SEMICONDUCTOR INTEGRATED CIRCUIT AND INFORMATION PROCESSING APPARATUS

CROSS REFERENCES TO RELATED APPLICATIONS

The present invention contains subject matter related to Japanese Patent Application JP 2004-201075 filed in the Japanese Patent Office on July 7, 2004, the entire contents of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a semiconductor integrated circuit and an information processing apparatus and more specifically relates to a reader-writer apparatus capable of performing data communication with a noncontact integrated circuit (IC) card without any contact and a semiconductor integrated circuit included in the reader-writer apparatus.

2. Description of the Related Art

Noncontact IC card systems using noncontact IC cards have been commonly used recently in automatic ticket gates at train stations, security systems and electronic money systems.

In such a noncontact IC card system, for example, if a user holds a noncontact IC card against a reader-writer

apparatus, data communication begins between the noncontact IC card and the reader-writer apparatus.

More specifically, in such a case, the reader-writer apparatus emits electromagnetic waves to the noncontact IC card via an antenna unit. The noncontact IC card rectifies the voltage induced in the antenna unit in the noncontact IC card in response to the electromagnetic waves and uses this as a driving power to operate without a battery.

Such a reader-writer apparatus includes an antenna unit configured to perform data communication with a noncontact IC card and a semiconductor integrated circuit connected with the antenna unit. The semiconductor integrated circuit executes programs of various processing for performing data communication with a noncontact IC card accordingly. The programs are stored in an internal memory included in the semiconductor integrated circuit. The internal memory in the semiconductor integrated circuit also stores other various programs and data items (refer to Japanese Patent Unexamined Patent Application Publication No. 11-25003 illustrated in Fig. 2).

SUMMARY OF THE INVENTION

Recently, the amount of data handled by semiconductor integrated circuits has been increasing. Therefore, structures for storing data not only in an internal memory

in a semiconductor integrated circuit but also in an external memory disposed outside the semiconductor integrated circuit have been proposed.

However, if data processed by the semiconductor integrated circuit is directly stored in an external memory, the data can be easily exposed compared to data stored inside the semiconductor integrated circuit. Therefore, data could not be stored very security in an external memory.

A semiconductor integrated circuit and an information processing apparatus according to an embodiment of the present invention are capable of storing data security in an external memory.

According to embodiments of the present invention, a semiconductor integrated circuit includes encrypting means for generating encrypted data by encrypting the data to be stored in an external memory disposed outside the semiconductor integrated circuit, write means for writing in the encrypted data in the external memory, reading means for reading out the encrypted data from the external memory, and decrypting means for decrypting the readout encrypted data.

An information processing apparatus according to an embodiment of the present invention includes a semiconductor integrated circuit and an external memory disposed outside the semiconductor integrated circuit. The semiconductor integrated circuit includes encrypting means for generating

encrypted data by encrypting the data to be stored in an external memory disposed outside the semiconductor integrated circuit, write means for writing in the encrypted data in the external memory, readout means for reading out the encrypted data from the external memory, and decrypting means for decrypting the readout encrypted data.

Accordingly, by encrypting the data to be stored in the external memory, the data can be safely stored in the external memory.

In the semiconductor integrated circuit according an embodiment of the present invention, the encrypting means generates the encrypted data by performing encryption in accordance with the storage location of the data to be stored in the external memory, and the decrypting means decrypts the readout encrypted data in accordance with the storage location of the encrypted data.

In the information processing apparatus according to an embodiment of the present invention, the encrypting means generates the encrypted data by performing encryption in accordance with the storage location of the data to be stored in the external memory, and the decrypting means decrypts the readout encrypted data in accordance with the storage location of the encrypted data.

According to an embodiment of the present invention, data can be stored security in an external memory by

encrypting the data to be stored in the external memory.

The data to be stored in the external memory is encrypted in accordance with the storage location of the data. Consequently, for example, if the encrypted data is copied from the external memory onto another storage medium, it will be difficult to decrypt the encrypted data without knowing the storage location of the encrypted data in the external memory. As a result, data can be security stored in the external memory.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates a schematic view of the structure of a reader-writer apparatus according to an embodiment of the present invention;

Fig. 2 illustrates a schematic view of the structure of an external interface unit (1);

Fig. 3 illustrates a timing chart; and

Fig. 4 illustrates a schematic view of the structure of an external interface unit (2).

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Embodiments of the present invention will now be described in detail with reference to the drawings.

