120a outputs information which is input to the input port [2] from the output port [4].

The logical arithmetic operation element 121a is a logical arithmetic operation element that arithmetically operates an exclusive logical sum (XOR) of two pieces of information which are input.

10 [0026]

Writing data WR_data is input to the input port [1] of the multiplexer 120a and the logical arithmetic operation element 121a. The writing data WR_data is information which is transmitted from the main memory-side device 10 through the data bus DB toward the external storage device 11, and is information which is output as information

15 to be written in the external storage device 11 by the CPU 100 (the writing processing unit 1001).

Data for encoding XOR_data recorded in the random number recording memory 13 is further input to the logical arithmetic operation element 121a. The data for encoding XOR_data is information which is used for an encoding process in the

20 encoding circuit 12a, and is specifically information which is a target for the arithmetic operation of an exclusive logical sum (XOR) together with the writing data WR_data in the logical arithmetic operation element 121a.

An arithmetic operation result of the exclusive logical sum of the writing data WR_data and the data for encoding XOR_data by the logical arithmetic operation

25 element 121a is input to the input port [2] of the multiplexer 120a.

Storage device writing data Storage_WR_data is output from the output port [4] of the multiplexer 120a. The storage device writing data Storage_WR_data is information which is actually written in the external storage device 11. In a case where the control signal WR_mux which is input to the selection port [3] of the multiplexer 120a is “L,” the storage device writing data Storage_WR_data becomes the writing data WR_data itself. That is, in a case where the control signal WR_mux is “L,” the encoding process of the encoding circuit 12a is disabled. On the other hand, in a case where the control signal WR_mux which is input to the selection port [3] of the multiplexer 120a is “H,” the storage device writing data Storage_WR_data becomes an arithmetic operation result of the exclusive logical sum by the logical arithmetic operation element 121a. That is, in a case where the control signal WR_mux is “H,” the encoding process of the encoding circuit 12a is enabled.

[0027]

In addition, as shown in Fig. 3, the decoding circuit 12b is configured to include a multiplexer 120b (a selection element) and a logical arithmetic operation element 121b.

The multiplexer 120b outputs information which is input to any one of two input ports [1] and [2] from an output port [4]. Specifically, in a case where a control signal RD_mux which is input to a selection port [3] is “H” (High), the multiplexer 120b outputs information which is input to the input port [2] from the output port [4]. In addition, in a case where the control signal RD_mux which is input to the selection port [3] is “L” (Low), the multiplexer 120b outputs information which is input to the input port [1] from the output port [4].

The logical arithmetic operation element 121b is a logical arithmetic operation element that arithmetically operates an exclusive logical sum (XOR) of two pieces of information which are input.

[0028]

Storage device readout data Storage_RD_data is input to the input port [1] of the multiplexer 120b and the logical arithmetic operation element 121b. The storage device readout data Storage_RD_data is information which is transmitted from the external storage device 11 through the data bus DB toward the main memory-side device 10, and is information which is output as information to be read out into the main memory 101 by the CPU 100 (the readout processing unit 1002).

Data for decoding XOR_data recorded in the random number recording memory 13 is further input to the logical arithmetic operation element 121b (since data for decoding according to the present embodiment is the same information as the data for encoding, the data for decoding will be described with the same reference sign as that of the data for encoding (XOR_data) assigned thereto). The data for decoding XOR_data is information which is used for a decoding process in the decoding circuit 12b, and is specifically information which is a target for the arithmetic operation of an exclusive logical sum (XOR) together with the storage device readout data Storage_RD_data in the logical arithmetic operation element 121b.

An arithmetic operation result of the exclusive logical sum of the storage device readout data Storage_RD_data and the data for decoding XOR_data by the logical arithmetic operation element 121b is input to the input port [2] of the multiplexer 120b.

