

DESCRIPTION

PORTABLE ELECTRONIC DEVICE, INFORMATION PROCESSING
APPARATUS, INFORMATION PROCESSING SYSTEM, AND INFORMATION
PROCESSING METHOD

5

FIELD

Embodiments described herein relate generally to a
portable electronic device, an information processing
apparatus, an information processing system, and an
10 information processing method.

BACKGROUND

Security devices such as integrated circuit cards (IC
cards) provided with integrated circuit chips (IC chips)
are widely used as credit cards or electronic passports. IC
15 cards are called portable electronic devices or the like
since they are carried by users.

For example, both electronic passports and reading
apparatuses generate an elliptic cryptographic key each
time, exchange their public keys with each other, and
20 generate a session key for encrypting and communicating
subsequent processing. The session key is used to secure
confidentiality and integrity, and is used not only for
encryption but also for generating authentication data. In
passports, session keys for encryption and for
25 authentication are simultaneously generated and shared.
Since only the public keys are exchanged in this method, it
is very difficult to identify the session key.

CITATION LIST

PATENT LITERATURE

Patent Literature 1: Jpn. PCT National Publication
No. 2022-537733

Patent Literature 2: International Publication
5 No. 2021/029173

Patent Literature 3: Japanese Patent No. 7004654

SUMMARY

TECHNICAL PROBLEM

With the advent of quantum computers, it is becoming
10 necessary to shift to cryptography (post quantum
cryptography: PQC), which is considered to be difficult to
compute with quantum computers. Under such circumstances,
even though security devices such as IC cards have very
high security, a volatile memory and a nonvolatile memory
15 are small and a computing speed of a central processing
unit (CPU) is not sufficient for installing PQC as compared
with reading apparatuses. That is, the hardware resources
of the IC cards are the hurdle to installing PQC. For such
devices with difficult hardware resources, a technology
20 that enables installation of a predetermined cryptographic
algorithm such as PQC is desired.

An object of the present invention is to provide a
portable electronic device, an information processing
apparatus, an information processing system, and an
25 information processing method that enable installation of a
predetermined cryptographic algorithm with limited hardware
resources.

SOLUTION TO PROBLEM

According to an embodiment, a portable electronic device includes a memory, an interface, and a processor. The memory stores cryptographic information including a cryptographic algorithm. The interface is configured to communicate with an information processing apparatus. The processor is configured to generate a random number. The interface is configured to transmit the cryptographic information to the information processing apparatus, and receive a public key transmitted from the information processing apparatus, the public key and a secret key being generated based on the cryptographic algorithm. The processor is configured to generate an encrypted random number from the random number through an encryption process based on the public key. The interface is configured to transmit the encrypted random number to the information processing apparatus. The processor is configured to generate a session key for use for communication with the information processing apparatus based on the random number.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram showing an example of an information processing system according to an embodiment that includes an IC card as a portable electronic device and an IC card processing apparatus as an information processing apparatus that communicates with the IC card.

FIG. 2 is a block diagram schematically showing an

example of a configuration of the IC card according to the embodiment.

FIG. 3 is a diagram showing a first example of a session-key sharing process sequence according to the
5 embodiment.

FIG. 4 is a diagram showing a second example of a session-key sharing process sequence according to the embodiment.

FIG. 5 is a diagram showing a third example of a session-key sharing process sequence according to the
10 embodiment.

FIG. 6 is a diagram showing a fourth example of a session-key sharing process sequence according to the embodiment.

FIG. 7 is a diagram showing a fifth example of a session-key sharing process sequence according to the
15 embodiment.

FIG. 8 is a diagram showing a sixth example of a session-key sharing process sequence according to the
20 embodiment.

FIG. 9 is an illustration of Algorithm 1 of a PQC standard (Kyber).

FIG. 10 is an illustration of Algorithm 2 of a PQC standard (Kyber).

25 DETAILED DESCRIPTION

Hereinafter, embodiments will be described with reference to the accompanying drawings.

FIG. 1 is a block diagram showing an example of an information processing system according to an embodiment that includes an IC card as a portable electronic device and an IC card processing apparatus as an information processing apparatus that communicates with the IC card.

As shown in FIG. 1, the information processing system includes an IC card processing apparatus 1 and an IC card 2. The IC card processing apparatus 1 is a host apparatus that provides a command to the IC card 2 and receives a response from the IC card 2.

In the configuration example shown in FIG. 1, the IC card processing apparatus 1 includes a central processing unit (CPU) 11, a display 12, an operation unit 13, a card reader-writer 14, an optical character recognition or optical character reader (OCR) 15, and a storage unit 16.

The CPU 11 is a processor that controls the operation of the entire IC card processing apparatus 1. The CPU 11 performs various processes based on the control programs and control data stored in the storage unit 16. For example, the CPU 11 performs various processes corresponding to the operational control of the IC card processing apparatus 1 or the operational mode of the IC card processing apparatus 1 by executing the programs stored in a memory such as the storage unit 16. Some of the various functions may be implemented by a hardware circuit. In this case, the CPU 11 controls the functions implemented by a hardware circuit.