(1) Structure of Reader-writer Apparatus

Fig. 1 illustrates the overall view of a reader-writer

apparatus 1 including an antenna unit 2 for performing data communication with an external noncontact IC card without contacting the noncontact IC card, a semiconductor integrated circuit 3 connected with the antenna unit 2, and an external memory 4 disposed outside the semiconductor integrated circuit 3. The external memory 4, for example, may be a nonvolatile memory, such as a flash memory.

In the semiconductor integrated circuit 3, a central processing unit (CPU) 5 controlling the entire semiconductor integrated circuit 3 is connected to an internal memory 7, which includes a read only memory (ROM), a random access memory (RAM), and an electrically erasable programmable read only memory (EEPROM), an encryption circuit 8 configured to carry out various encryption processes, as described below, an external memory interface unit 9 configured to control reading and writing of data in the external memory 4, a modulation unit 10, and a demodulation unit 11 via a bus 6.

The modulation unit 10 and the demodulation unit 11 are connected to the antenna unit 2 via a transmission unit 12 and a reception unit 13, respectively. For example, the modulation unit 10 modulates data to be sent to an external noncontact IC card under the control of the CPU 5 and supplies the signal obtained as a result to the transmission unit 12. At this time, the transmission unit 12 sends out the signal supplied from the modulation unit 10 to the

outside via the antenna unit 2. The reception unit 13, for example, digitizes the signal received from the external noncontact IC card via the antenna unit 2 and supplies the digitized signal to the demodulation unit 11. At this time, the demodulation unit 11 demodulates the signal supplied from the reception unit 13 and sends the data obtained as a result to the CPU 5.

The semiconductor integrated circuit 3 according to an embodiment of the present invention has four modes for reading out data from and writing data in the external memory 4 disposed outside the semiconductor integrated circuit 3. The processes of writing in data and reading out data from the external memory 4 are performed by the CPU 5 of the semiconductor integrated circuit 3 in one of the four modes set in advance by the user. The four modes will be described below.

In a first mode, the CPU 5 of the semiconductor integrated circuit 3 supplies data to be stored in the external memory 4 to the external memory interface unit 9 and, at the same time, supplies address information indicating a storage location of the data in the external memory interface unit 9. At this time, the external memory interface unit 9 writes the supplied data in a storage location corresponding to the supplied address information in the storage area of the external memory 4.

When reading out such stored data from the external memory 4, the CPU 5 supplies address information indicating the storage location of the data to the external memory interface unit 9. At this time, the external memory interface unit 9 reads out the data stored at a storage location corresponding to the supplied address information in the storage area in the external memory 4 and supplies the readout data to the CPU 5.

In a second mode, the CPU 5 of the semiconductor integrated circuit 3 supplies data to be stored in the external memory 4 and address information indicating the storage location of the data to the encryption circuit 8 before supplying these to the external memory interface unit 9.

At this time, the encryption circuit 8 calculates the exclusive-OR for the supplied data and the supplied address information and supplies the data obtained as a result as encrypted data to the CPU 5. The CPU 5 then supplies the encrypted data sent from the encryption circuit 8 and the address information corresponding to the encrypted data to the external memory interface unit 9.

At this time, the external memory interface unit 9 writes in the encrypted data in a storage area in the external memory 4 corresponding to the storage location indicated by the supplied address information.

In this way, the address information indicating the storage location in the external memory 4 and the data encrypted by calculating the exclusive-OR are stored in the external memory 4.

To read out such encrypted data from the external memory 4, the CPU 5 supplies the address information indicating the storage location of the stored encrypted data to the external memory interface unit 9. At this time, the external memory interface unit 9 reads out the encrypted data stored at a storage location corresponding to the supplied address information in the storage area in the external memory 4. Subsequently, the external memory interface unit 9 calculates the exclusive-OR for the address information supplied from the CPU 5 and the readout encrypted data so as to decrypt the data and supplies the decrypted data to the CPU 5.

In a third mode, the CPU 5 of the semiconductor integrated circuit 3 supplies data to be stored in the external memory 4 and address information indicating the storage location of the data to the encryption circuit 8 before supplying these to the external memory interface unit 9.

At this time, the encryption circuit 8 calculates the exclusive-OR for the supplied data and the higher-order bits of the supplied address information and then performs data

encryption standard (DES) encryption on the data obtained as a result of the calculation. The encryption circuit 8 according to this embodiment, for example, uses the higher 21 bits of the 24-bit address information as higher-order bits used for calculating the exclusive-OR.