Readout data RD_data is output from an output port [4] of the multiplexer 120b. The readout data RD_data is information which is actually read out (loaded) into the main memory 101. In a case where the control signal RD_mux which is input to the selection port [3] of the multiplexer 120b is "L," the readout data RD_data becomes the storage device readout data Storage_RD_data itself. That is, in a case where the control signal RD_mux is "L," the decoding process of the decoding circuit 12b is disabled. On

the other hand, in a case where the control signal RD_mux which is input to the selection port [3] of the multiplexer 120b is “H,” the readout data RD_data becomes an arithmetic operation result of the exclusive logical sum by the logical arithmetic operation element 121b. That is, in a case where the control signal RD_mux is “H,” the decoding process
 5 of the decoding circuit 12b is enabled.

[0029]

In Fig. 3, address information Address is information which is transmitted from the main memory-side device 10 through the address bus to the external storage device 11, and is information for designating a storage place (an address) of data to be written in
 10 and read out from the external storage device 11.

A writing control signal WR# is information which is transmitted from the main memory-side device 10 through the control bus to the external storage device 11, and is a signal for giving an instruction for writing the storage device writing data Storage_WR_data in a storage place which is designated in the address information
 15 Address of the external storage device 11.

A readout control signal RD# is information which is transmitted from the main memory-side device 10 through a control bus to the external storage device 11, and is a signal for giving an instruction for reading out the storage device readout data Storage_RD_data stored in a storage place which is designated in the address information
 20 Address of the external storage device 11.

[0030]

Next, various types of information which are output from the main memory-side device 10 to the random number recording memory 13 will be described.

Random number recording memory address information Data_address is
 25 information for designating a storage place for storage of random numbers (random

numbers Random_data) generated by the CPU 100 (the random number generation unit 1003).

The random numbers Random_data are random numbers generated by the CPU 100 (the random number generation unit 1003).

5 A random number recording memory writing control signal WR#_random is a signal for giving an instruction for writing the random numbers Random_data in a storage place which is designated in the random number recording memory address information Data_address of the random number recording memory 13.

[0031]

10 (First process flow of information processing device)

Fig. 4 is a diagram showing a first process flow of the information processing device according to the first embodiment.

In addition, Fig. 5 is a diagram showing operations relating to the first process flow of the information processing device according to the first embodiment in detail.

15 [0032]

The first process flow shown in Fig. 4 shows a flow of processes for recording random numbers (data for encoding and data for decoding) in the random number recording memory 13 in advance during a normal operation in order to enable high-speed startup after power-off.

20 [0033]

As shown in Fig. 4, the random number generation unit 1003 of the CPU 100 generates the random number Random_data during a normal operation of the information processing device 1 (step S01).

Next, the random number generation unit 1003 records the generated random
25 number Random_data in a designated address of the random number recording memory

13 (step S02).

For example, as shown in Fig. 5, the random number generation unit 1003 outputs random number recording memory address information Data_address “A0000” and a random number Random_data “X0001.” The random number generation unit 1003 transitions the random number recording memory writing control signal WR#_random from “H” to “L,” so that the random number “X0001” is written in the address “A0000” of the random number recording memory 13.

The random number generation unit 1003 writes another random number Random_data (for example, “X0010”) generated similarly with respect to another address (for example, “A0001”) of the random number recording memory 13.

The random number Random_data recorded in the random number recording memory 13 in this manner is read out from the random number recording memory 13, as the data for encoding XOR_data and the data for decoding XOR_data, during writing and reading out of a snapshot image of the main memory 101.

15 [0034]

(Second process flow of information processing device)

Fig. 6 is a diagram showing a second process flow of the information processing device according to the first embodiment.

In addition, Figs. 7 and 8 are diagrams showing operations relating to the second process flow of the information processing device according to the first embodiment in detail.

[0035]

The second process flow shown in Fig. 6 shows a flow of a series of processes of the information processing device 1 until the power is turned on and the power is turned off again.

[0036]

First, the information processing device 1 in a state of power-off is powered on by a user's operation or the like (step S11).

When the power is turned on, the CPU 100 accesses a predetermined storage
5 area (such as a dedicated ROM or a flash memory which is not shown Fig. 1), and reads out a program for startup for operating a boot loader (step S12).

The readout processing unit 1002 of the CPU 100 that operates as a boot loader sets the control signal RD_mux which is input to the multiplexer 120b of the decoding circuit 12b to be in a "H" state (step S13).