For example, the CPU 11 functions to obtain cryptographic information transmitted from the IC card 2 via the card reader-writer 14 and generate a public key (Pub Key) and a secret key (Sec Key), which are a PQC's key pair, based on a PQC cryptographic algorithm and a key length included in the cryptographic information. The CPU 11 also functions to transmit various types of data such as a public key or an encrypted public key to the IC card 2 via the card reader-writer 14. The CPU 11 also functions to encrypt various types of data such as a public key that are transmitted to the IC card 2 via the card reader-writer 14. The CPU 11 also functions to decrypt various types of encrypted data such as encrypted random numbers that are transmitted from the IC card 2 via the card reader-writer 14. The CPU 11 also functions to generate a session key and the like based on the decrypted random numbers. The CPU 11 may operate based on an input to the operation unit 13 via the card reader-writer 14. For example, the CPU 11 transmits a write command including data input to the operation unit 13 to the IC card 2 and thereby requests the IC card 2 to write the data. In the present embodiment, a case where a PQC cryptographic algorithm is installed will be described; however, the present embodiment is not limited to a PQC cryptographic algorithm, and the mechanism of the present embodiment is applicable to a predetermined cryptographic algorithm.

The display 12 is a display device that displays

various types of information under the control of the CPU 11. The display 12 is, for example, a liquid crystal monitor or the like.

5 Various operation instructions, data, and the like are input to the operation unit 13 from a user of the IC card processing apparatus 1. The operation unit 13 transmits the input operation instructions, data, and the like to the CPU 11. Examples of the operation unit 13 include a keyboard, a numerical keypad, a touch panel, and the like.

10 The card reader-writer 14 is an interface (second interface) that communicates with the IC card 2. The card reader-writer 14 is configured by an interface corresponding to a predetermined communication protocol or the like of the IC card 2.

15 For example, if the IC card 2 is a contact IC card, the card reader-writer 14 is configured by a contact portion and the like for physically and electrically connecting to a contact portion of the IC card 2 in accordance with ISO/IEC 7816. For example, if the IC card 2
20 is a non-contact IC card, the card reader-writer 14 is configured by an antenna, a communication control unit, and the like for wirelessly communicating with the IC card 2 in accordance with ISO/IEC 14443.

25 If the IC card 2 is a dual card that supports both the contact type and the non-contact type, the card reader-writer 14 of the IC card processing apparatus 1 has a configuration corresponding to the dual card. That is, the

card reader-writer 14 is configured by a communication control unit and a contact unit for physically and electrically contacting the communication unit 25 of the IC card 2 to transmit and receive signals, and by an antenna and a communication control unit such as a modulation-demodulation circuit for wirelessly communicating with the communication unit 25 of the IC card 2.

The card reader-writer 14 also performs power supply, clock supply, reset control, and data transmission/reception for the IC card 2. For example, the card reader-writer 14 activates the IC card 2 based on the control of the CPU 11, transmits various commands, and receives responses to the transmitted commands.

The OCR 15 is an interface (external interface) for obtaining information from the IC card 2. Optically readable information such as a combination of characters, numerals, and symbols, a bar code, or a QR Code (registered trademark) is printed on the IC card 2, and the OCR 15 optically reads the information and outputs the read result to the CPU 11. For example, the CPU 11 generates a random number from an encrypted random number through a decryption process based on the read result.

With the card reader-writer 14 and the OCR 15, the IC card processing apparatus 1 obtains information from the IC card 2 via these two independent paths.

The storage unit 16 includes a nonvolatile memory and a volatile memory; the nonvolatile memory prestores a

control program, control data, and the like; the volatile memory temporarily stores data and the like that are being processed by the CPU 21, and functions as a reception buffer, a computation buffer, and a transmission buffer.

5 Next, the IC card 2 will be described.

 The IC card 2 is activated by receiving power or the like from a host apparatus such as the IC card processing apparatus 1, and becomes operable. For example, if the IC card 2 is connected to the IC card processing apparatus 1
10 via contact communication, that is, if the IC card 2 is configured by a contact IC card, the IC card 2 is activated by receiving an operation power supply and an operation clock from the IC card processing apparatus 1 via a contact unit as a communication interface.

15 If the IC card 2 is connected to the IC card processing apparatus 1 by a non-contact communication method, that is, if the IC card 2 is a non-contact IC card, the IC card 2 receives radio waves from the IC card processing apparatus 1 via an antenna, a modulation-
20 demodulation circuit, and the like as communication interfaces, generates an operation power supply and an operation clock from the radio waves via a power supply unit, and is activated.

 The IC card 2 includes a machine-readable zone (MRZ)
25 20 on one side or both sides of the card, and the MRZ includes optically readable print information such as a combination of characters, numerals, and symbols, a

barcode, or a QR code.

Next, an example of a configuration of the IC card 2 will be described.

FIG. 2 is a block diagram schematically showing an example of a configuration of the IC card according to the embodiment.

The IC card 2 has a card-shaped main body C formed of plastic or the like. The IC card 2 has a module M built in the main body C. The module M is formed integrally in a state where one or more IC chips Ca and an external interface for communication are connected to each other, and is embedded in the main body C of the IC card 2. As shown in FIG. 2, the module M of the IC card 2 includes a CPU 21, a ROM 22, a RAM 23, an NVM 24, and a communication unit 25. These units are connected to each other via a data bus.

The CPU 21 is a processor that functions as a control unit that controls the entire IC card 2. The CPU 21 performs various processes based on the control program and control data stored in the ROM 22 or the NVM 24. For example, the CPU 21 performs various processes corresponding to the operational control of the IC card 2 or the operational mode of the IC card 2 by executing the programs stored in the ROM 22. Some of the various functions may be implemented by a hardware circuit. In this case, the CPU 21 controls the functions implemented by a hardware circuit.

For example, the CPU 21 functions to read cryptographic information from the ROM 22 and transmit cryptographic information including a PQC cryptographic algorithm and a key length supported by the IC card 2 to the IC card processing apparatus 1 via the communication unit 25. The CPU 21 also functions to generate an encrypted random number from a random number through an encryption process based on a public key transmitted from the IC card processing apparatus 1. The CPU 21 also functions to transmit the encrypted random number to the IC card processing apparatus 1 via the communication unit 25. The CPU 21 also functions to generate a session key and the like based on a random number.