Subsequently, the encryption circuit 8 supplies the data obtained from performing DES encryption to the CPU 5 as encrypted data. In response, the CPU 5 supplies the encrypted data supplied from the encryption circuit 8 and the corresponding address information to the external memory interface unit 9.

At this time, the external memory interface unit 9 writes in the encrypted data in a storage area in the external memory 4 corresponding to the storage location indicated by the supplied address information.

In this way, the address information indicating the storage location in the external memory 4 and the DES encrypted data encrypted by calculating the exclusive-OR are stored in the external memory 4.

When reading out encrypted data from the external memory 4, the CPU 5 supplies address information indicating the storage location of the encrypted data to the external memory interface unit 9. At this time, the external memory interface unit 9 reads out the encrypted data from a storage area in the external memory 4 corresponding to the storage

location indicated by the supplied address information. Subsequently, the external memory interface unit 9 performs DES decryption on the readout encrypted data and decrypts the data by calculating the exclusive-OR for the resulting data and the higher-order bits of the address information. Then, the decrypted data is supplied to the CPU 5.

In a fourth mode, the CPU 5 of the semiconductor integrated circuit 3 supplies data to be stored in the external memory 4 and address information indicating the storage location of the data to the encryption circuit 8 before supplying these to the external memory interface unit 9.

At this time, the encryption circuit 8 calculates the exclusive-OR for the supplied data and the higher-order bits of the supplied address information and then performs triple DES encryption on the resulting data. In this case also, the encryption circuit 8, for example, uses the higher 21 bits of the 24-bit address information as higher-order bits used for calculating the exclusive-OR.

Subsequently, the encryption circuit 8 supplies the data obtained from performing triple DES encryption to the CPU 5 as encrypted data. In response, the CPU 5 supplies the encrypted data supplied from the encryption circuit 8 and the corresponding address information to the external memory interface unit 9.

At this time, the external memory interface unit 9 writes in the encrypted data in a storage area in the external memory 4 corresponding to the storage location indicated by the supplied address information.

In this way, the address information indicating the storage location in the external memory 4 and the triple DES encrypted data encrypted by calculating the exclusive-OR are stored in the external memory 4.

When reading out encrypted data from the external memory 4, the CPU 5 supplies address information indicating the storage location of the encrypted data to the external memory interface unit 9. At this time, the external memory interface unit 9 reads out the encrypted data from a storage area in the external memory 4 corresponding to the storage location indicated by the supplied address information. Subsequently, the external memory interface unit 9 performs triple DES decryption on the readout encrypted data and decrypts the data by calculating the exclusive-OR for the resulting data and the higher-order bits of the address information. Then, the decrypted data is supplied to the CPU 5.

When set to one of the second to fourth modes, the semiconductor integrated circuit 3 stores the encrypted data encrypted by the encryption circuit 8 in the external memory 4. When such encrypted data stored in the external memory 4

is read out from the external memory 4, the external memory interface unit 9 performs decryption of the encrypted data.

According to this embodiment, encrypted data is stored in the external memory 4 after the data is encrypted by the encryption circuit 8. However, the present invention is not limited, and, for example, the data may be encrypted outside the semiconductor integrated circuit 3 and then the encrypted data may be stored in the external memory 4 in advance.

(2) External Memory Interface Unit

The external memory interface unit 9 will now be described in detail with reference to Fig. 2. For example, in the first mode, the CPU 5 may supply data (DATA) to be stored in the external memory 4 and address information (ADR) indicating the storage location for the data (DATA) to the external memory interface unit 9 together with a data-write command signal (WR) of a write instruction for the data.

At this time, the address information (ADR) supplied from the CPU 5 is input to an address decoder 20 included in the external memory interface unit 9. The address decoder 20 generates a chip select signal (ECS) for assigning a memory chip among a plurality of memory chips included in the external memory 4 for writing in the data based on the input address information (ADR). Then the address decoder

20 outputs this chip select signal (ECS) to the external memory 4 and an OR circuit 21. In response, the OR circuit 21 sends the data-write command signal (WR) from the CPU 5 to the external memory 4 as a data-write command signal (EWR). When the data-write command signal (EWR) is output from the OR circuit 21 in this way, a switch circuit 22 sends the data (DATA) supplied from the CPU 5 via a data bus to the external memory 4 as output data (EDATA).

In the external memory interface unit 9, the address information (ADR) supplied from the CPU 5 is separated into higher-order bits and lower-order bits. Then, the higher-order bits are directly output to the external memory 4, and the lower-order bits are output to the external memory 4 via a timing control unit 23.

