

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
21 September 2006 (21.09.2006)

PCT

(10) International Publication Number
WO 2006/098498 A1

(51) International Patent Classification:
H04L 1/08 (2006.01)

(21) International Application Number:
PCT/JP2006/305753

(22) International Filing Date: 16 March 2006 (16.03.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2005-079621 18 March 2005 (18.03.2005) JP

(71) Applicant (for all designated States except US): **NEC ELECTRONICS CORPORATION** [JP/JP]; 1753, Shimonumabe, Nakahara-ku, Kawasaki-shi, Kanagawa, 2118668 (JP).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **HATAGUCHI, Takeshi** [JP/JP]; c/o NEC ELECTRONICS CORPORATION, 1753, Shimonumabe, Nakahara-ku, Kawasaki-shi, Kanagawa, 2118668 (JP).

(74) Agent: **KATO, Asamichi**; c/o A. Kato & Associates, daVinci BOSEI 7th Floor, 20-12, Shin-Yokohama 3-chome, Kohoku-ku, Yokohama-shi, Kanagawa 222-0033 (JP).

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

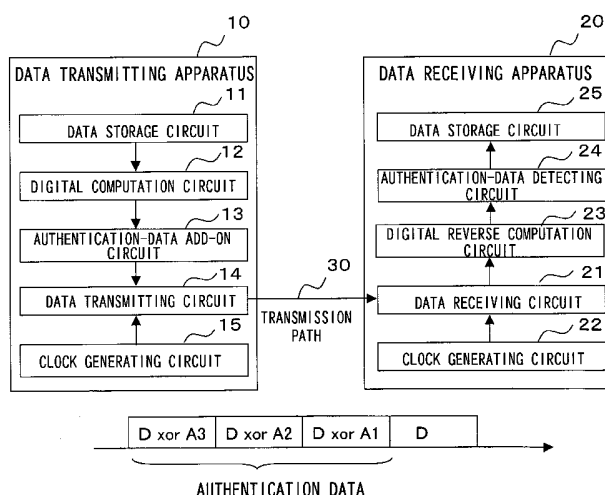
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT,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

Published:

— with international search report

[Continued on next page]

(54) Title: DATA TRANSMITTING APPARATUS, DATA RECEIVING APPARATUS, COMMUNICATION SYSTEM, ERROR DETECTION METHOD AND PROGRAM



(57) Abstract: The fact that erroneous data has been received is sensed easily even if the data has been received at an erroneous timing on the receiving side. A data transmitting apparatus includes a digital computation circuit for subjecting digital data to be transmitted to n (where n is an integer of 2 or greater) different exclusive-OR computations, an authentication-data add-on circuit for gathering the n items of computed data into one set of data, and a data transmitting circuit for transmitting the set of data to a data receiving apparatus. A data receiving apparatus includes a digital reverse computation circuit for subjecting the n items of computed data, which have been received via a data receiving circuit, to respective ones of computations (exclusive-OR computations) that are the reverse of the digital computations on the transmitting side, and an authentication-data detecting circuit for detecting error in the receive data based upon degree of agreement among the n items of receive data obtained by the reverse computations.



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

DESCRIPTION

DATA TRANSMITTING APPARATUS, DATA RECEIVING
APPARATUS, COMMUNICATION SYSTEM, ERROR

5 DETECTION METHOD AND PROGRAM

FIELD OF THE INVENTION

This invention relates to a data transmitting apparatus, a data receiving apparatus, a communication system, an error
10 detection method and related programs. More particularly, the invention relates to a method of detecting error ascribable to a shift in receive timing, a data receiving apparatus for implementing this detection method, a data transmitting apparatus for transmitting data to this data receiving apparatus,
15 a communication system having this data receiving apparatus and data transmitting apparatus, and programs for causing a computer to function as the data receiving apparatus and data transmitting apparatus.

20 BACKGROUND OF THE INVENTION

A variety of error detection methods are known in communication systems for the purpose of detecting, on the receiving side, the occurrence of error on a transmission path, etc. For example, when a single parity bit is added to data
25 bits representing one character on the transmitting side in a

parity check, the parity bit is transmitted upon being set to "0" or "1" in such a manner that the total number of "1" bits will be odd or even. The receiving side detects error based upon whether the number of "1"s in the received data is odd or even.

5 Further, a method using a checksum includes dividing up data into blocks before transmission, computing a checksum for each block by regarding the data in each block as a numerical value, and transmitting the computed checksum together with the data. The receiving side computes the
10 checksum similarly from the data stream transmitted and determines whether there is a match with the checksum that has been transmitted from the transmitting side.

In a case where error has been detected with either of the above-mentioned methods, it is necessary on each such
15 occasion to follow a procedure in which the receiving side issues a re-transmission request and the transmitting side re-transmits the data. The specification of Japanese Patent Kokai Publication No. JP-P2002-217877A (Patent Document 1) discloses a receive-data error detection method that attempts
20 to solve this problem. According to this method, the transmitting side treats a plurality of items of data as one data block and transmits one packet to the receiving side upon including at least three identical data blocks in the packet. The receiving side contrasts the data contained in each of the
25 data blocks included in the received packet. If two or more

items of identical data are present over each data block, this data is adopted as being error free. If identical data is not present over each data block, it is judged that the data contains an error. This method is such that even though a
5 re-transmission request signal is issued to the transmitting side in a case where an error has been detected on the receiving side, opportunities to issue the re-transmission request signal are greatly diminished, overall transceive time is shortened and data can be received reliably on the receiving
10 side.

In an electronic device such as a mobile telephone (cellular phone) or digital camera, a battery pack loaded with batteries that supply the device with power is generally used. Since the temperature of the battery pack rises when the
15 batteries are charged, various proposals have been put forward with a view to preventing the temperature of the battery pack from rising above a prescribed value. However, owing to the appearance recently of imitations and copies of battery packs, the possibility that such problems as abnormal evolution of
20 heat, leakage of fluid and rupture may arise not only during charging but also during use of the battery pack within the electronic device has been pointed out.

A known technique for preventing these problems is to authenticate the battery pack in order to identify whether the
25 battery pack is the one authorized. That is, IDs (identifiers)

are stored in the battery pack and device. At connection, the ID that is output from the battery pack is compared with the ID stored in the device and the suitability of the battery pack is authenticated. This authentication makes it possible to
5 identify an improper battery pack not suitable for the device.

This problem is not limited to battery packs. It is known that imitations of toner packs for copiers also are available on the market and cause great difficulties for users. Applying the above-mentioned authentication system to these
10 cases as well would be effective in solving the problem.

[Patent Document 1]

Japanese Patent Kokai Publication NO.
JP-P2002-217877A

15 SUMMARY OF THE DISCLOSURE

When data relating to such authentication of a battery pack or toner pack is loaded on the device side, a simple data transmission is performed between the battery pack, etc., and the device. In order to control such a data transmission,
20 often the battery pack and device are equipped with CPUs. The hardware provided on the side of the battery pack is required to be as simple as possible, i.e., to readily lend itself to single-chip design, and to be low in cost. To achieve this, a solid-state oscillating element or the like is not used in the
25 clock generating circuit that supplies the CPU with a reference

clock. Rather, often use is made of a circuit such as a ring oscillator in which an odd number of cascade-connected inverter circuits are connected in a feedback configuration. Furthermore, in data transmission as well, use is made of
5 start-stop synchronization that relies upon on a low transmission speed of, e.g., 9600 bps and in which the amount of data transmitted is not that large. The transceiving of data by start-stop synchronization is controlled by a CPU.