The ROM 22 is a nonvolatile memory that prestores a control program, control data, cryptographic information, identification information, and the like. The ROM 22 is incorporated into the IC card 2 in a manufacturing stage with a control program, control data, and the like being stored in the ROM 22. That is, the program, the control data, the cryptographic information, and the identification information stored in the ROM 22 are incorporated in advance in accordance with the specifications of the IC card 2. The ROM 22 may be configured by a flash memory, and writing may be performed in a manufacturing stage, or writing and rewriting can be performed in a subsequent phase. The information regarding cryptography can be written in a manufacturing stage, but may be written and

updated in a subsequent phase.

The cryptographic information includes a PQC
cryptographic algorithm and a key length supported by the
IC card 2. The identification information is unique
5 information that can identify the IC card 2. The MRZ 20
includes identification information as optically readable
print information such as a combination of characters,
numerals, and symbols, a barcode, or a QR code. The MRZ 20
may include all of the identification information or a
10 portion of the identification information. The MRZ 20 may
include the identification information in a form other than
printing. For example, if the identification information is
a combination of characters, numerals, and symbols, the MRZ
20 may include embossments corresponding to the
15 identification information.

The RAM 23 is a volatile memory. The RAM 23
temporarily stores data and the like that are being
processed by the CPU 21. For example, the RAM 23 includes a
reception buffer, a computation buffer, a transmission
20 buffer, and the like. The reception buffer holds data
transmitted from the IC card processing apparatus 1 and
received via the communication unit 25. The computation
buffer holds temporary results for the CPU 21 to perform
various computations. The transmission buffer holds data to
25 be transmitted to the IC card processing apparatus 1
through the communication unit 25.

The NVM 24 is configured by a nonvolatile memory on

which data may be written and rewritten, such as an EEPROM or a flash ROM. The NVM 24 stores a control program, an application, and various types of data in accordance with the operational use of the IC card 2. For example, a
5 program file, a data file, etc., are created in the NVM 24. A control program, various types of data, etc., are written in each of the files created. The NVM 24 may store cryptographic information and identification information.

The communication unit 25 communicates with the card
10 reader-writer 14 of the IC card processing apparatus 1, and is configured by an interface (first interface) corresponding to a predetermined communication protocol or the like. If the IC card 2 is realized as a contact IC card, the communication unit 25 is configured by a
15 communication control unit and a contact unit for transmitting and receiving signals by physically and electrically contacting the card reader-writer 14 of the IC card processing apparatus 1. If the IC card 2 is realized as a non-contact IC card, the communication unit 25 is
20 configured by an antenna and a communication control unit such as a modulation-demodulation circuit for wirelessly communicating with the card reader-writer 14 of the IC card processing apparatus 1.

If the IC card 2 is a dual card that supports both the
25 contact type and the non-contact type, the communication unit 25 is configured by a communication control unit and a contact unit for physically and electrically contacting the

card reader-writer 14 of the IC card processing apparatus 1
to transmit and receive signals, and by an antenna and a
communication control unit such as a modulation-
demodulation circuit for wirelessly communicating with the
5 card reader-writer 14 of the IC card processing apparatus
1.

A session-key sharing process according to the
embodiment will be described below.

In the IC card processing system according to the
10 embodiment, the IC card processing apparatus 1 newly
generates a public key and a secret key, which are a PQC's
key pair, each time based on a PQC cryptographic algorithm
and a key length transmitted from the IC card 2, and
transmits the public key to the IC card 2. This eliminates
15 the need to store a fixed key in the IC card 2, and can
suppress the consumption of the nonvolatile memory. The IC
card 2 generates a random number, generates an encrypted
random number from the random number through an encryption
process based on the received public key, and transmits the
20 encrypted random number to the IC card processing apparatus
1. The IC card 2 generates a session key from a random
number, the IC card processing apparatus 1 generates a
random number from an encrypted random number through a
decryption process based on a secret key, and generates a
25 session key from the random number, and the session key is
shared by the IC card processing apparatus 1 and the IC
card 2.

The IC card processing apparatus 1 may transmit information for generating a public key to the IC card 2, and the IC card 2 may generate a public key based on the received information. That is, the IC card processing
5 apparatus 1 is not necessarily limited to a method of transmitting a public key itself to the IC card 2, and may share a generated public key with the IC card 2.

Since the IC card processing apparatus 1 has greater hardware resources than the IC card 2, the IC card
10 processing apparatus 1 can support PQC as an information processing system by handling a process for generating a PQC's key pair. Also, the IC card 2 does not need to store a PQC's key pair in a fixed manner, reducing the load on the memory. Moreover, since a PQC's key pair is newly
15 generated every time, the risk of a secret key being identified can be reduced.

Next, the session-key sharing process according to the embodiment will be described in detail.

<Concept 1>

20 FIG. 3 is a diagram showing a first example of a session-key sharing process sequence according to the embodiment. The first example described here is a broader concept of a second example and the subsequent examples described later.

25 In order to encrypt communication between the IC card processing apparatus 1 and the IC card 2 using a session key, the CPU 21 of the IC card 2 reads cryptographic

information from the ROM 22. The cryptographic information includes a PQC cryptographic algorithm and a key length supported by the IC card 2. The CPU 21 executes control such that the read cryptographic information is transmitted
5 to the IC card processing apparatus 1; the communication unit 25 transmits the cryptographic information to the IC card processing apparatus 1 (ST 101).