10 Next, the readout processing unit 1002 reads out a snapshot image of the main memory 101 from the external storage device 11 (step S14). The snapshot image is information indicating the storage state of data in all the storage areas (or a part of storage areas) of the main memory 101 immediately before the information processing device 1 is powered off. As will be described later, the snapshot image is written in a
15 specified storage area of the external storage device 11 by the CPU 100 (the readout processing unit 1002) immediately before the information processing device 1 is powered off.

[0037]

The process of step S14 described above will be described in detail with
20 reference to Fig. 7.

[0038]

A snapshot image readout process which is performed by the readout processing unit 1002 in step S14 of Fig. 6 is as shown in a period B1 of Fig. 7.

That is, the readout processing unit 1002 outputs address information Address
25 indicating an address in which a snapshot image is written (for example, an address

corresponding to “A1000”) to the external storage device 11 in a state where the control signal RD_mux of the multiplexer 120b is maintained to be “H.” Meanwhile, an address of the external storage device 11 in which the snapshot image of the main memory 101 is written is set in advance. In addition, an address of the external storage device 11 to be designated in order to read out a snapshot image is described in advance in the program for startup (the boot loader).

Here, as shown in the period B1 of Fig. 7, storage device readout data Storage_RD_data (a snapshot image) “D1010” is written in the address corresponding to “A1000” of the external storage device 11. In addition, data for decoding XOR_data “X0010” is written in the address corresponding to “A1000” of the random number recording memory 13 (the address corresponding to the address “A1000” of the external storage device 11). In this case, when the readout processing unit 1002 transitions the readout control signal RD# from “H” to “L,” the storage device readout data Storage_RD_data “D1010” is output from the external storage device 11, the data for decoding XOR_data “X0010” is output from the random number recording memory 13. As a result, the logical arithmetic operation element 121b of the decoding circuit 12b arithmetically operates an exclusive logical sum of the information at once, and outputs its result. As shown in the period B1 of Fig. 7, since the control signal RD_mux which is input to the multiplexer 120b is “H,” the readout data RD_data which is output from the multiplexer 120b becomes an exclusive logical sum (D1000) of the storage device readout data Storage_RD_data (D1010) and the data for decoding XOR_data (X0010). That is, a snapshot image (D1000) in which decoding has been performed on an encoded snapshot image (D1010) by the decoding circuit 12b is input to the main memory-side device 10.

Referring back to Fig. 6, the readout processing unit 1002 reads out a snapshot image into the main memory 101, and completes high-speed startup by restoring a state immediately before the power is turned off. When the high-speed startup is completed, the CPU 100 can perform a normal operation based on an OS and an application program.

- 5 In a step in which the normal operation based on an OS and an application program can be performed, the CPU 100 sets both the control signal WR_mux and the control signal RD_mux to be “L” (step S15).

- When step S15 is completed, the CPU 100 reads out and writes normal data in the external storage device 11 on the basis of an OS and an application program in order to exhibit an original function as the information processing device 1 (step S16).

[0040]

The process of step S16 described above will be described in detail with reference to Figs. 7 and 8.

[0041]

- 15 A process for reading out normal data which is performed by the readout processing unit 1002 in step S16 of Fig. 6 is as shown in a period A1 of Fig. 7.

- That is, the readout processing unit 1002 outputs address information Address indicating an address in which normal data is written (for example, an address “A0000”) to the external storage device 11 in a state where the control signal RD_mux of the multiplexer 120b is maintained to be “L.”