As a result, in response to the data-write command signal (EWR) from the external memory interface unit 9, the external memory 4 writes in the data (EDATA) from the external memory interface unit 9 in a storage location determined by the chip select signal (ECS) and address information (EADR) from the external memory interface unit 9.

For example, in the first mode, the CPU 5 may supply address information (ADR) indicating the storage location of data to be read out from the external memory 4 to the external memory interface unit 9 together with a data-readout command signal (RD) of a readout instruction for the

data.

At this time, the address information (ADR) supplied from the CPU 5 is input to the address decoder 20 in the external memory interface unit 9. The address decoder 20 generates a chip select signal (ECS) based on the input address information (ADR) and outputs the generated chip select signal (ECS) to the external memory 4. In the external memory interface unit 9, the address information (ADR) is separated into higher-order bits and lower-order bits. Then the higher-order bits are directly output to the external memory 4 and the lower-order bits are output to the external memory 4 via the timing control unit 23.

In the external memory interface unit 9, the data-readout command signal (RD) supplied from the CPU 5 is input to the timing control unit 23. The timing control unit 23 outputs the input data-readout command signal (RD) to the external memory 4 as a data-readout command signal (ERD).

As a result, the external memory 4 reads out data from a storage location specified by the chip select signal (ECS) and address information (EADR) from the external memory interface unit 9 in response to the data-readout command signal (ERD) from the external memory interface unit 9. Then the readout data is supplied to the external memory interface unit 9.

At this time, in the external memory interface unit 9,

the data read out from the external memory 4 is input to a data processing unit 24 including a cash memory 24A and a decryption circuit 24B. In this case, since the readout data is not encrypted, the data processing unit 24 directly supplies the data to the CPU 5.

When the semiconductor integrated circuit 3 is set to the second mode, the external memory 4 stores encrypted data encrypted by calculating the exclusive-OR.

In this case, for example, the CPU 5 may supply address information (ADR) indicating a storage location of data to be readout from the external memory 4 and a data-readout command signal (RD) of a readout instruction for the data to the external memory interface unit 9.

At this time, in the external memory interface unit 9, the address information (ADR) supplied from the CPU 5 is input to the address decoder 20. The address decoder 20 generates a chip select signal (ECS) based on the input address information (ADR) and outputs the generated chip select signal (ECS) to the external memory 4. In the external memory interface unit 9, the address information (ADR) is separated into higher-order bits and lower-order bits. Then, the higher-order bits are directly output to the external memory 4 and the lower-order bits are output to the external memory 4 via the timing control unit 23.

In the external memory interface unit 9, the data-

readout command signal (RD) supplied from the CPU 5 is input to the timing control unit 23. The timing control unit 23 outputs the input data-readout command signal (RD) to the external memory 4 as a data-readout command signal (ERD).

As a result, the external memory 4 reads out encrypted data from a storage location specified by the chip select signal (ECS) and address information (EADR) from the external memory interface unit 9 in response to the data-readout command signal (ERD) from the external memory interface unit 9. Then the readout encrypted data is supplied to the external memory interface unit 9.

At this time, in the external memory interface unit 9, the data read out from the external memory 4 is input to the data processing unit 24. In this case, since the data read out from the external memory 4 is encrypted using the exclusive-OR, the decryption circuit 24B in the data processing unit 24 decrypts the encrypted data by calculating the exclusive-OR for the encrypted data and the address information (ADR) supplied from the CPU 5. Then the decryption circuit 24B supplies the decrypted data to the CPU 5.

When the semiconductor integrated circuit 3 is set to the third mode, the external memory 4 stores encrypted data encrypted using the exclusive-OR and DES encryption.

When using DES encryption, data is encrypted in 64-bit

units. Therefore, the encrypted data will be stored in the external memory 4 in 64-bit units. Accordingly, in order for the external memory interface unit 9 to read out 8 bits of data from the external memory 4 in response to the data-readout command signal (RD) from the CPU 5, the semiconductor integrated circuit 3 reads out the 8 bits of data and also the other bits of data encrypted as a unit with the 8 bits of data.

More specifically, for example, as shown in Fig. 3, the CPU 5 may start supplying address information (ADR) "000006 (hexadecimal)" indicating storage location of data to be read out from the external memory 4 at a timing T1 and then start supplying (activate) a data-readout command signal (RD) to the external memory interface unit 9 at a timing T2.