A clock generating circuit that relies upon a ring
10 oscillator is a simple circuit. However, since the circuit is composed solely of semiconductor elements, the oscillation frequency readily fluctuates as the circuit is susceptible to the effects of fluctuation due to noise, a fluctuation in temperature and power-supply fluctuations. There are also
15 individual differences. Such fluctuation can exceed several percent at times. Consequently, there is also influence upon data transmission that relies upon start-stop synchronization in which transceive timing is controlled by the clock generating circuit, and hence the timing of data reception
20 deviates with respect to the timing of data transmission and the correct data may not be received.

Described next will be an example of a case where, taking start-stop synchronization as an example, correct data cannot be received owing to such a deviation in receive timing.
25 Fig. 8 is a diagram illustrating a waveform that prevails when

data is received normally in start-stop synchronized data transmission. With the negative-going edge (T_s) of a start bit as the reference, receive-data load timing (intervals T) starts upon elapse of time $1.5T$, and correct receive data (D_0 to D_7) is loaded at timings T_0 to T_7 centered on the data. By contrast, Fig. 9 is a diagram illustrating an example of a waveform that prevails when receive timing has deviated in start-stop synchronized data transmission. With the negative-going edge (T_s) of a start bit as the reference, if receive-data load timing (intervals T') starts upon elapse of time $1.5T'$ and receive data is loaded at timings T_0 to T_7 , then load timing shifts from T to T' . As a consequence, receive data D_0 , D_1 , D_2 , D_4 , D_5 , D_6 , D_7 and "stop bit" are loaded instead of the original receive data D_0 to D_7 .

In this case, with the technique set forth in Patent Document 1 cited above, the same data is transmitted repeatedly and the same data is received even if receive timing deviates. This means that the loaded data is received and construed as being correct data. However, since the data actually accepted is not data in accordance with correct timing, erroneous data happens to be recognized as correct data.

With the advances that have been made in implementing system LSI in recent years, there are now many cases where single-chip design is adopted even on the device side. When a clock generating circuit that relies upon a ring oscillator or

the like is used in such cases, there is also the possibility that periodic noise synchronized to the clock will occur. If this noise is picked up by the transmitting apparatus, the data will become garbled (the high and low levels will be reversed) periodically. In this case also, with the technique set forth in Patent Document 1 cited above, an attempt is made to transmit the same data repeatedly. What happens, however, is that the garbled data is transmitted repeatedly in similar fashion owing to the fact that the transmitting apparatus picks up noise. Accordingly, since the receiving side receives the same data, the loaded data is received and processed upon being construed as being correct data. However, since the data actually accepted is not data in accordance with correct timing, erroneous data happens to be recognized as correct data. A similar problem can arise also in a case where the receiving apparatus picks up noise.

In order to solve the problems set forth above, the present invention according to one aspect thereof provides a data receiving apparatus comprising: a receiving unit receiving n (where n is an integer of 2 or greater) items of computed data obtained by subjecting digital data to n different reversely computable digital computations; a computing unit subjecting the n items of computed data to computations that are the reverse of the digital computations; a determination unit determining degree of agreement among

the n items of receive data obtained by the reverse computations; and an error detector detecting error in the receive data based upon result of determination made by the determination unit.

5 The present invention according to one aspect thereof further provides an error detection method in a communication system for transmitting data from a transmitting side to a receiving side, the method comprising the steps of: on the transmitting side, transmitting n (where n is an integer of 2 or
10 greater) items of computed data obtained by subjecting digital data to be transmitted to n different reversely computable digital computations; and, on the receiving side, detecting error in receive data based upon degree of agreement among n items of receive data obtained by subjecting n items of
15 computed data received to respective ones of computations that are the reverse of the digital computations.

 The present invention according to one aspect thereof further provides a program for causing a computer constituting a data receiving apparatus to execute the following processing:
20 processing of receiving n (where n is an integer of 2 or greater) items of computed data obtained by subjecting digital data to n different reversely computable digital computations;
processing of subjecting the n items of computed data to computations that are the reverse of the digital computations;
25 processing of determining degree of agreement among the n

items of receive data obtained by the reverse computations;
and processing of detecting error in the receive data based
upon result of determination made by the determination
processing.

5 The meritorious effects of the present invention are
summarized as follows.

 In accordance with the present invention, digital data to
be transmitted is subjected to reversely computable digital
computations that differ from one another, whereby a plurality
10 of items of computed data are obtained. The computed data is
transmitted. On the receiving side this data is subjected to
computations that are the reverse of the digital computations
to thereby authenticate the receive data. Accordingly, even if
data has been received on the receiving side at an erroneous
15 timing, the fact that erroneous data has been received can be
sensed with ease.

 Other features and advantages of the present invention
will be apparent from the following description taken in
conjunction with the accompanying drawings, in which like
20 reference characters designate the same or similar parts
throughout the figures thereof.

BRIEF DESCRIPTION OF THE DRAWINGS

 Fig. 1 is a block diagram illustrating the structures of a
25 data transmitting apparatus and data receiving apparatus

according to an embodiment of the present invention;

Fig. 2 is a diagram illustrating a change in data sent from the data transmitting apparatus to the data receiving apparatus;

5 Fig. 3 is a block diagram illustrating the structures of a main device and its peripheral according to a first embodiment of the present invention;

Fig. 4 is a flowchart illustrating operation relating to sending and receiving of authentication data between the main
10 device and its peripheral according to the first embodiment;

Fig. 5 is a flowchart illustrating operation relating to data authentication when the data transmitting apparatus and data receiving apparatus send and receive data;

Fig. 6 is a block diagram illustrating the structures of a
15 main device and its peripheral according to a second embodiment of the present invention;

Fig. 7 is a flowchart illustrating operation relating to sending and receiving of authentication data between the main device and its peripheral according to the second embodiment;

20 Fig. 8 is a diagram illustrating a waveform that prevails when data is received normally in start-stop synchronized data transmission; and

Fig. 9 is a diagram illustrating an example of a waveform that prevails when receive timing has deviated in start-stop
25 synchronized data transmission.

PREFERRED EMBODIMENTS OF THE INVENTION

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

5 Fig. 1 is a block diagram illustrating the structures of a data transmitting apparatus 10 and data receiving apparatus 20 according to an embodiment of the present invention. As shown in Fig. 1, the data transmitting apparatus 10 includes a data storage circuit 11, a digital computation circuit 12, an authentication-data add-on circuit 13, a data transmitting
10 circuit 14 and a clock generating circuit 15. Further, the data receiving apparatus 20 includes a data receiving circuit 21, a clock generating circuit 22, a digital reverse computation circuit 23, an authentication-data detecting circuit 24 and a
15 data storage circuit 25. The data transmitting apparatus 10 transmits data, with attached authentication data, to the data receiving apparatus 20 via a transmission path 30. It should be noted that although the data transmitting apparatus 10 and data receiving apparatus 20 have a variety of circuits that
20 cause them to perform other functions as well, these circuits are not related to the features of the present invention and are neither illustrated nor described here.

The data storage circuit 11 stores, on the transmitting side, data D that is to be transmitted. The digital
25 computation circuit 12 subjects the data D, which has been

stored in the data storage circuit 11, to n (where n is an integer of 2 or greater) different digital computations that are capable of being computed in reverse. By way of example, reversely computable digital computations are operations such as
5 exclusive-OR (XOR) between the data and predetermined numbers that differ from one another; prescribed rotations that differ from one another (a shift of a prescribed number of bits is made to the right or left and bits are inserted from the right end or left end with regard to bits that have overflowed from
10 the left end or right end; and addition and subtraction between the data and predetermined numbers that differ from each other (digits that overflow are discarded). These are computations that are capable of restoring the original data by reverse computation. It is assumed here that digital
15 computation includes computation that performs no operation whatsoever. That is, an exclusive-OR between the data and zero, rotation of a "0" bit and addition between the data and zero are regarded as reversely computable digital computations.