- Here, as shown in the period A1 of Fig. 7, storage device readout data Storage_RD_data (normal data) “D0000” is written in the address “A0000” of the external storage device 11. In addition, data for decoding XOR_data “X0001” is written in the address “A0000” of the random number recording memory 13 (the address corresponding to the address “A0000” of the external storage device 11). In this case,

- 25

when the readout processing unit 1002 transitions the readout control signal RD# from “H” to “L,” the storage device readout data Storage_RD_data “D0000” is output from the external storage device 11, and the data for decoding XOR_data “X0001” is output from the random number recording memory 13. In this case, the logical arithmetic operation element 121b of the decoding circuit 12b arithmetically operates an exclusive logical sum of the information at once, and outputs its result. However, since the control signal RD_mux which is input to the multiplexer 120b in the period A1 is “L,” the readout data RD_data which is output from the multiplexer 120b becomes the storage device readout data Storage_RD_data (D0000) itself which is output without going through the logical arithmetic operation element 121b. That is, in this case, the normal data (D0000) itself which is output from the external storage device 11 is input to the main memory-side device 10.

[0042]

On the other hand, a process for writing normal data which is performed by the writing processing unit 1001 in step S16 of Fig. 6 is as shown in a period A2 of Fig. 8.

That is, the writing processing unit 1001 outputs address information Address indicating an address in which normal data is to be written (for example, an address “A0000”) to the external storage device 11 in a state where the control signal WR_mux of the multiplexer 120a is maintained to be “L.”

Here, as shown in the period A2 of Fig. 8, writing data WR_data (normal data) “D0000” which is output from the main memory-side device 10 is to be written in the address “A0000” of the external storage device 11. In addition, data for encoding XOR_data “X0001” is written in the address “A0000” of the random number recording memory 13 (the address corresponding to the address “A0000” of the external storage device 11). In this case, when the writing processing unit 1001 transitions the writing

control signal WR# from “H” to “L,” the writing data WR_data “D0000” is output from the main memory-side device 10, and the data for encoding XOR_data “X0001” is output from the random number recording memory 13. In this case, the logical arithmetic operation element 121a of the encoding circuit 12a arithmetically operates an exclusive
 5 logical sum of the information at once, and outputs its result. However, since the control signal WR_mux which is input to the multiplexer 120a in the period A2 is “L,” the storage device writing data Storage_WR_data which is output from the multiplexer 120a becomes the writing data WR_data (D0000) itself which is output without going through the logical arithmetic operation element 121a. That is, the normal data (D0000)
 10 itself which is output from the main memory-side device 10 is input to the external storage device 11.

[0043]

In this manner, the CPU 100 of which startup is completed sets both the control signal WR_mux and the control signal RD_mux to be “L” in step S15, and thus can write
 15 and read out normal data without an encoding process and a decoding process between the external storage device 11 and the CPU in the normal process of step S16.

[0044]

The CPU 100 determines whether a power-off instruction (such as, for example, a user’s pressing of a power OFF button) has been input to the information processing
 20 device 1 (step S17). In a case where the power-off instruction is not input (step S17: NO), the CPU 100 reads out and writes normal data from and in the external storage device 11 in a normal process as the information processing device 1. On the other hand, in a case where the power-off instruction is input (step S17: YES), the CPU 100 performs a process for writing and saving the snapshot image of the main memory 101 in
 25 the external storage device 11, as follows, before the power is actually turned off.

[0045]

Specifically, the writing processing unit 1001 first sets the control signal WR_mux which is input to the multiplexer 120a of the encoding circuit 12a to be “H” (step S18).

- 5 The writing processing unit 1001 then writes the snapshot image of the main memory 101 in the external storage device 11 (step S19).

When writing the snapshot image is completed, the CPU 100 turns the power off (step S20).

[0046]

- 10 The process of step S19 described above will be described in detail with reference to Fig. 8.

[0047]

A process for reading out a snapshot image which is performed by the writing processing unit 1001 in step S19 of Fig. 6 is as shown in a period B2 of Fig. 8.

- 15 That is, the writing processing unit 1001 outputs address information Address indicating an address in which a snapshot image is to be written (for example, an address “A1000”) to the external storage device 11 in a state where the control signal WR_mux of the multiplexer 120a is maintained to be “H.” Meanwhile, as described above, an address of the external storage device 11 in which the snapshot image of the main
20 memory 101 is written is set in advance.

Here, as shown in the period B2 of Fig. 8, writing data WR_data (snapshot image) “D1000” is to be written in the address “A1000” of the external storage device 11.