The card reader-writer 14 of the IC card processing apparatus 1 receives the cryptographic information. The CPU
10 11 generates a public key and a secret key based on a PQC cryptographic algorithm and a key length included in the received cryptographic information. That is, the CPU 11 generates a public key and a secret key as a PQC's key pair of a PQC cryptographic algorithm and a key length included
15 in the received cryptographic information (ST 102).

The CPU 11 executes control such that the public key is transmitted to the IC card 2; the card reader-writer 14 transmits the public key to the IC card 2 (ST 103).

The communication unit 25 receives the public key
20 transmitted from the IC card processing apparatus 1, and the CPU 21 obtains the received public key.

The CPU 21 generates a random number and generates an encrypted random number from the random number through an encryption process based on the obtained public key. For
25 example, the CPU 21 generates an encrypted random number from a random number through an encryption process based on the public key (ST 104). Alternatively, the CPU 21

generates an encrypted random number from a random number and identification information through an encryption process based on the public key.

5 The CPU 21 executes control such that the encrypted random number is transmitted to the IC card processing apparatus 1 via the communication unit 25; the communication unit 25 transmits the encrypted random number to the IC card processing apparatus 1 (ST 105).

10 The CPU 21 generates a session key based on the random number (ST 106). The CPU 21 encrypts data to be transmitted in the subsequent process with the session key, and the communication unit 25 transmits the data encrypted with the session key.

15 The card reader-writer 14 of the IC card processing apparatus 1 receives the encrypted random number. The CPU 11 generates a random number from the encrypted random number through a decryption process based on the secret key (ST 107). Alternatively, the CPU 11 generates a random number and identification information from the encrypted random number through a decryption process based on the secret key.

20 The CPU 11 generates a session key based on the random number (ST 108). The CPU 11 encrypts data to be transmitted in the subsequent process with the session key, and the card reader-writer 14 transmits the data encrypted with the session key.

For example, the IC card 2 encrypts data received from

the IC card processing apparatus 1 with the session key,
and transmits the encrypted data to the IC card processing
apparatus 1. The IC card processing apparatus 1 encrypts
data received from the IC card 2 with the session key, and
5 transmits the encrypted data to the IC card 2. The IC card
2 and the IC card processing apparatus 1 verify whether or
not the session key is correctly generated based on the
received encrypted data.

The above process produces the following effects.

10 PQC includes multiple schemes as standard. Different
schemes may be implemented depending on the issuer of the
IC card 2 (e.g., a country that issued an e-passport). The
information processing system can handle the differences in
e-passport schemes via the PQC cryptographic algorithm and
15 key length included in the cryptographic information
transmitted from the IC card 2.

By using a public key as a single-use key, the
information processing system eliminates concerns about
long-term use of a fixed key.

20 <Concept 2-1>

FIG. 4 is a diagram showing a second example of a
session-key sharing process sequence according to the
embodiment. The second example described here is a narrower
concept of the first example described above. Mainly the
25 different parts will be described, and description of
common parts will be omitted as appropriate.

An operator of the IC card processing apparatus 1

holds a read unit of the OCR 15 over the MRZ 20 of the IC
card 2 or holds the MRZ 20 of the IC card 2 over the read
unit of the OCR 15. Thus, the OCR 15 reads identification
information from the MRZ 20 of the IC card 2. The CPU 11
5 obtains the read identification information (ST 201). In
FIG. 4, the identification information read from the MRZ 20
and the identification information read from the ROM 22 are
denoted by MRZ.

The CPU 21 of the IC card 2 reads cryptographic
10 information from the ROM 22 and executes control such that
the read cryptographic information is transmitted to the IC
card processing apparatus 1; the communication unit 25
transmits the cryptographic information to the IC card
processing apparatus 1 (ST 202).

15 The card reader-writer 14 of the IC card processing
apparatus 1 receives the cryptographic information.

The CPU 21 generates a first random number (RND) (ST
203), reads identification information (MRZ) from the ROM
22, and encrypts the first random number with the
20 identification information (MRZ) (E (RND, MRZ)). That is,
the CPU 21 generates a first encrypted random number from
the first random number through an encryption process based
on the read identification information (MRZ) (ST 204).

The CPU 21 executes control such that the generated
25 first encrypted random number (Encrypted RND) is
transmitted to the IC card processing apparatus 1; the
communication unit 25 transmits the first encrypted random

number to the IC card processing apparatus 1 (ST 205).

The card reader-writer 14 receives the first encrypted random number.

5 The CPU 11 decrypts the first encrypted random number obtained via the card reader-writer 14 with the identification information (MRZ) obtained from the IC card 2 via the OCR 15 (D (RND, MRZ)). That is, the CPU 11 generates a first random number from the first encrypted random number through a decryption process based on the
10 obtained identification information (MRZ) (ST 206).

The CPU 11 generates a public key and a secret key based on a PQC cryptographic algorithm and a key length included in the received cryptographic information. That is, the CPU 11 generates a public key and a secret key as a
15 PQC's key pair of the PQC cryptographic algorithm and the key length included in the received cryptographic information (ST 207).

The CPU 11 executes control such that the public key is transmitted to the IC card 2; the card reader-writer 14
20 transmits the public key to the IC card 2 (ST 209).

The communication unit 25 receives the public key transmitted from the IC card processing apparatus 1, and the CPU 21 obtains the received public key.

The CPU 21 generates a second random number, and
25 generates a second encrypted random number from the second random number through an encryption process based on the obtained public key (ST 211).