20 The authentication-data add-on circuit 13 outputs n items of data to the data transmitting circuit 14 as authentication data. These n items of data are obtained by subjecting the original data to the n different reversely computable digital computations. On the basis of a clock
25 generated by the clock generating circuit 15, the data

transmitting circuit 14 transmits the authentication data to the data receiving apparatus 20 via the transmission path 30. In the example of authentication data illustrated in Fig. 1, four items of data are transmitted, namely data D, which is the data to be transmitted; data obtained by taking the exclusive-OR (xor) between data D and A1; data obtained by taking the exclusive-OR (xor) between data D and A2; and data obtained by taking the exclusive-OR (xor) between data D and A3. Here A1, A2 and A3 are constants having values that differ from one another.

On the basis of the clock generated by the clock generating circuit 22, the data receiving circuit 21 receives the data and outputs it to the digital reverse computation circuit 23. The latter subjects the items of data that enter from the data receiving circuit 21 to computations that are the reverse of the computations performed by the digital computation circuit 12. With regard to the example of authentication data illustrated in Fig. 1, the digital reverse computation circuit 23 performs no operation on the leading data D (i.e., takes the exclusive-OR with zero), takes the exclusive-OR between the second item of data D xor A1 and A1 $[(D \text{ xor } A1) \text{ xor } A1 = D]$, and takes the exclusive-OR between the third and fourth items of data and A2 and A3, respectively.

The authentication-data detecting circuit 24 performs data authentication based upon degree of agreement in data

reversely computed in the digital reverse computation circuit 23. More specifically, in the case of the example cited above, since data D, data (D xor A1) xor A1, data (D xor A2) xor A2 and data (D xor A3) xor A3 are the data items D, D, D, D, respectively, the authentication-data detecting circuit 24 judges that all of the data agrees and outputs the data D, which is the result of authentication, to the data storage circuit 25.

An instance where non-agreement is detected in the authentication process will be described next. Assume that the clock frequencies generated by the clock generating circuit 15 and clock generating circuit 22 differ by 10%. If the data transmitting circuit 14 transmits data to the data receiving circuit 21 by start-stop synchronization in such case, the receive data will be loaded at an improper timing of the kind shown in Fig. 9. Assume that transmit data D is composed of one byte, i.e., eight bits (D7, D6, D5, D4, D3, D2, D1, D0), and that these bits are 11110000 (0xF0 in hexadecimal notation). In this case, the bits loaded as the receive data are the stop bit (1) instead of D7; D7(1) instead of D6; D6(1) instead of D5; D5(1) instead of D4; and D4(1) instead of D3. Data D3 is not loaded. Accordingly, the data received on the receiving side is 11111000 (0xF8).

In accordance with the conventional technique described in Patent Document 1 cited above, 11111000 will be received three times and therefore 11111000 will be treated as being the

correct data. Processing will proceed on the receiving side based upon this supposedly correct data and a contradiction of some sort will occur later in other processing at a higher level.

In this embodiment according to the present invention, assume that $A1 = 0x55h$, $A2 = 0xAA$, $A3 = 0x33$ hold. In this case, as depicted in Fig. 2, the transmit data that is sent from the data transmitting circuit 14 to the data receiving circuit 21 is $0xF0$, $0xA5$ ($= 0xF0 \text{ xor } 0x55$), $0x5A$ ($= 0xF0 \text{ xor } 0xAA$) and $0xC3$ ($= 0xF0 \text{ xor } 0x33$). On the other hand, the receive data that is received by the data receiving circuit 21 has "1" (which corresponds to the stop bit) added onto the most significant bit and lacks the bit 3 (D3) and therefore is $0xF8$, $0xD5$, $0xAA$ and $0xE3$, respectively. When these items of data are subjected to the reverse computation (xor) by the digital reverse computation circuit 23, the results obtained are $0xF8$, $0x80$ ($= 0xD5 \text{ xor } 0x55$), $0x00$ ($= 0xAA \text{ xor } 0xAA$) and $0xD0$ ($= 0xE3 \text{ xor } 0x33$), respectively. That is, none of the four items of data received and subjected to reverse computation (the exclusive-OR operation) agree. The authentication-data detecting circuit 24 is capable of recognizing that none of the reversely computed results agree and can immediately execute a predetermined processing based upon the fact that the data cannot be authenticated.

In the description set forth above, it is described that the transmit data is composed of four bytes and that none of them

agree on the receiving side. However, this does not impose any limitation. It may be arranged generally to transmit n (where n is an integer of 2 or greater) items of computed data obtained by subjecting digital data of an original block to be transmitted to n different reversely computable digital computations, and to authenticate the data of the original transmission based upon the degree of agreement among these items of data.

10 [First Embodiment]

Fig. 3 is a block diagram illustrating the structures of a main device 40 and a peripheral 50 thereof according to a first embodiment of the present invention. The main device 40 in Fig. 3 is a portable electronic device such as a digital camera and includes a main CPU 41; a microcomputer 42 that controls the transmission of data to the peripheral 50; and a ring oscillator 43 for supplying the microcomputer 42 with a clock signal. The main CPU 41 incorporates a data transmitting unit 10a, a data receiving unit 20a and a program 44 for implementing the functions of the main device 40. The data transmitting unit 10a and data receiving unit 20a correspond to the data transmitting apparatus 10 and data receiving apparatus 20, respectively, of Fig. 1, and are implemented by the program 44.

25 The microcomputer 42 incorporates a data transmitting

unit 10b, a data receiving unit 20b, a data transmitting unit 10c, a data receiving unit 20c and a program 45. The microcomputer 42 sends data and to and from the main CPU 41 via a communication path 32 and sends and receives data to and from the peripheral 50 via a communication path 31. The data transmitting units 10b and 10c correspond to the data transmitting apparatus 10 of Fig. 1, and the data receiving units 20b and 20c correspond to the data receiving apparatus 20 of Fig. 1. These units are implemented by the program 45.

10 The data receiving unit 20b receives data from the data transmitting unit 10a via the communication path 32, and the data transmitting unit 10b transmits data to the data receiving unit 20a via the communication path 32. Further, the data receiving unit 20c receives data from a data transmitting unit 10d via the communication path 31, and the data transmitting unit 10c transmits data to a data receiving unit 20d via the communication path 31.

The peripheral 50, which is a device such as a battery pack connected to the main device 40 for the purpose of supplying power, has a microcomputer 51 and a ring oscillator 52 for supplying the microcomputer 51 with a clock signal. The microcomputer 51 incorporates the data transmitting unit 10d, the data receiving unit 20d and a program 53 for implementing the functions of the peripheral 50. The program 53 causes the peripheral 50 to function and controls

the data transmitting unit 10d and data receiving unit 20d so as to send and receive data to and from the main device 40 via the communication path 31. It should be noted that although the main device 40 and peripheral 50 have various circuits that
5 cause them to perform other functions as well, these circuits are not related to the features of the present invention and are neither illustrated nor described here.

Operation relating to the sending and receiving authentication data in the main device 40 and peripheral 50
10 will be described next. Fig. 4 is a flowchart illustrating operation relating to sending and receiving of authentication data between the main device and its peripheral according to the first embodiment. In Fig. 4, the main device 40 executes the authentication processing of the main device 40 by a
15 challenge-response method.

The main CPU 41 instructs the microcomputer 42 to start authentication at step S0.

Upon being instructed to start authentication, the microcomputer 42 generates random numbers and sends the
20 random numbers to the microcomputer 51 at step S1.

The microcomputer 51 notifies the microcomputer 42 at step S2 of the fact that the random numbers have been received normally.

The microcomputer 51 generates encrypted random
25 numbers, these being encrypted using the received random

numbers and the code of a key held internally.

The microcomputer 51 transmits the encrypted random numbers to the microcomputer 42 at step S4.