In addition, data for encoding XOR_data “X0010” is written in the address “A1000” of the random number recording memory 13 (the address corresponding to the address

- 25 “A1000” of the external storage device 11). In this case, when the writing processing

unit 1001 transitions the writing control signal WR# from “H” to “L,” the writing data WR_data “D1000” is output from the main memory-side device 10, and the data for encoding XOR_data “X0010” is output from the random number recording memory 13. As a result, the logical arithmetic operation element 121a of the encoding circuit 12a

5 arithmetically operates an exclusive logical sum of the information at once, and outputs its result. As shown in the period B2 of Fig. 8, since the control signal WR_mux which is input to the multiplexer 120a is “H,” the storage device writing data Storage_WR_data which is output from the multiplexer 120a becomes an exclusive logical sum (D1010) of the writing data WR_data (D1000) and the data for encoding XOR_data (X0010). That

10 is, a snapshot image (D1010) in which encoding has been performed on a plaintext (non-encoded) snapshot image (D1000) by the encoding circuit 12a is input to the external storage device 11.

[0048]

(Operation and Effect)

15 As described above, the information processing device 1 according to the first embodiment is provided on the data bus DB for connecting the main memory 101 and the external storage device 11, and includes the decoding circuit 12b capable of switching between enabling and disabling a process for decoding information which is transmitted through the data bus DB and the readout processing unit 1002 (the CPU 100) that reads

20 out information written in the external storage device 11 into the main memory 101. In a case where a snapshot image of the main memory 101 is read out as the information written in the external storage device 11, the readout processing unit 1002 enables the decoding process of the decoding circuit 12b.

In this manner, when the snapshot image is read out into the main memory 101

25 immediately after power-on, the encoded snapshot image is decoded at a high speed by

the decoding circuit 12b configured as hardware in a process in which the snapshot image is transmitted on the data bus DB from the external storage device 11 toward the main memory-side device 10.

In addition, when normal data is read out from the external storage device 11
5 after an OS and an application program are started up, the decoding process of the decoding circuit 12b is disabled, and then the normal data is transmitted on the data bus DB from the external storage device 11 toward the main memory-side device 10.

However, according to the information processing device 1 of the first embodiment, since the encoded snapshot image can be read out without decreasing the
10 effect of high-speed startup, it is possible to enable high-speed startup, and to enhance security performance.

[0049]

In addition, the information processing device 1 according to the first embodiment is provided on the data bus DB, and includes the encoding circuit 12a
15 capable of switching between enabling and disabling a process for encoding information which is transmitted through the data bus DB and the writing processing unit 1001 (the CPU 100) that writes information stored in the main memory 101 in the external storage device 11. In a case where a snapshot image of the main memory 101 is written as the information stored in the main memory 101, the writing processing unit 1001 enables the
20 encoding process of the encoding circuit 12a.

In this manner, when the information processing device 1 writes a snapshot image in the external storage device 11 immediately before power-off, a plaintext snapshot image is encoded at a high speed by the encoding circuit 12a configured as hardware in a process in which the snapshot image is transmitted on the data bus DB
25 from the main memory-side device 10 toward the external storage device 11.

In addition, when normal data is written in the external storage device 11 after an OS and an application program are started up, the encoding process by the encoding circuit 12a is disabled, and then the normal data is transmitted on the data bus DB from the main memory-side device 10 toward the external storage device 11.

5 Therefore, according to the information processing device 1 of the first embodiment, it is possible to speed up encoding of a snapshot image to be written in the external storage device 11 during power-off.

[0050]

 In addition, the decoding circuit 12b is configured to include the logical
10 arithmetic operation element 121b for performing a decoding process and the multiplexer 120b (a selection element) capable of selecting whether information which is transmitted through the data bus DB passes through the logical arithmetic operation element 121b in accordance with the control signal RD_mux which is input.

 In this manner, it is possible to realize the decoding circuit 12b capable of
15 switching between enabling and disabling a decoding process, as hardware, with an extremely simple configuration.

 Similarly, the encoding circuit 12a is configured to include the logical arithmetic operation element 121a for performing an encoding process and the multiplexer 120a (a selection element) capable of selecting whether information which is transmitted through
20 the data bus DB passes through the logical arithmetic operation element 121a in accordance with the control signal WR_mux which is input.