The CPU 21 executes control such that the second encrypted random number is transmitted to the IC card processing apparatus 1 via the communication unit 25; the communication unit 25 transmits the second encrypted random number to the IC card processing apparatus 1 (ST 212).

The CPU 21 generates a session key based on the first and second random numbers (ST 213). The CPU 21 encrypts data to be transmitted in the subsequent process with the session key, and the communication unit 25 transmits the data encrypted with the session key.

The CPU 21 generates an encrypted MRZ (authentication data) from the MRZ through an encryption process based on the second random number (ST 214).

The card reader-writer 14 receives the second encrypted random number. The CPU 11 generates a second random number from the second encrypted random number through a decryption process based on the secret key (ST 215).

The CPU 11 generates a session key based on the first and second random numbers (ST 216). The CPU 11 encrypts data to be transmitted in the subsequent process with the session key, and the card reader-writer 14 transmits the data encrypted with the session key.

The CPU 21 generates an encrypted MRZ (authentication data) from the MRZ through an encryption process based on the second random number (ST 217).

The above process produces the following effects.

According to the information processing system, by combining the identification information read via the OCR 15 with the cryptographic information read via the card reader-writer 14, the final session key can be protected if either piece of information is secure.

Also, by making the public key disposable, the information processing system ensures security, even if an attack on the public key is detected, until the moment the public key would be instantaneously decrypted before the session is established.

<Concept 2-2>

FIG. 5 is a diagram showing a third example of a session-key sharing process sequence according to the embodiment. The third example described here is a modification of the second example described above. Mainly the different parts will be described, and description of common parts will be omitted as appropriate.

As described in the second example, the steps ST 201 through ST 207 are performed, and the CPU 11 generates an encrypted public key (Encrypted Pub Key) from the public key through an encryption process based on the first random number (ST 208a). For example, the CPU 11 uses an advanced encryption standard (AES) to encrypt the public key using the first random number as a key.

The CPU 11 executes control such that the encrypted public key is transmitted to the IC card 2; the card reader-writer 14 transmits the public key to the IC card 2

(ST 209).

The communication unit 25 receives the encrypted public key transmitted from the IC card processing apparatus 1, and the CPU 21 obtains the received encrypted public key.

The CPU 21 generates a public key from the encrypted public key through a decryption process based on the first random number (ST 210a). For example, the CPU 21 uses the AES to take out the public key from the encrypted public key using the first random number as a key.

The CPU 21 generates a second random number, and generates a second encrypted random number from the second random number through an encryption process based on the obtained public key (ST 211).

The CPU 21 executes control such that the second encrypted random number is transmitted to the IC card processing apparatus 1 via the communication unit 25; the communication unit 25 transmits the second encrypted random number to the IC card processing apparatus 1 (ST 212).

The CPU 21 generates a session key based on the first and second random numbers (ST 213). The CPU 21 encrypts data to be transmitted in the subsequent process with the session key, and the communication unit 25 transmits the data encrypted with the session key.

The CPU 21 generates an encrypted MRZ (authentication data) from the MRZ through an encryption process based on the second random number (ST 214).

The card reader-writer 14 receives the second encrypted random number. The CPU 11 generates a second random number from the second encrypted random number through a decryption process based on the secret key (ST 215).

The CPU 11 generates a session key based on the first and second random numbers (ST 216). The CPU 11 encrypts data to be transmitted in the subsequent process with the session key, and the card reader-writer 14 transmits the data encrypted with the session key.

The CPU 21 generates an encrypted MRZ (authentication data) from the MRZ through an encryption process based on the second random number (ST 217).

The above process produces the following effects.

Unless the first encrypted random number is decrypted, a third party cannot know the public key encrypted with the first random number. Accordingly, the information processing system can enhance security by not providing any clues for decryption.

<Concept 2-3>

FIG. 6 is a diagram showing a fourth example of a session-key sharing process sequence according to the embodiment. Here, the fourth example is a modification of the third example described above. Mainly the different parts will be described, and description of common parts will be omitted as appropriate.

As described in the second example, the steps ST 201

through ST 207 are performed, and the CPU 11 generates an encrypted public key from the public key through an encryption process based on the MRZ (ST 208b).

5 The CPU 11 executes control such that the encrypted public key is transmitted to the IC card 2; the card reader-writer 14 transmits the public key to the IC card 2 (ST 209).

10 The communication unit 25 receives the encrypted public key transmitted from the IC card processing apparatus 1, and the CPU 21 obtains the received encrypted public key.

 The CPU 21 generates a public key from the encrypted public key through a decryption process based on the MRZ (ST 210b).

15 Thereafter, the steps ST 212 through ST 217 are performed as described in the second example.

 <Concept 3-1>

20 FIG. 7 is a diagram showing a fifth example of a session-key sharing process sequence according to the embodiment. Here, the fifth example is a modification of the second to fourth examples described above. Mainly the different parts will be described, and description of common parts will be omitted as appropriate.

25 In the fifth example, a PQC standard (Kyber) is used. FIG. 9 is an illustration of Algorithm 1 of a PQC standard (Kyber); FIG. 10 is an illustration of Algorithm 2 of a PQC standard (Kyber).

Since PQC has a large data (public key) size, the data communication amount and the computing time increase. Thus, in the fifth example, seed information for generating a public key is shared in advance to reduce the amount of communication, and the IC card processing apparatus 1 performs computation in advance to generate a portion of the public key. That is, the storage unit 16 of the IC card processing apparatus 1 stores some or all of the PQC standard, which is seed information for generating a public key, and the ROM 22 or the NVM 24 of the IC card 2 stores some or all of the PQC standard.