The microcomputer 42 generates encrypted random
5 numbers at step S5, these being encrypted using the random numbers generated at step S1 and the code of a key held internally.

The microcomputer 42 compares the encrypted random numbers, which have sent from the microcomputer 51 at step
10 S4, and the encrypted random numbers, which have been generated at step S5, at step S6. If the result of the comparison is that the random numbers agree, the microcomputer 42 authenticates the peripheral 50 as being authorized. If the result of the comparison is that random
15 numbers do not agree, then the microcomputer 42 decides that the peripheral 50 is not authorized.

The microcomputer 42 transmits the result of authentication to the main CPU 41 at step S7.

Through such operation of the main device 40 and
20 peripheral 50, the main device 40 authenticates the peripheral 50. It should be noted that Fig. 4 illustrates only the principal operation involved in authentication. In addition to the communication processing shown in Fig. 4, the main device 40 transmits commands such as "start authentication" to the
25 peripheral 50, and the peripheral 50 transmits responses such

as "received normally" to the main device 40.

A method of authenticating data sent and received will be described next. This will be described taking as an example authentication of data sent and received when result
5 of authentication is transmitted at step S7 or when notification of normal reception is given at step S2.

Fig. 5 is a flowchart illustrating operation relating to data authentication when the data transmitting apparatus and data receiving apparatus send and receive data. In case of
10 step S7, this represents an example in which the data transmitting unit 10b transmits data to the data receiving unit 20a. In the case of step S2, this represents an example in which the data transmitting unit 10d transmits data to the data receiving unit 20c. A case where the data transmitting unit
15 10b transmits data to the data receiving unit 20a will be described by way of example.

At step S11, the data transmitting unit 10b prepares transmit data, namely data which is the result of authentication.

20 At step S12, the authentication-result data is subjected to four different exclusive-OR operations to obtain four items of computed data.

At step S13, the four items of computed data are transmitted to the data receiving unit 20a.

25 At step S14, the data receiving unit 20a receives the four

items of computed data transmitted thereto.

At step S15, the data receiving unit 20a subjects the four received items of computed data to four different exclusive-OR operations to obtain four items of data.

5 At step S16, it is determined whether the four items of data received agree. Control proceeds to step S17 if they agree and to step S19 if they do not.

At step S17, the received data is retained as being correct receive data.

10 At step S18, processing in a case where the result of authentication is "OK" is executed and this series of operations ends.

At step S19, processing in a case where the result of authentication is "NG" is executed and this series of
15 operations ends.

With the operations described above, steps S11 to S13 are executed by the program 45 and steps S14 to S19 are executed by the program 44.

Thus, the data transmitting unit 10b and data receiving
20 unit 20a execute authentication of transceive data by very simple digital computations such as exclusive-OR operations. A microcomputer with which a portable electronic device or battery pack is equipped usually requires to be of small size. By virtue of the simple digital computations, however,
25 computation can be performed by simple instructions. Even

if data has been received at an erroneous timing on the receiving side in the manner exemplified in the example of Fig. 2 owing to a deviation between the oscillation frequency of the ring oscillator 43 and the reference clock of main CPU 41 or a deviation between the oscillation frequency of the ring oscillator 43 and that of the ring oscillator 52, the fact that erroneous data has been received can be detected easily. The same is true also in a case where data has been received at an erroneous timing on the receiving side owing to periodic noise.

10

[Second Embodiment]

Fig. 6 is a block diagram illustrating the structures of a main device 40a and its peripheral 50 according to a second embodiment of the present invention. The main device 40a in Fig. 6 is one equivalent to the main device 40 of Fig. 1 and has a main CPU 41a. The main CPU 41a incorporates a data transmitting unit 10e, a data receiving unit 20e and a program 44a for implementing the functions of the main device 40a. The data transmitting unit 10e and data receiving unit 20e correspond to the data transmitting apparatus 10 and data receiving apparatus 20, respectively, of Fig. 1, and are implemented by the program 44a. The program 44a substantially incorporates the programs 44, 45 of Fig. 3. The main device 40a thus constructed operates in a manner similar to that of the main device 40 of Fig. 3, and the sending and

15

20

25

receiving of data between the main device 40a and peripheral 50 is performed in a manner identical with that of the first embodiment.

Operation relating to the sending and receiving authentication data in the main device 40a and peripheral 50 will be described next. Fig. 7 is a flowchart illustrating operation relating to sending and receiving of authentication data between the main device and its peripheral according to the second embodiment. Steps in Fig. 7 having the same step numbers as those in Fig. 4 indicate operations similar to those described in Fig. 4 and need not be described again. It should be noted that the main CPU 41a combines the functions of the main CPU 41 and microcomputer 42 of Fig. 4, and since the start of authentication and acquisition of results of authentication are performed by the main CPU 41a alone, steps S0 and S7 in Fig. 4 are unnecessary in Fig. 7 and are deleted.

It should be noted that the main device 40a generates a clock by a solid-state oscillator such as a quartz oscillator instead of using an oscillation circuit that relies upon a ring oscillator, and that the main CPU 41a operates and data is transmitted in accordance with this clock. Accordingly, the period of the data sent and received to and from the main device 40a is very accurate. However, in a case where the oscillation frequency of the ring oscillator 52 shifts relative to the clock of the main device 40a, authentication of the

transmitted data is performed in a manner similar to that described in the first embodiment.

Though the present invention has been described in accordance with the foregoing embodiments, the invention is
5 not limited to these embodiments and it goes without saying that the invention covers various modifications and changes that would be obvious to those skilled in the art within the scope of the claims.

The present invention is applicable to error detection in
10 data transmission between an electronic device and its peripheral equipment, namely between a device such as a mobile telephone or digital camera, its peripherals such as a battery pack and printer and cartridges used in these peripherals, another example being data transmission between
15 a copier and a toner cartridge serving as a copier peripheral.

CLAIMS:

1. A data receiving apparatus comprising:

a receiving unit receiving n (where n is an integer of 2 or greater) items of computed data obtained by subjecting digital
5 data to n different reversely computable digital computations;

a computing unit subjecting the n items of computed data to computations that are the reverse of the digital computations;

a determination unit determining degree of agreement
10 among the n items of receive data obtained by the reverse computations; and

an error detector detecting error in the receive data based upon result of determination made by said determination unit.

15 2. A data transmitting apparatus for transmitting the computed data to said data receiving apparatus set forth in claim 1, comprising:

a computing unit subjecting the digital data to the n different reversely computable digital computations; and

20 a transmitting unit transmitting n items of computed data that are output from said computing unit.

3. The data receiving apparatus according to claim 1, wherein said receiving unit receives the computed data by start-stop synchronization.

25 4. The data transmitting apparatus according to claim 2,

wherein said transmitting unit transmits the computed data by start-stop synchronization.

5. The data receiving apparatus according to claim 1, wherein the digital computations are digital computations for taking an exclusive-OR between the digital data and prescribed values that are different from one another.

6. The data transmitting apparatus according to claim 2, wherein the digital computations are digital computations for taking an exclusive-OR between the digital data and prescribed values that are different from one another.

7. A communication system comprising:
the data receiving apparatus set forth in claim 1; and
the data transmitting apparatus set forth in claim 2.

8. A communication system comprising:
15 the data receiving apparatus set forth in claim 3 and the data transmitting apparatus set forth in claim 4.

9. An electronic device comprising:
the data receiving apparatus set forth in claim 1; and
the data transmitting apparatus set forth in claim 2.

20 10. An electronic device comprising:
the data receiving apparatus set forth in claim 3; and
the data transmitting apparatus set forth in claim 4.

11. Peripheral equipment for an electronic device, comprising:

25 the data receiving apparatus set forth in claim 1; and

the data transmitting apparatus set forth in claim 2.