 In this manner, it is possible to realize the encoding circuit 12a capable of switching between enabling and disabling an encoding process, as hardware, with an extremely simple configuration.

25 [0051]

In addition, the information processing device 1 according to the first embodiment further includes the random number recording memory 13 (a data recording memory for decoding) in which the data for decoding XOR_data is recorded. The decoding circuit 12b performs a process for decoding information which is transmitted through the data bus DB on the basis of the data for decoding XOR_data which is read out from the random number recording memory 13.

In this manner, the decoding circuit 12b can perform decoding at a high speed using the data for decoding XOR_data which is read out directly from a dedicated memory (the random number recording memory 13).

10 In addition, the information processing device 1 according to the first embodiment further includes the random number recording memory 13 (a data recording memory for encoding) in which the data for encoding XOR_data is recorded. The encoding circuit 12a performs a process for encoding information which is transmitted through the data bus DB on the basis of the data for encoding XOR_data which is read out from the random number recording memory 13. In addition, in the present embodiment, the data for encoding XOR_data is the same as the data for decoding XOR_data.

In this manner, the encoding circuit 12a can perform encoding at a high speed using the data for encoding XOR_data which is read out directly from a dedicated memory (the random number recording memory 13).

[0052]

Meanwhile, the information processing device 1 according to the first embodiment may further have the following features.

That is, the CPU 100 of the information processing device 1 first reading out a program for startup for operating a boot loader immediately after power-on (step S11

shown in Fig. 9) (step S12) has been described. However, in a step in which a register or the like of the CPU 100 is not initialized immediately after power-on, the control signal RD_mux may be output as being “H.” In this case, it is assumed that the program for startup (a boot loader) is read out into the main memory 101 after the
5 decoding process of the decoding circuit 12b is performed through the decoding circuit 12b provided on the data bus DB. In this case, it is considered that the program for startup is destroyed by an unintended decoding process (a conversion process), and is not normally started up.

Consequently, an aspect may be used in which a storage area having a program
10 for startup for operating as a boot loader loaded therein (hereinafter denoted as a “storage area for a boot loader”) is prepared separately from the main memory 101, and a separate data bus DB which is not provided with the decoding circuit 12b is connected to the storage area for boot loader. Thereby, the program for startup is stored in the storage area for a boot loader, as it is, through the data bus DB which is not provided with the
15 decoding circuit 12b.

In addition, in another embodiment, an aspect may be used in which an address on the main memory 101 having a program for startup for operating as a boot loader stored therein is specified in advance, and a separate dedicated circuit (an address decoder) that inputs the address information Address is provided. In this case, the
20 dedicated circuit forcibly sets the control signal RD_mux which is input to the multiplexer 120b to be “L” in a case where it is detected that the address information Address which is input through the address bus is the address specified in advance. In this manner, in a case where the program for startup is loaded into the main memory 101, the control signal RD_mux is always guaranteed to be “L,” and thus the program is
25 stored in the main memory 101 as it is.

[0053]

Hereinbefore, the information processing device 1 according to the first embodiment has been described in detail, but the specific aspects of the information processing device 1 are not limited to those described above, and various design changes and the like can be made without departing from the scope of this invention.

[0054]

For example, the encoding circuit 12a and the decoding circuit 12b have been described in an aspect in which the logical arithmetic operation elements 121a and 121b that arithmetically operate an exclusive logical sum are included, but another embodiment is not limited to this aspect.

That is, in a case where an encoding circuit 12a and a decoding circuit 12b according to another embodiment are configured, as hardware, on the data bus DB, and are configured to be capable of realizing an encoding process and a decoding process which are used as an objective, these circuits may be constituted by a logical arithmetic operation element that performs arithmetic operations other than the exclusive logical sum or a combination of multiple types of logical arithmetic operation elements.

[0055]

In addition, an aspect may be used in which an information processing device 1 in another embodiment does not include the encoding circuit 12a configured as hardware.