As illustrated in FIG. 7, an operator of the IC card processing apparatus 1 holds a read unit of the OCR 15 over the MRZ 20 of the IC card 2 or holds the MRZ 20 of the IC card 2 over the read unit of the OCR 15. Thus, the OCR 15 reads identification information from the MRZ 20 of the IC card 2. The CPU 11 obtains the read identification information (ST 301). In FIG. 7, the identification information read from the MRZ 20 and the identification information read from the ROM 22 are denoted by MRZ.

The CPU 21 generates a first random number (RND) (ST 302), reads identification information (MRZ) from the ROM 22, and encrypts the first random number with the identification information (MRZ) (E (RND, MRZ)). That is, the CPU 21 generates a first encrypted random number from the first random number through an encryption process based on the read identification information (MRZ) (ST 303).

The CPU 21 executes control such that the generated first encrypted random number is transmitted to the IC card processing apparatus 1; the communication unit 25 transmits the first encrypted random number to the IC card processing apparatus 1 (ST 304).

The card reader-writer 14 receives the first encrypted random number.

The CPU 11 decrypts the first encrypted random number obtained via the card reader-writer 14 with the identification information (MRZ) obtained from the IC card 2 via the OCR 15 (D (RND, MRZ)). That is, the CPU 11 generates a first random number from the first encrypted random number through a decryption process based on the obtained identification information (MRZ) (ST 305).

The CPU 11 generates a public key ($pk = (t, \rho)$) and a secret key ($sk = s$), which are a Kyber's key pair, based on a PQC standard ($RND = \rho$ (a part of the Kyber's public key and a source of the generation of a matrix A)) stored in the storage unit 16 (ST 306).

The CPU 11 sets t in plaintext (a part of the public key) (ST 307) and executes control such that t is transmitted to the IC card 2; the card reader-writer 14 transmits t to the IC card 2 (ST 308). Alternatively, the CPU 11 encrypts t (ST 307) and executes control such that encrypted t is transmitted to the IC card 2; the card reader-writer 14 transmits encrypted t to the IC card 2 (ST 308).

The communication unit 25 receives t transmitted from the IC card processing apparatus 1 or encrypted t , and the CPU 21 obtains the received t or the encrypted t .

5 If the CPU 21 obtains the encrypted t based on the PQC standard ($RND = \rho$ (a part of the Kyber's public key and a source of the generation of a matrix A)) stored in the ROM 22 or the NVM 22, it decrypts t from the encrypted t (ST 309).

10 The CPU 21 generates a second random number, and generates a second encrypted random number from the second random number through an encryption process based on the public key (ST 310).

15 The CPU 21 executes control such that the second encrypted random number is transmitted to the IC card processing apparatus 1 via the communication unit 25; the communication unit 25 transmits the second encrypted random number to the IC card processing apparatus 1 (ST 311).

20 The CPU 21 generates a session key based on the first and second random numbers (ST 312). The CPU 21 encrypts data to be transmitted in the subsequent process with the session key, and the communication unit 25 transmits the data encrypted with the session key.

25 The CPU 21 generates an encrypted MRZ (authentication data) from the MRZ through an encryption process based on the second random number (ST 313A).

The card reader-writer 14 receives the second encrypted random number. The CPU 11 generates a second

random number from the second encrypted random number through a decryption process based on the secret key ($sk = s$) (ST 314).

5 The CPU 11 generates a session key based on the first and second random numbers (ST 315). The CPU 11 encrypts data to be transmitted in the subsequent process with the session key, and the card reader-writer 14 transmits the data encrypted with the session key.

10 The CPU 21 generates an encrypted MRZ (authentication data) from the MRZ through an encryption process based on the second random number (ST 316A).

The above process produces the following effects.

15 According to the information processing system, as with the introduction of the first encrypted random number, a third party cannot know ρ , which is a part of the public key. Accordingly, the information processing system can enhance security by not providing any clue for decryption. Further, since there is no need to transmit or receive ρ , which is a part of the public key, the information
20 processing system can reduce the data size of communication. After transmitting the first encrypted random number ($RND = \rho$) to the reader, the IC card 2 can generate ciphertext in advance using ρ during the waiting time.

25 <Concept 3-2>

FIG. 8 is a diagram showing a sixth example of a session-key sharing process sequence according to the

embodiment. Here, the sixth example is a modification of the fifth example described above. Mainly the different parts will be described, and description of common parts will be omitted as appropriate.

5 As described in the fifth example, the steps ST 301 through ST 312, ST 314, and ST 315 are performed.

 On the other hand, the CPU 21 generates an encrypted MRZ (first authentication data) from the MRZ through an encryption process based on the second random number (ST
10 316B).

 The card reader-writer 14 transmits the first authentication data to the IC card 2 (ST 317).

 The CPU 21 generates an encrypted public key (second authentication data) from the public key through an
15 encryption process based on the second random number (ST 313B).

 The communication unit 25 transmits the second authentication data to the IC card processing apparatus 1 (ST 318).

20 The information processing system according to the first to fifth examples described above can provide a portable electronic device, an information processing apparatus, an information processing system, and an information processing method that enable installation of
25 PQC with limited hardware resources.