12. Peripheral equipment for an electronic device, comprising:

the data receiving apparatus set forth in claim 3; and

5 the data transmitting apparatus set forth in claim 4.

13. A battery pack comprising:

the data receiving apparatus set forth in claim 1; and

the data transmitting apparatus set forth in claim 2.

14. A battery pack comprising:

10 the data receiving apparatus set forth in claim 3; and

the data transmitting apparatus set forth in claim 4.

15. An error detection method in a communication system for transmitting data from a transmitting side to a receiving side, said method comprising the steps of:

15 on the transmitting side, transmitting n (where n is an integer of 2 or greater) items of computed data obtained by subjecting digital data to be transmitted to n different reversely computable digital computations; and

on the receiving side, detecting error in receive data
20 based upon degree of agreement among n items of receive data obtained by subjecting n items of computed data received to respective ones of computations that are the reverse of the digital computations.

16. A program for causing a computer constituting a data
25 receiving apparatus to execute the following processing steps:

receiving n (where n is an integer of 2 or greater) items of computed data obtained by subjecting digital data to n different reversely computable digital computations;

subjecting the n items of computed data to computations
5 that are the reverse of the digital computations;

determining degree of agreement among the n items of receive data obtained by the reverse computations; and

detecting error in the receive data based upon result of determination made by said determination processing.

10 17. A program for causing a computer constituting a data transmitting apparatus, which transmits data to the computer that executes the program set forth in claim 16, to execute the following processing steps:

subjecting the digital data to the n different reversely
15 computable digital computations; and

transmitting the n items of computed data.