That is, an aspect may be used in which, when a snapshot image of the main memory 101 is written in the external storage device 11, the information processing device 1 according to another embodiment performs encoding through the process of the CPU 100 (software process) immediately before power-off, and writes the encoded snapshot image in the external storage device 11.

[0056]

<Second embodiment>

Next, an information processing device according to a second embodiment will be described in detail with reference to Figs. 9 and 10.

[0057]

5 (Functional configuration of CPU)

Fig. 9 is a diagram showing a functional configuration of a CPU according to the second embodiment.

Meanwhile, the hardware configuration of an information processing device 1 according to the second embodiment is the same as that in the first embodiment (Fig. 1),
10 and thus is not shown in the drawing.

[0058]

As shown in Fig. 9, a CPU 100 according to the second embodiment exhibits the function of a PUF information recording processing unit 1003a.

The PUF information recording processing unit 1003a acquires physical
15 unclonable function (PUF) information of the main memory 101, and performs a process for recording the PUF information in the random number recording memory 13. Here, the term “PUF information” refers to information recorded in the main memory 101 in an initial state (a state before initialization is performed) immediately after power-on, and to information which is generated on the basis of a slight individual difference in the
20 electrical characteristics of a transistor or the like constituting the main memory 101. Therefore, the PUF information is information which is different for each main memory 101.

[0059]

(Second process flow of information processing device)

25 Fig. 10 is a diagram showing a second process flow of the information

processing device according to the second embodiment.

The second process flow of the information processing device 1 according to the second embodiment is different from that in the first embodiment in that step S13a is included.

5 That is, the PUF information recording processing unit 1003a of the CPU 100 (Fig. 9) reads out the PUF information from the main memory 101 immediately after power-on (step S11) before a snapshot image is read out into the main memory 101 (step S14). The PUF information recording processing unit 1003a records the read-out PUF information in the random number recording memory 13 (step S13a).

10 [0060]

 The PUF information of the main memory 101 is recorded in the random number recording memory 13 through the process of step S13a which is performed by the PUF information recording processing unit 1003a. Subsequently, as is the case with the first embodiment, the readout processing unit 1002 performs a process for reading out
15 a snapshot image written in the external storage device 11 into the main memory 101 (step S14). Here, the PUF information (the data for decoding XOR_data) recorded in the random number recording memory 13 in step S13a is input to the logical arithmetic operation element 121b of the decoding circuit 12b. Thereby, the snapshot image decoded on the basis of the PUF information is read out into the main memory 101.

20 [0061]

 In addition, in a case where a power-off instruction is accepted (step S17), as is the case with the first embodiment, the writing processing unit 1001 performs a process for writing a snapshot image of the main memory 101 in the external storage device 11 (step S19). Here, the PUF information (the data for encoding XOR_data) recorded in
25 the random number recording memory 13 in step S13a is input to the logical arithmetic

operation element 121a of the encoding circuit 12a. Thereby, the encoded snapshot image on the basis of the PUF information is written in the external storage device 11.

[0062]

(Operation and Effect)

5 As described above, according to the information processing device 1 of the second embodiment, the data for decoding and the data for encoding become the PUF information recorded in the main memory 101 in an initial state immediately after the information processing device 1 is powered on.

In this manner, it is possible to achieve encoding of a snapshot image on the basis of the information (PUF information) recorded in the main memory from the initial state. Thereby, it is possible to further enhance security performance of the information processing device 1.

[0063]

Meanwhile, in second embodiment, since the PUF information is read out from the main memory 101 immediately after power-on, it is not necessary to hold the PUF information as data for decoding while the information processing device 1 is powered off. Therefore, in the second embodiment, the random number recording memory 13 needs not to be a non-volatile memory.

[0064]

20 In addition, in each embodiment described above, various processes of the information processing device 1 described above are stored in a computer readable recording medium in a format of a program, and the various processes are performed by a computer reading out and executing this program. In addition, the term “computer readable recording medium” refers to a magnetic disc, a magnetooptic disc, a CD-ROM, a DVD-ROM, a semiconductor memory, or the like. In addition, such a computer

25

program may be delivered to a computer through a communication line, and the computer having received this delivery may execute the program.