 Variations relating to the public key include the following:

- (1) The IC card processing apparatus 1 transmits a public key in plaintext.
- (2) The IC card processing apparatus 1 encrypts a public key with a first random number and transmits the encrypted public key.
5
- (3) The IC card processing apparatus 1 encrypts a public key with the identification information read from the MRZ 20 and transmits the encrypted public key.
- (4) The IC card processing apparatus 1 generates ρ ,
10 generates t from ρ , and transmits t in plaintext.
- (5) The IC card processing apparatus 1 generates ρ , generates t from ρ , encrypts t , and transmits the encrypted t .
- (6) The IC card 2 generates ρ and a first random number,
15 and transmits both ρ and the first random number. The IC card processing apparatus 1 generates t from ρ .
- (7) The IC card 2 generates ρ , sets ρ as a first random number, and transmits ρ . The IC card processing apparatus 1 generates t from ρ .
- (8) The IC card 2 hashes a first random number to obtain ρ
20 rather than converting the first random number to ρ .
- (9) The IC card processing apparatus 1 and the IC card 2 use a second random number as a session key.
- (10) The IC card processing apparatus 1 and the IC card 2
25 generate a session key from an exclusive OR (XOR) of a first random number and a second random number.

Variations of a session key confirmation means include

the following:

(1) The IC card processing apparatus 1 and the IC card 2 exchange authentication data in which the identification information read from the MRZ 20 is encrypted with a second random number, and thereby verify a session key.

(2) The IC card processing apparatus 1 and the IC card 2 encrypt the identification information read from the MRZ 20 with a result of performing an exclusive OR on a first random number and a second random number, and thereby verify a session key.

Variations of the presentation of a cryptographic algorithm and a key length include the following:

(1) The IC card 2 presents cryptographic information including a cryptographic algorithm and a key length together with the MRZ 20. For example, the MRZ 20 is optically read via the OCR 15 of the IC card processing apparatus 1, and cryptographic information is received via the card reader-writer 14 of the IC card processing apparatus 1.

(2) The IC card 2 presents cryptographic information including a cryptographic algorithm and a key length together with a first random number. For example, the IC card 2 encrypts information including a first random number and cryptographic information and presents the encrypted information.

(3) The IC card 2 presents cryptographic information including a cryptographic algorithm and a key length in

plaintext separately from a first random number.

The case where the IC card processing apparatus 1 obtains identification information via the OCR 15 is described above; however, the embodiment is not limited thereto. For example, the communication unit 25 of the IC card 2 may transmit the identification information stored in the ROM 22 or the like, and the card reader-writer 14 of the IC card processing apparatus 1 may receive the identification information transmitted from the IC card 2. In this case, the CPU 21 of the IC card 2 may realize transmission and reception of an encrypted random number and plaintext or an encrypted key and transmission of identification information by using different communication methods (contact communication and non-contact communication).

For example, the communication unit 25 of the IC card 2 transmits and receives an encrypted random number and plaintext or an encrypted key through contact communication (a communication control unit and a contact unit for transmitting and receiving signals via physical and electrical contact), and transmits identification information through non-contact communication (an antenna and a communication control unit such as a modulation-demodulation circuit for performing wireless communication). The card reader-writer 14 of the IC card processing apparatus 1 transmits and receives an encrypted random number and plaintext or an encrypted key through

contact communication, and receives identification information through non-contact communication.

Alternatively, the communication unit 25 of the IC card 2 transmits identification information through contact communication, and transmits and receives an encrypted random number and plaintext or an encrypted key through non-contact communication. The card reader-writer 14 of the IC card processing apparatus 1 receives identification information through contact communication, and transmits and receives an encrypted random number and plaintext or an encrypted key through non-contact communication.

As described above, the information processing system according to the embodiment realizes transmission and reception of a random number and a key and transmission and reception of identification information via different communication methods. This can significantly reduce the risk of a random number and a key and identification information being stolen simultaneously, and can improve security.

The program according to the present embodiment may be transferred in a state of being stored in electronic devices such as the IC card processing apparatus 1, the IC card 2, and the like or in a state of not being stored in the electronic devices. In the latter case, the program may be transferred through a network or may be transferred in a state of being stored in a storage medium. The storage medium is a non-transitory tangible medium. The storage

medium is a computer-readable medium. The storage medium may be of any type, such as an optical disc or a memory card, as long as it can store programs and can be read by a computer. The electronic devices download a program
5 transferred (provided) via a network and install the program in a memory, or read a program from a storage medium and install the program in a memory.

While several embodiments have been described, these embodiments have been presented by way of example and are
10 not intended to limit the scope of the invention. The novel embodiments described herein can be implemented in a variety of other forms; furthermore, various omissions, substitutions, and changes can be made without departing from the spirit of the invention. The accompanying claims
15 and their equivalents are intended to cover such embodiments or modifications as would fall within the scope and spirit of the inventions.

CLAIMS

1. A portable electronic device comprising:
a memory storing cryptographic information including a
5 cryptographic algorithm;
an interface configured to communicate with an
information processing apparatus; and
a processor configured to generate a random number,
wherein
10 the interface is configured to transmit the
cryptographic information to the information processing
apparatus and receive a public key transmitted from the
information processing apparatus, the public key and a
secret key being generated based on the cryptographic
15 algorithm,
the processor is configured to generate an encrypted
random number from the random number through an encryption
process based on the public key,
the interface is configured to transmit the encrypted
20 random number to the information processing apparatus, and
the processor is configured to generate a session key
for use for communication with the information processing
apparatus based on the random number.
- 25 2. The portable electronic device according to
claim 1, wherein the cryptographic algorithm is a
cryptographic algorithm using post quantum cryptography.

3. The portable electronic device according to
claim 1, wherein the interface is configured to transmit
the encrypted random number to the information processing
5 apparatus in order to cause the information processing
apparatus to generate the random number from the encrypted
random number through a decryption process based on the
secret key and generate the session key for use for
communication with the portable electronic device based on
10 the random number.