FIG. 1

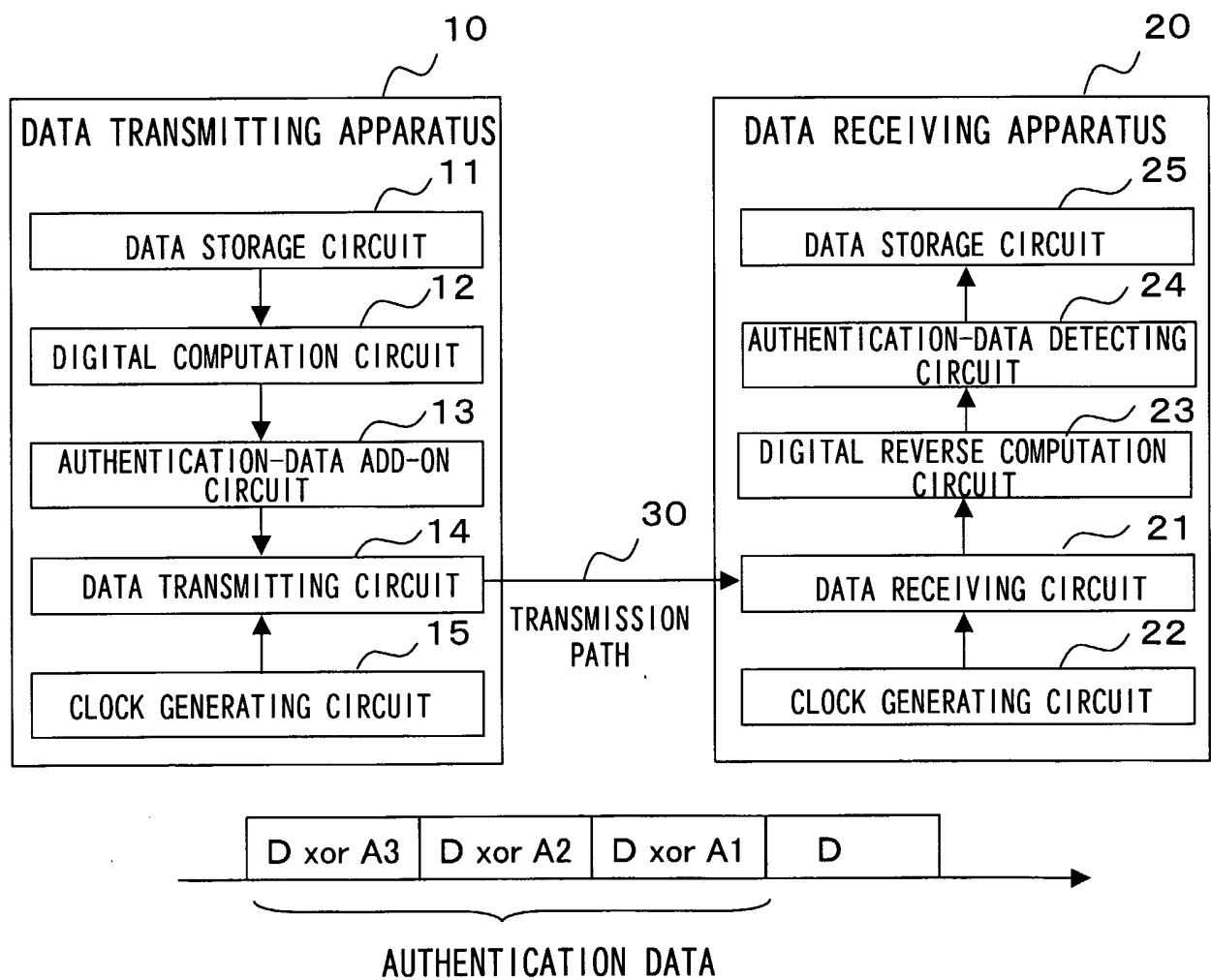


FIG. 2

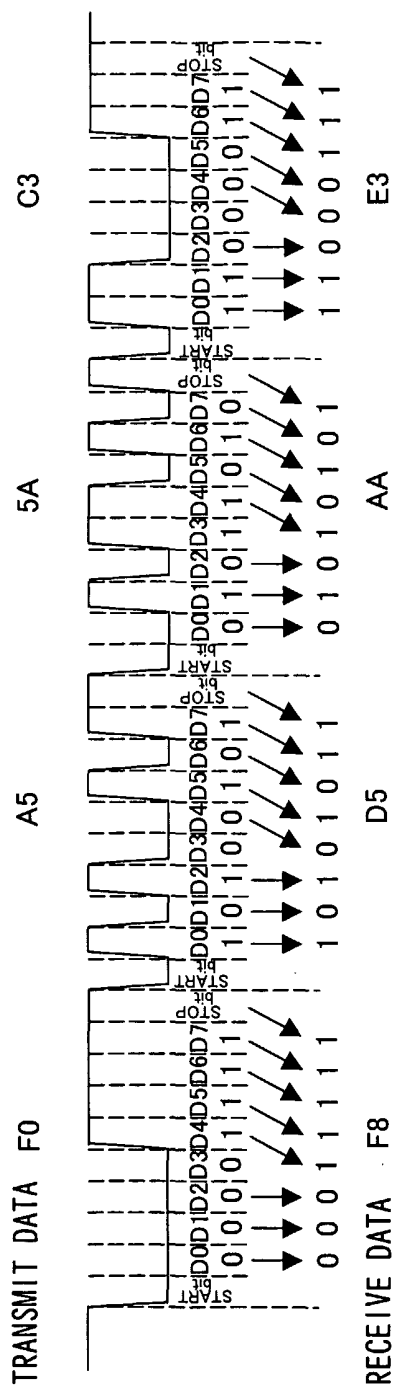


FIG. 3

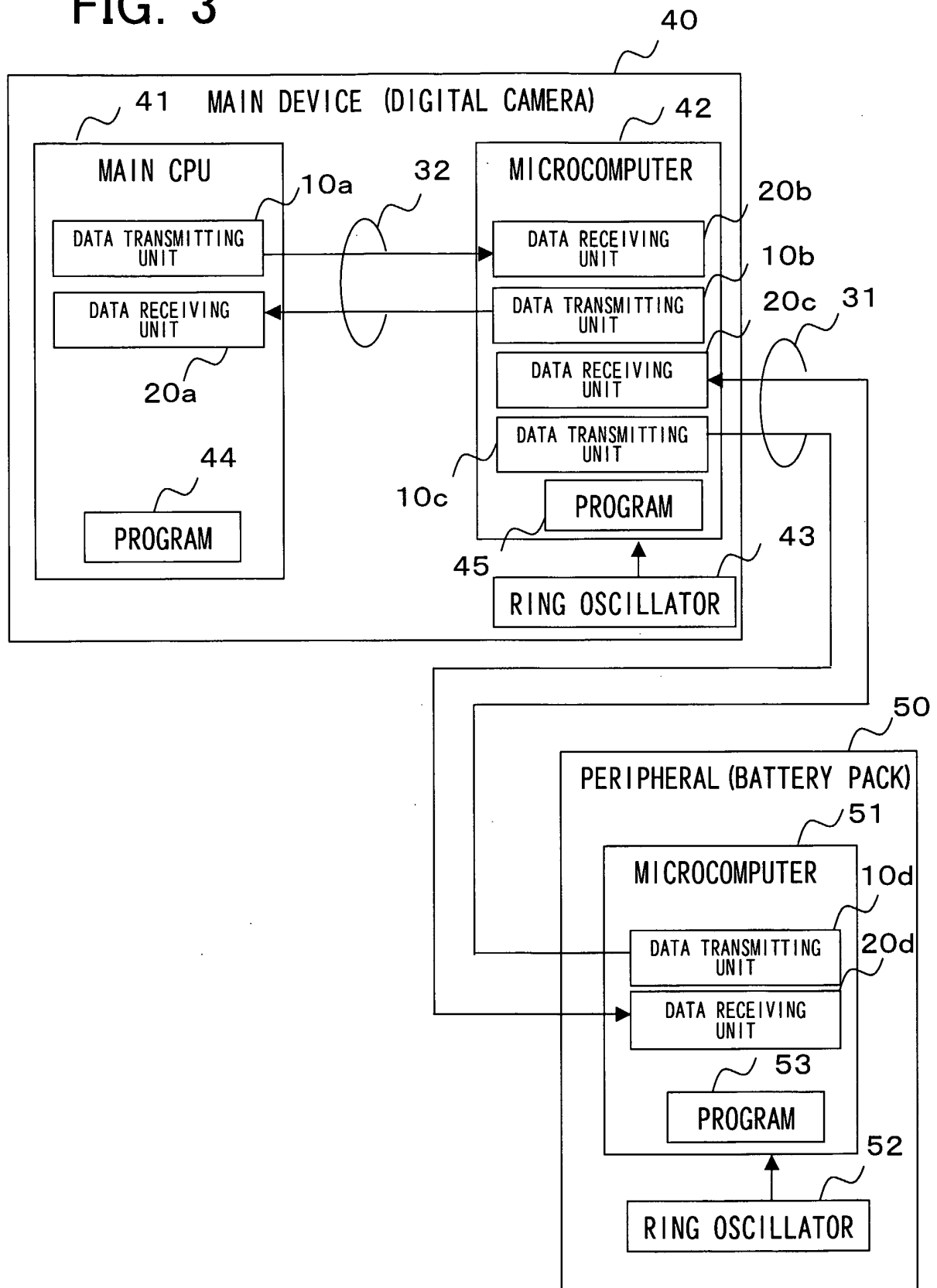


FIG. 4

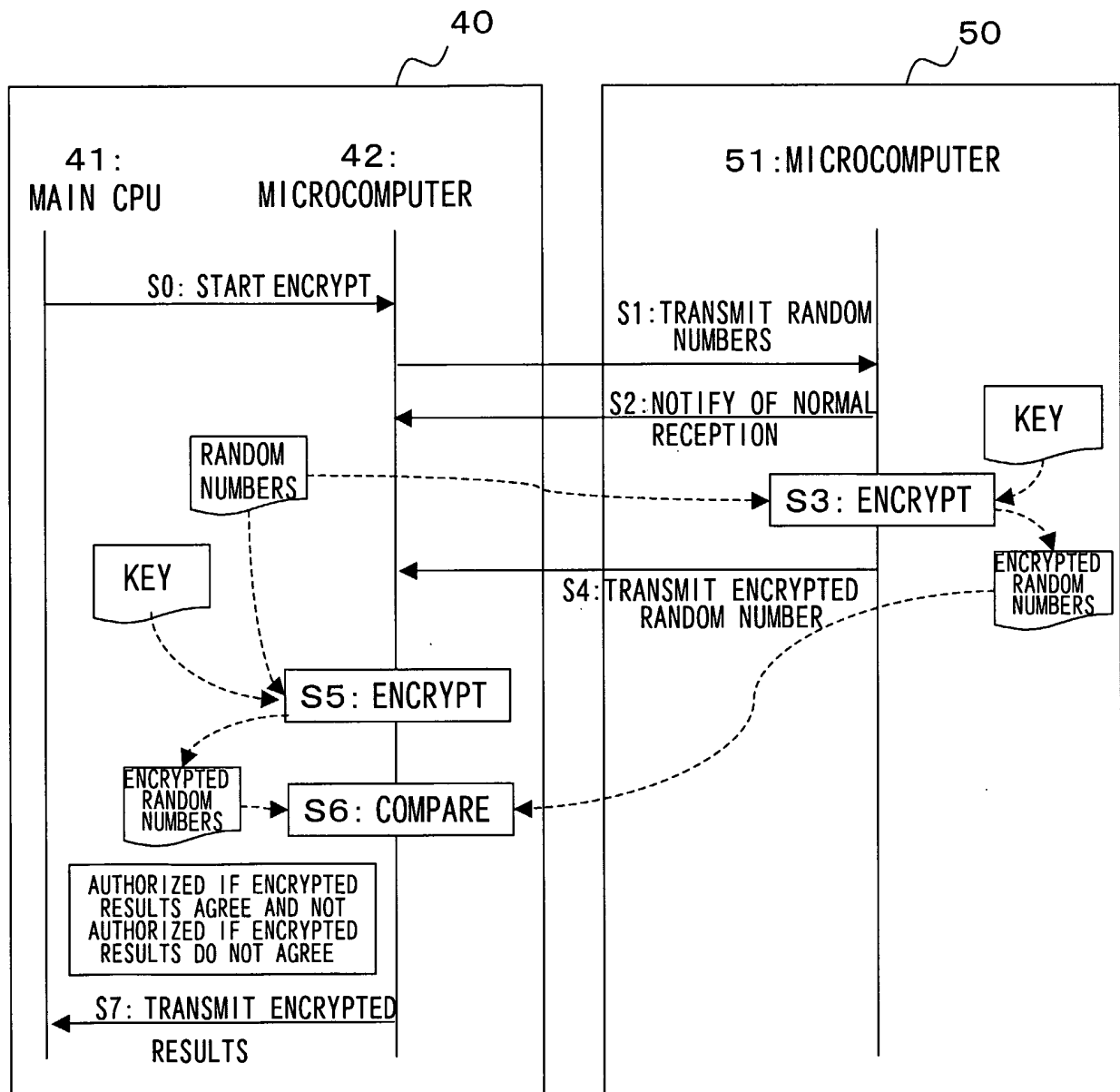


FIG. 5

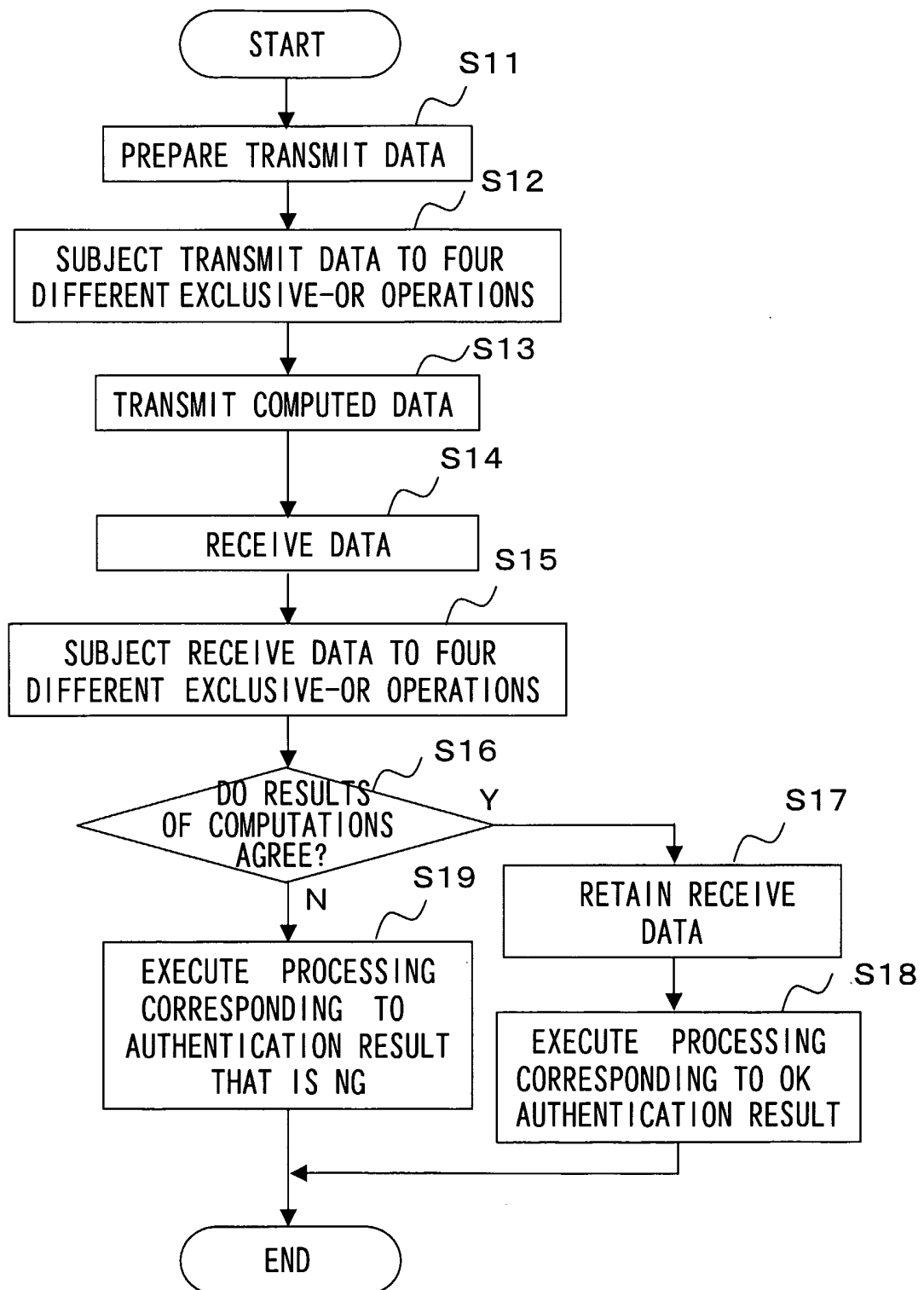


FIG. 6

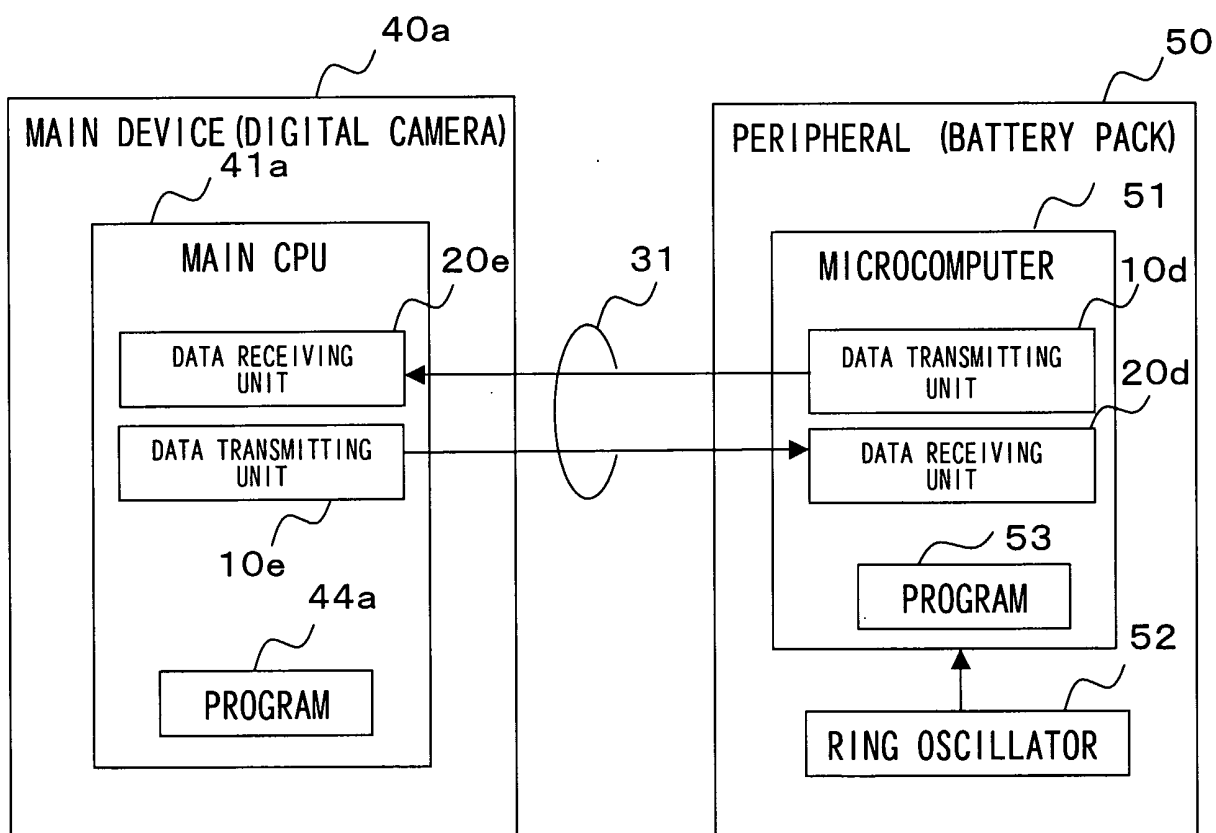


FIG. 7

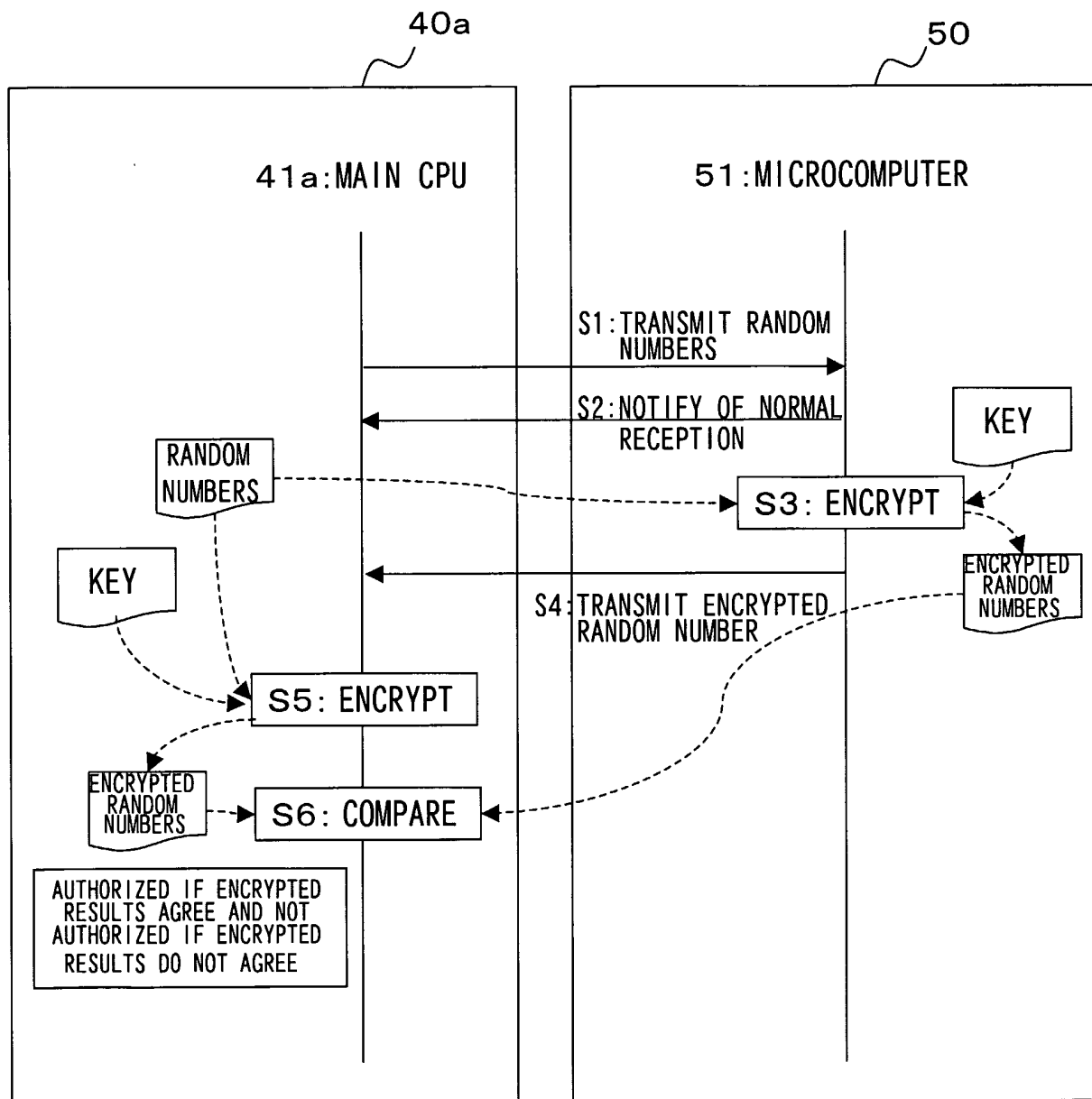


FIG. 8

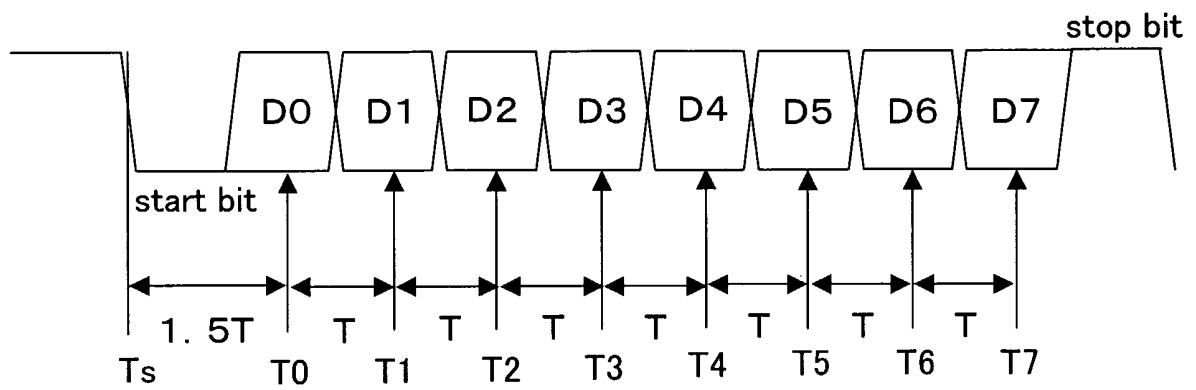
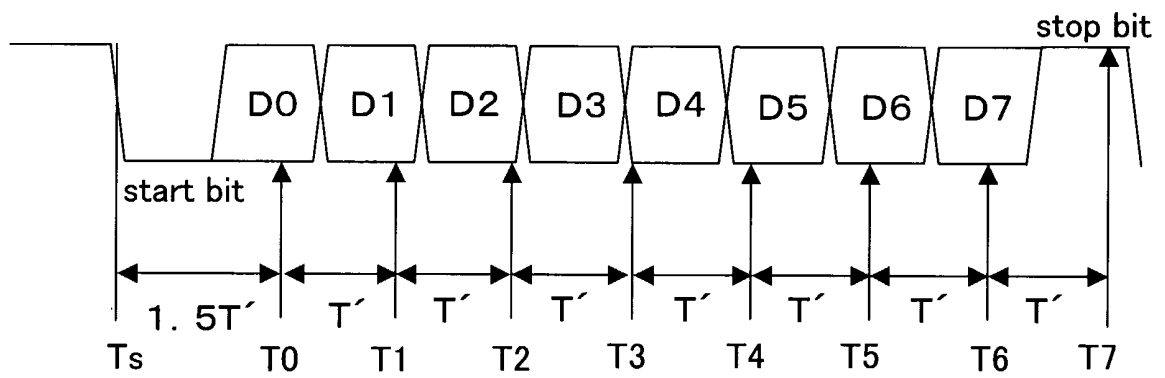


FIG. 9



INTERNATIONAL SEARCH REPORT

International application No
PCT/JP2006/305753

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L1/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L H02J

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 052 217 A (STORNO A/S) 21 January 1981 (1981-01-21) abstract page 2, left-hand column, line 57 - right-hand column, line 129; figures 3a,3b claim 1	1-17