In response, the external memory interface unit 9 starts supplying (activates) a wait signal (WAIT) instructing the CPU 5 to wait until data is read out from the external memory 4 at a subsequent timing T3.

In the external memory interface unit 9, the address information (ADR) "000006 (hexadecimal)" supplied from the CPU 5 is input to the address decoder 20. The address decoder 20 generates a chip select signal (ECS) based on the input address information (ADR) and outputs the generated chip select signal (ECS) to the external memory 4. In the external memory interface unit 9, the address information

(ADR) is separated into higher-order bits and lower-order bits. Then the higher-order bits are directly output to the external memory 4 and the lower-order bits are output to the external memory 4 via the timing control unit 23.

According to an embodiment of the present invention, the address information (ADR), for example, is a 24-bit data, as described above. The higher-order bits, for example, are the higher 21 bits of the address information (ADR) and the lower-order bits, for example, are the lower 3 bits of the address information (ADR).

The timing control unit 23 moves back the value of the lower-order bits of the input address information (ADR) by a predetermined amount using an internal counter circuit and supplies this value to the external memory 4. As a result, at the timing T2, the external memory interface unit 9 outputs the value "000000 (hexadecimal)" as address information (EADR) including both the higher-order bits and the lower-order bits to the external memory 4.

In the external memory interface unit 9, the data-readout command signal (RD) supplied from the CPU 5 is input to the timing control unit 23. For example, during the period of timing T3 to T4, the timing control unit 23 outputs the input data-readout command signal (RD) as a data-readout command signal (ERD) to the external memory 4.

As a result, the external memory 4 reads out, for

example, 16 bits of encrypted data from a storage location specified by the chip select signal (ECS) and the address information (ADR) "000000 (hexadecimal)" sent from the external memory interface unit 9 during the period of timing T3 to T4 in response to the data-readout command signal (ERD) sent from the external memory interface unit 9. Then, the external memory 4 supplies the readout 16 bits of encrypted data to the external memory interface unit 9.

At this time, in the external memory interface unit 9, the 16 bits of encrypted data read out from the external memory 4 is input to the data processing unit 24. The data processing unit 24 stores the 16 bits of encrypted data in the internal cash memory 24A included in the data processing unit 24.

Subsequently, the timing control unit 23 moves back the value of the lower-order bits of the input address information (ADR) by a predetermined amount using the internal counter circuit and supplies this value to the external memory 4. As a result, for example, at a timing T5, the external memory interface unit 9 outputs a value "000002 (hexadecimal)" as address information (EADR) including both the higher-order bits and the lower-order bits to the external memory 4.

Furthermore, the timing control unit 23 outputs the data-readout command signal (RD) input from the CPU 5 as a

data-readout command signal (ERD) to the external memory 4, for example, during the period of timing T6 to T7.

As a result, in response to the data-readout command signal (ERD) from the external memory interface unit 9, the external memory 4 reads out, for example, 16 bits of encrypted data from a storage location specified by the chip select signal (ECS) and the address information (EADR) "000002 (hexadecimal)" from the external memory interface unit 9 during the period of timing T6 to T7 and supplies the 16 bits of encrypted data to the external memory interface unit 9.

At this time, in the external memory interface unit 9, the 16 bits of encrypted data read out from the external memory 4 are input to the data processing unit 24. The data processing unit 24 stores the 16 bits of encrypted data in the cash memory 24A included in the data processing unit 24. As a result, a total of 32 bits of encrypted data is stored in the cash memory 24A.

In a similar manner, the timing control unit 23 moves forward, in sequence, the values of the lower-order bits of the input address information (ADR) using the internal counter circuit and supplies the values to the external memory 4 in sequence. As a result, the external memory interface unit 9 outputs a value "000004 (hexadecimal)" and "000006 (hexadecimal)" in sequence as address information

(EADR) including both the higher-order bits and the lower-order bits to the external memory 4.

In this way, the external memory 4 reads out 16 bits of encrypted data from a storage location specified by the address information "000004 (hexadecimal)" and, at the same time, reads out 16 bits of encrypted data from another storage location specified by the address information "000006 (hexadecimal)." Then the external memory 4 supplies the two sets of 16 bits of encrypted data to the external memory interface unit 9 in sequence.

As a result, for example, at a timing T13, 64 bits of encrypted data will be stored in the cash memory 24A included in the data processing unit 24.