4. The portable electronic device according to
claim 1, wherein
the cryptographic information includes a key length,
15 and
the public key and the secret key are generated based
on the cryptographic algorithm and the key length included
in the cryptographic information.

20 5. The portable electronic device according to
claim 1, wherein
the memory stores identification information that
allows identification of the portable electronic device,
the processor is configured to generate a first random
25 number and generate a first encrypted random number from
the first random number through an encryption process based
on the identification information,

the interface is configured to transmit the first encrypted random number to the information processing apparatus and receive the public key transmitted from the information processing apparatus,

5 the processor is configured to generate a second random number and generate a second encrypted random number from the second random number through an encryption process based on the public key,

10 the interface is configured to transmit the second encrypted random number to the information processing apparatus, and

the processor is configured to generate the session key based on the first and second random numbers.

15 6. The portable electronic device according to claim 5, wherein the interface is configured to transmit the first and second encrypted random numbers to the information processing apparatus in order to cause the information processing apparatus to generate the first
20 random number from the first encrypted random number through a decryption process based on the identification information obtained from the portable electronic device, generate the second random number from the second encrypted random number through a decryption process based on the
25 secret key, and generate the session key based on the first and second random numbers.

7. The portable electronic device according to claim 5, wherein

the information processing apparatus is configured to generate an encrypted public key from the public key
5 through an encryption process based on the first random number and transmit the encrypted public key in place of the public key,

the interface is configured to receive the encrypted public key transmitted from the information processing
10 apparatus, and

the processor is configured to generate the public key from the encrypted public key through a decryption process based on the first random number.

15 8. The portable electronic device according to claim 5, comprising a readable zone on which the identification information is printed,

wherein the information processing apparatus is configured to obtain the identification information from
20 the readable zone via an optically readable external interface and generate the first random number from the first encrypted random number through a decryption process based on the identification information.

25 9. The portable electronic device according to claim 5, wherein

the interface is an interface for communicating with

the information processing apparatus in a contact or non-contact manner based on a predetermined communication protocol,

the processor is configured to transmit the
5 identification information to the information processing apparatus via the interface, and

the information processing apparatus is configured to obtain the identification information via the interface and generate the first random number from the first encrypted
10 random number through a decryption process based on the identification information.

10. The portable electronic device according to claim 9, wherein

15 the interface is configured to:

transmit the identification information to the information processing apparatus through contact communication, and

through non-contact communication, transmit the
20 first encrypted random number to the information processing apparatus, receive the public key transmitted from the information processing apparatus, and transmit the second encrypted random number to the information processing apparatus; or

25 transmit the identification information to the information processing apparatus through the non-contact communication, and

through the contact communication, transmit the first encrypted random number to the information processing apparatus, receive the public key transmitted from the information processing apparatus, and transmit the second encrypted random number to the information processing apparatus.

11. An information processing apparatus comprising:
an interface for communicating with a portable electronic device; and
a processor configured to generate a key,
wherein
the interface is configured to receive cryptographic information transmitted from the portable electronic device,
the processor is configured to generate a public key and a secret key based on a cryptographic algorithm included in the cryptographic information,
the interface is configured to transmit the public key to the portable electronic device and receive an encrypted random number generated from a random number through an encryption process based on the public key in the portable electronic device, and
the processor is configured to generate the random number from the encrypted random number through a decryption process based on the secret key and generate a session key for use for communication with the portable

electronic device based on the random number.

12. An information processing system comprising a portable electronic device and an information processing apparatus, wherein

the portable electronic device comprises:

a memory storing cryptographic information including a cryptographic algorithm;

a first interface configured to communicate with the information processing apparatus; and

a processor configured to generate a random number,

the first interface being configured to transmit the cryptographic information to the information processing apparatus and receive a public key transmitted from the information processing apparatus, the public key and a secret key being generated based on the cryptographic algorithm,

the processor being configured to generate an encrypted random number from the random number through an encryption process based on the public key,

the first interface being configured to transmit the encrypted random number to the information processing apparatus,

the processor being configured to generate a session key for use for communication with the information processing apparatus based on the random number, and

the information processing apparatus includes:

a second interface for communicating with the portable electronic device; and

5 a second processor configured to generate a key, the second interface being configured to receive the cryptographic information transmitted from the portable electronic device,

the second processor being configured to generate the public key and the secret key based on the
10 cryptographic algorithm included in the cryptographic information,

the second interface being configured to transmit the public key to the portable electronic device and receive the encrypted random number generated from the
15 random number through an encryption process based on the public key in the portable electronic device,

the second processor being configured to generate the random number from the encrypted random number through a decryption process based on the secret key and generate
20 the session key for use for communication with the portable electronic device based on the random number.

13. An information processing method performed by a portable electronic device and an information processing
25 apparatus, the method comprising:

the portable electronic device transmitting cryptographic information including a cryptographic

algorithm to the information processing apparatus;

the information processing apparatus receiving the cryptographic information transmitted from the portable electronic device, generating a public key and a secret key
5 based on the cryptographic algorithm included in the cryptographic information, and transmitting the public key to the portable electronic device;

the portable electronic device receiving the public key transmitted from the information processing apparatus,
10 generating an encrypted random number from a random number through an encryption process based on the public key, transmitting the encrypted random number to the information processing apparatus, and generating a session key for use for communication with the information processing apparatus
15 based on the random number; and

the information processing apparatus receiving the encrypted random number transmitted from the portable electronic device, generating the random number from the encrypted random number through a decryption process based
20 on the secret key, and generating the session key for use for communication with the portable electronic device based on the random number.