X	US 4 670 880 A (JITSUKAWA ET AL) 2 June 1987 (1987-06-02) abstract; figure 1	1,2,7-9, 16,17
A	US 2003/102842 A1 (TAMAI MIKITAKA ET AL) 5 June 2003 (2003-06-05) abstract	13,14
A	US 6 429 622 B1 (SVENSSON LARS) 6 August 2002 (2002-08-06) abstract	13,14

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

A document defining the general state of the art which is not considered to be of particular relevance

E earlier document but published on or after the international filing date

L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

O document referring to an oral disclosure, use, exhibition or other means

P document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

G document member of the same patent family

Date of the actual completion of the international search

23 June 2006

Date of mailing of the international search report

05/07/2006

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Martínez Martínez, V

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/JP2006/305753

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
GB 2052217	A	21-01-1981	DE 3022047 A1	18-12-1980
			DK 243679 A	13-12-1980
			FR 2458958 A1	02-01-1981
			SE 448139 B	19-01-1987
			SE 8004301 A	13-12-1980
US 4670880	A	02-06-1987	DE 3586708 D1	05-11-1992
			DE 3586708 T2	22-04-1993
			EP 0177690 A2	16-04-1986
			IN 165546 A1	11-11-1989
			JP 1598733 C	28-01-1991
			JP 2023888 B	25-05-1990
			JP 61070637 A	11-04-1986
			KR 9006920 B1	24-09-1990
US 2003102842	A1	05-06-2003	CN 1421954 A	04-06-2003
			JP 3625799 B2	02-03-2005
			JP 2003168406 A	13-06-2003
US 6429622	B1	06-08-2002	NONE	