In response to this, the decryption circuit 24B performs DES decryption on the 64 bits of encrypted data stored in the cash memory 24A, for example, during the period of timing T13 to T17. Then the decryption circuit 24B decrypts the 64 bits of encrypted data by calculating the exclusive-OR for the data obtained as a result of the DES decryption and the higher-order bits of the address information (ADR) supplied from the CPU 5. The decryption circuit 24B extracts 8 bits of data corresponding to the address information "000006 (hexadecimal)" sent from the CPU 5 from the 64 bits of decrypted data. Then, the decryption circuit 24B starts to output the extracted 8 bits of data to

the data bus connected to the CPU 5. At the same timing T17, the timing control unit 23 stops supplying (inactivates) the wait signal (WAIT) to the CPU 5.

When the wait signal (WAIT) is stopped in this way, the CPU 5 stops supplying (inactivates) the data-readout command signal (RD) to the external memory interface unit 9 and latches the 8 bits of data output to the data bus. Accordingly, the CPU 5 is capable of reading out data stored in the external memory 4 via the external memory interface unit 9.

When the semiconductor integrated circuit 3 is set to the fourth mode, encrypted data encrypted using an exclusive-OR and triple DES encryption is stored in the external memory 4. In this case, data is read out from the external memory 4 in the same manner as the above-described third mode.

(3) Operation and Advantages

The semiconductor integrated circuit 3 is capable of performing encryption in accordance with the storage location of data to be stored in the external memory 4 by employing the above-described structure.

For example, when the semiconductor integrated circuit 3 is set to the second mode, encryption is performed by calculating the exclusive-OR for the data to be stored in the external memory 4 and the address information indicating

the storage location of the data. When the semiconductor integrated circuit 3 is set to the third mode, encryption is performed by calculating the exclusive-OR for the data to be stored in the external memory 4 and the address information indicating the storage location of the data and by subsequently performing DES encryption. When the semiconductor integrated circuit 3 is set to the third mode, encryption is performed by calculating the exclusive-OR for the data to be stored in the external memory 4 and the address information indicating the storage location of the data and by subsequently performing triple DES encryption.

The semiconductor integrated circuit 3 writes in the encrypted data obtained as a result of the encryption process into the external memory 4.

In this way, the encrypted data stored in the external memory 4 is encrypted in accordance with the storage location. Therefore, for example, if the encrypted data is copied from the external memory 4 onto another storage medium, it will be difficult to decrypt the encrypted data without knowing the storage location of the encrypted data in the external memory 4. As a result, data can be safely stored in the external memory 4.

When the external memory interface unit 9 in the semiconductor integrated circuit 3 reads out encrypted data from the external memory 4 in response to a data-readout

command signal from the CPU 5, the external memory interface unit 9 decrypts the encrypted data and supplies the decrypted data obtained by the decryption process to the CPU 5. As a result, the CPU 5 can directly use the data supplied from the external memory interface unit 9 without decrypting the data.

Furthermore, when data is written in and/or read out from the internal memory 7 in the semiconductor integrated circuit 3 instead of the external memory 4, data-write command signals, data-readout command signals, and address information addressed to the internal memory 7 are output from the CPU 5. According to this embodiment, these signals and information are not sent outside the semiconductor integrated circuit 3. By preventing data related to the internal structure of the semiconductor integrated circuit 3 from being sent outside the semiconductor integrated circuit 3, the security of the data stored inside the semiconductor integrated circuit 3 is maintained.

According to the above-described structure, data to be stored in the external memory 4 is encrypted in accordance with the storage location of the data. Consequently, for example, if the encrypted data is copied from the external memory 4 onto another storage medium, it will be difficult to decrypt the encrypted data without knowing the storage location of the encrypted data in the external memory 4. As

a result, data can be security stored in the external memory 4.

The CPU 5 in the semiconductor integrated circuit 3 according to this embodiment, for example, stores the address information of each item of data (encrypted data) stored in the external memory 4 in the internal memory 7. In this way, the semiconductor integrated circuit 3 can recognize the storage location of each data item stored in the external memory 4 and can easily read out the data from the external memory 4.

(4) Other Embodiments

In the embodiment described above, as illustrated in Fig. 2, only the decryption circuit 24B is disposed inside the external memory interface unit 9. However, the present invention is not limited, and an encryption circuit 24CX may also be disposed in the external memory interface unit 9X, as illustrated in Fig. 4 (components in Fig. 4 that are the same as those in Fig. 2 are indicated by the same reference numerals).