[0065]

The program may be a program for realizing some of the above-described
5 functions. Further, the program may be a so-called differential file (a differential program) that makes it possible to realize the above-described functions in combination with programs already recorded in a computer system.

In addition, the information processing device 1 may be constituted by one computer having all of the various functions described above, or may be constituted by a
10 plurality of computers that have some of the functions and are communicably connected to each other.

[0066]

Hereinbefore, while certain embodiments of the present invention have been described, these embodiments have been presented by way of example only, and are not
15 intended to limit the scope of the invention. Indeed, these embodiments described herein may be embodied in a variety of other forms, and furthermore, various omissions, substitutions and changes in the form of the embodiments described herein may be made without departing from the spirit of the present invention. The appended claims and their equivalents are intended to cover such forms or modifications as would fall within
20 the scope and spirit of the present invention.

[Industrial Applicability]

[0067]

According to the information processing device, the method for controlling an information processing device, and the program, it is possible to enable high-speed
25 startup and to enhance security performance.

[Reference Signs List]

[0068]

	1	Information processing device
	10	Main memory-side device
5	100	CPU
	1001	Writing processing unit
	1002	Readout processing unit
	1003	Random number generation unit
	1003a	PUF information recording processing unit
10	101	Main memory
	11	External storage device
	12a	Encoding circuit
	12b	Decoding circuit
	120a, 120b	Multiplexer
15	121a, 121b	Logical arithmetic operation element
	13	Random number recording memory
	DB	Data bus

[CLAIMS]

[Claim 1]

An information processing device comprising:

a decoding circuit, provided on a data bus for connecting a main memory and an
5 external storage device, which is capable of switching between enabling and disabling a
process for decoding information that is transmitted through the data bus; and

a readout processing unit that is configured to read out information written in the
external storage device into the main memory,

wherein the readout processing unit is configured to enable the decoding process
10 of the decoding circuit in a case where a snapshot image of the main memory is read out
as the information written in the external storage device.

[Claim 2]

The information processing device according to claim 1, further comprising:

an encoding circuit, provided on the data bus, which is capable of switching
15 between enabling and disabling a process for encoding the information that is transmitted
through the data bus; and

a writing processing unit that writes information stored in the main memory in
the external storage device,

wherein the writing processing unit is configured to enable the encoding process
20 of the encoding circuit in a case where a snapshot image of the main memory is written
as the information stored in the main memory.

[Claim 3]

The information processing device according to claim 1 or 2, wherein the
decoding circuit includes

25 a logical arithmetic operation element that is configured to perform the decoding

process, and

a selection element capable of selecting whether the information that is transmitted through the data bus passes through the logical arithmetic operation element in accordance with a control signal that is input.

5 [Claim 4]

The information processing device according to any one of claims 1 to 3, further comprising a data recording memory for decoding in which data for decoding is recorded,

wherein the decoding circuit performs the process for decoding the information
10 that is transmitted through the data bus on the basis of the data for decoding read out from the data recording memory for decoding.

[Claim 5]

The information processing device according to claim 4, wherein the data for decoding is information recorded in the main memory in an initial state immediately after
15 power-on.

[Claim 6]

A method for controlling an information processing device including a decoding circuit, provided on a data bus for connecting a main memory and an external storage device, which is capable of switching between enabling and disabling a process for
20 decoding information that is transmitted through the data bus,

wherein the method comprises a readout step of reading out information written in the external storage device into the main memory, and

the decoding process of the decoding circuit is enabled in the readout step in a case where a snapshot image of the main memory is read out as the information written
25 in the external storage device.

[Claim 7]

A program causing an information processing device including a decoding circuit that is provided on a data bus for connecting a main memory and an external storage device and is capable of switching between enabling and disabling a process for
5 decoding information transmitted through the data bus to function as a readout processing unit that is configured to read out information written in the external storage device into the main memory,

wherein the readout processing unit is configured to enable the decoding process of the decoding circuit in a case where a snapshot image of the main memory is read out
10 as the information written in the external storage device.