The operation of an external memory interface unit 9X, as illustrated in Fig. 4, for storing data encrypted only by an exclusive-OR in an external memory 4 will be described below.

For example, a CPU 5 may supply data (DATA) to be stored in the external memory 4 and address information

(ADR) indicating the storage location of the data (DATA) to the external memory interface unit 9X together with a data-write command signal (WR) of a write instruction for the data.

At this time, in the external memory interface unit 9X, the data (DATA) supplied from the CPU 5 is supplied to an encryption circuit 24CX in a data processing unit 24X. The encryption circuit 24CX calculates the exclusive-OR for the supplied data (DATA) and, for example, the address information (ADR) supplied from the CPU 5 via a timing control unit 23X. The data obtained as a result is sent to a switch circuit 22X as encrypted data.

In the external memory interface unit 9X, the address information (ADR) supplied from the CPU 5 is input to an address decoder 20X. The address decoder 20X generates a chip select signal (ECS) based on the input address information (ADR) and outputs the generated chip select signal (ECS) to the external memory 4. In the external memory interface unit 9X, the address information (ADR) supplied from the CPU 5 is separated into higher-order bits and lower-order bits. Then, the higher-order bits are directly output to the external memory 4, and the lower-order bits are output to the external memory 4 via a timing control unit 23X.

Furthermore, in the external memory interface unit 9X,

the data-write command signal (WR) supplied from the CPU 5 is supplied to the timing control unit 23X. The timing control unit 23X outputs the data-write command signal (WR) to the external memory 4 at a predetermined timing as a data-write command signal (EWR). When the data-write command signal (EWR) is output from the timing control unit 23X, the switch circuit 22X, in response, starts sending the encrypted data supplied from the encryption circuit 24CX to the external memory 4.

In this way, the external memory 4 writes in the encrypted data from the external memory interface unit 9X in a storage location specified by the chip select signal (ECS) and address information (EADR) from the external memory interface unit 9X in response to the data-write command signal (EWR) sent from the external memory interface unit 9X.

Next, the operation of the semiconductor integrated circuit 3 for updating data encrypted by an exclusive-OR and DES encryption and already stored in the external memory 4 will be described below.

For example, the CPU 5 may supply data (DATA) for updating 8 bits of data already stored in the external memory 4 (hereinafter, this data is referred to as 'update data') and address information (ADR) indicating the storage location of 8 bits of data to be updated by the update data (DATA) (hereinafter, this data is referred to as 'updated

data') to the external memory interface unit 9X together with a data-write command signal (WR).

At this time, the external memory interface unit 9X starts supplying, to the CPU 5, a wait signal (WAIT) instructing the CPU 5 to wait until the update data (DATA) is written in the external memory 4.

Then the external memory interface unit 9X directly outputs the higher-order bits of the address information (ADR) supplied from the CPU 5 to the external memory 4. Subsequently, the external memory interface unit 9X modifies the lower-order bits of the address information (ADR) in sequence using a counter circuit included in the timing control unit 23X to read out, in sequence, 64 bits of encrypted data including the updated data from the external memory 4 and then stores the read out encrypted data in the cash memory 24AX in the data processing unit 24X.

When the 64 bits of encrypted data including the updated data is stored in the cash memory 24AX in this way, a decryption circuit 24BX in the data processing unit 24X, in response, performs DES decryption on the 64 bits of encrypted data. The decryption circuit 24BX calculates the exclusive-OR for the data obtained after performing DES decryption and the higher-order bits of the address information (ADR) supplied from the CPU 5 to decrypt the 64 bits of data.

The data processing unit 24X overwrites the updated data included in the 64 bits of data decrypted by the decryption circuit 24BX with the update data supplied from the CPU 5. Subsequently, the encryption circuit 24CX in the data processing unit 24X calculates the exclusive-OR for the overwritten data and the higher-order bits of the address information (ADR) supplied from the CPU 5. In this way, 64 bits of encrypted data are generated by performing DES encryption on the data obtained as a result.

Subsequently, the external memory interface unit 9X directly outputs the higher-order bits of the address information (ADR) supplied from the CPU 5 to the external memory 4 and modifies, in sequence, the lower-order bits of the address information (ADR) using the counter circuit in the timing control unit 23X. In this way, the external memory interface unit 9X rewrites the 64 bits of encrypted data in the external memory 4. After rewriting the 64 bits of encrypted data, the external memory interface unit 9X stops supplying the wait signal (WAIT) to the CPU 5.

In this way, the encrypted data in the external memory 4 is updated. The readout operation of the external memory interface unit 9X illustrated in Fig. 4 is the same as the readout operation of the external memory interface unit 9 described above.

In the embodiments above, the reader-writer apparatus 1

for performing data communication with a noncontact integrated circuit (IC) card without any contact is used as an information processing apparatus including the semiconductor integrated circuit 3 and the external memory 4 disposed outside the semiconductor integrated circuit 3. The present invention, however, is not limited, and embodiments of the present invention may be employed in various other information processing apparatuses, such as personal computers, mobile phones, and personal digital assistances (PDAs).

In the above-described embodiments, combination processing for calculating an exclusive-OR to combine data to be stored in the external memory 4 and address information indicating the storage location of the data is performed. The present invention, however, is not limited, and for example, combination processing for calculating AND, OR, NAND, or NOR may be performed instead. Before carrying out such a process, a transposition process for moving each bit of the data stored in the external memory 4 to a different location or moving each bit of the address information indicating the storage location of the data stored in the external memory 4 to a different location may be performed. Furthermore, the transposition processing may be performed on the data obtained by the combination processing.

In the above-described embodiments, nonvolatile memory is used as the external memory 4 disposed outside the semiconductor integrated circuit 3. The present invention, however, is not limited, and various other storage units, such as a ROM and hard disk drive, may be used to store data outside the semiconductor integrated circuit 3.

In the above-described embodiments, the encryption circuits 8 and 24CX are used as encrypting means for generating encrypted data. The present invention, however, is not limited, and various other structures may be employed. Likewise, in the above-described embodiments, the external memory interface units 9 and 9X are used as write means for writing encrypted data in the external memory 4 and readout means for reading out encrypted data from the external memory 4. The present invention, however, is not limited, and various other structures may be employed. In the above-described embodiments, the decryption circuits 24B and 24BX are used as decrypting means for decrypting the encrypted data in accordance with the storage location of the encrypted data. The present invention, however, is not limited, and various other structures may be employed.

It should be understood by those skilled in the art that various modifications, combinations, sub-combinations and alterations may occur depending on design requirements and other factors insofar as they are within the scope of

the appended claims or the equivalents thereof.

Claims:

1. A semiconductor integrated circuit comprising:

a central processing unit for controlling operations of the semiconductor integrated circuit;

means for generating encrypted data by encrypting data to be stored in an external memory disposed outside the semiconductor integrated circuit, the encrypted data being generated by carrying out at least combination processing for combining the data and address information indicating the storage location of the data;

an interface unit for controlling read/write data from/to the external memory; and

means for decrypting encrypted data read by the interface unit in accordance with the storage location of the encrypted data;

wherein the central processing unit controls data-writing by providing the interface unit with the data or the encrypted data together with the address information when the data or the encrypted data is stored in the external memory, and the central processing unit controls data-reading by providing the interface unit with the address information so that the interface unit reads the data or the encrypted data corresponding to the provided address information when the data or the encrypted data stored in the external memory is read.

2. The semiconductor integrated circuit according to Claim 1, wherein the combination processing is computing an exclusive-OR for the data and the address information.

3. The semiconductor integrated according to Claim 1, wherein the encrypted data is generated by encrypting data obtained from the combination processing.

4. An information processing apparatus comprising:

a semiconductor integrated circuit;

an external memory disposed outside the semiconductor integrated circuit; and

an antenna connected to the semiconductor integrated circuit;

wherein the semiconductor integrated circuit includes,

a central processing unit for controlling operations of the semiconductor integrated circuit;

means for generating encrypted data by encrypting data to be stored in an external memory disposed outside the semiconductor integrated circuit, the encrypted data

being generated by carrying out at least combination processing for combining the data and address information indicating the storage location of the data;

an interface unit for controlling read/write data from/to the external memory; and

means for decrypting encrypted data read by the interface unit in accordance with the storage location of the encrypted data;

wherein the central processing unit controls data-writing by providing the interface unit with the data or the encrypted data together with the address information when the data or the encrypted data is stored in the external memory, and the central processing unit controls data-reading by providing the interface unit with the address information so that the interface unit reads the data or the encrypted data corresponding to the provided address information when the data or the encrypted data stored in the external memory is read.

5. The information processing apparatus according to Claim 4, wherein the combination processing is computing an exclusive-OR for the data and the address information.

6. The information processing apparatus according to Claim 4, wherein the encrypted data is generated by encrypting data obtained from the combination processing.