



CERTIFIED SHUFFLE-DECRYPTING SYSTEM,
CERTIFIED SHUFFLE-DECRYPTING METHOD
AND
CERTIFIED SHUFFLE-DECRYPTION VERIFYING METHOD

FIELD OF THE INVENTION

The present invention relates to a certified shuffle-decrypting system, a certified shuffle-decrypting method and a certified shuffle-decryption verifying method, for performing certified shuffling and certified decryption which are employed, for example, in configurations such as an anonymous communication channel.



159159

BACKGROUND OF THE INVENTION

[Conventional Certified Shuffling]

A conventional certified shuffling technique is described, for example, in Japanese Patent Application No. 2000-059091 (Japanese Patent Laid-Open Application No. 2001-251289) (hereinafter, referred to as "Document 1").

Figure 6 is a block diagram showing a configuration of the conventional technique described in Document 1. In each of the accompanying drawings, a joining arrow means that pieces of information at the roots of the arrow are sent together to the tip of the joining arrow, while a branched arrow means that at least part of the information at the root of the arrow is sent to the tips of the branched arrow.

The term "shuffling" used herein is referred to as "re-

encryption shuffling" in Document 1. Herein, "shuffling" means to shuffle the order of the input encrypted texts and to re-encrypt them.

Referring to Figure 6, first, encrypted texts/public keys 100 are input to be shuffled at the shuffling step 101. At this point, the input encrypted texts and shuffling information 102 specifying the shuffling are sent to the identical conversion certifying step 103 as well as to the substitution certifying step 104. The identical conversion certifying step 103 generates and outputs identical conversion certificates 105, and sends random numbers 106 used for generating the certificates 105 to the substitution certifying step 104. The substitution certifying step 104 outputs substitution certificates 107. The identical conversion certificates 105, the substitution certificates 107, the encrypted texts/public keys 100, and shuffled encrypted texts 109 are input to the response generating step 108, where responses are added to the identical conversion certificates 105, the substitution certificates 107 and the encrypted texts to generate and output shuffling certificates 110.

The identical conversion certificates 105 together with the responses prove that they have the knowledge of the order of the shuffled input texts and the content of conversion for encryption, and, when the input encrypted texts each contain multiple integer elements, prove that the elements of each

encrypted text are shuffled in the same order and received are subjected to corresponding encryption. The substitution certificates 107 together with the responses prove that the shuffling order of the input encrypted texts is correct.

In order to prove that this shuffling process is correct, two certificating steps, namely the identical conversion certificating step and the substitution certificating step, are employed in Document 1. Document 1 achieves efficient generation of shuffling certificates by separating the processed subjects of the certifying step.

[Conventional certified decryption]

A conventional technique for certified decryption is disclosed, for example, in Japanese Patent Application No. 08-263575 (Japanese Patent No. 3003771) (hereinafter, referred to as "Document 2").

Figure 7 is a block diagram showing a configuration of the conventional technique disclosed in Document 2. Referring to Figure 7, shuffled encrypted texts 200 and secret keys 201 are first input into the decrypting step 203 for decryption. Then, the input shuffled encrypted texts 200, the secret keys 201 and the decrypted texts 204 are sent to the decryption certifying step 205. Based on these information, the decryption certifying step 205 outputs decryption certificates 206.

Herein, "decryption" means to partially decrypt the encrypted texts by using at least one of the secret keys that

are kept separately from each other. By repeating such partial decryption by using all of the secret keys, the encrypted texts can be decrypted completely.

[Certified Shuffle-decrypting Method According to Prior Art]

The certified shuffling technique of Document 1 and the certified decrypting technique of Document 2 can be combined to obtain a certified shuffle-decrypting method.

Figure 8 is a block diagram for illustrating the certified shuffle-decrypting method by simply combining the conventional techniques of Documents 1 and 2. This method is characterized in that shuffled encrypted texts 404 are contained in shuffle-decryption certificates 416, that the shuffled encrypted texts 404 are input into decryption certifying step 417 and that no data is transformed from the response generating step to the decryption certifying step.

However, this conventional technique has the following problems.

Assume a system in which the encrypted texts are input to be shuffled and decrypted to give decrypted texts, and then validation certificates for the shuffling/decrypting process are generated and output. Although an anonymous communication channel can be configured by combining the conventional techniques of Documents 1 and 2 as described above, this method requires unnecessary shuffled encrypted texts to be output to prove validation. When there are a

number of encrypted texts, outputting unnecessary shuffled encrypted texts adversely increases the amount of certificates and deteriorates communication efficiency.

According to the conventional technique of Document 2, modular exponentiations accompanied by a large amount of calculation proportional to the number of the encrypted texts have to be carried out for generating the certificates. This adversely affects efficiency of the shuffle-decryption.

In view of the drawbacks of the above-described conventional techniques, a first objective of the present invention is to combine the techniques of Documents 1 and 2 to provide a certified shuffle-decrypting system, a certified shuffle-decrypting method and a shuffle-decryption verifying method, which are efficient since there is no need of outputting shuffled encrypted texts and thus an amount of calculation as well as an amount of certificates are minimized.

In view of the drawbacks of the above-described conventional techniques, a second objective of the present invention is to provide a certified shuffle-decrypting system, a certified shuffle-decrypting method and a shuffle-decryption verifying method, which can realize further high-speed processing by greatly decreasing the number of modular exponentiations and an amount of calculation.

SUMMARY OF THE INVENTION

In order to achieve the above-described objectives, one aspect of the present invention is a certified shuffle-decryption device of the invention for shuffle-decrypting multiple encrypted texts to generate shuffle-decrypting texts and for generating shuffle-decryption certificates for certifying that the shuffle-decryption has correctly taken place, in which: the order of the encrypted texts is shuffled and encrypted with public keys to obtain shuffled encrypted texts, which are then decrypted with secret keys to obtain the shuffle-decrypting texts; responses are generated as references for certifications; based on the responses, certificates certifying validity of the shuffling of order, the encryption and the decryption for obtaining the shuffle-decrypting texts are generated; and the generated certificates and the response are output as shuffle-decryption certificates.

Moreover, the certified shuffle-decryption device of the present invention comprises: a shuffling unit into which the multiple encrypted texts and the public keys are input and which shuffles the order of the multiple encrypted texts and encrypts them with the public keys, thereby generating multiple shuffled encrypted texts; a decrypting unit into which the multiple shuffled encrypted texts and the secret keys are input and which decrypts the shuffled encrypted texts with the secret keys, thereby generating multiple shuffle-decrypting texts; and a certifying unit into which the multiple encrypted texts, the public keys and the secret keys

are input and which generates the shuffle-decryption certificates.

Moreover, in the certified shuffle-decryption device of the present invention, the certifying unit comprises: an identical conversion certifying unit for generating a certificate certifying that it knows the ordering relationship among the encrypted texts before and after the shuffling as well as random numbers used for encryption are known, and, when each of the input encrypted texts consists of multiple integer elements, that it knows that the elements of each encrypted text have been shuffled in the same order with the same random numbers; a substitution certifying unit for generating a certificate certifying that the input encrypted texts have been correctly shuffled; a response generating unit for generating responses for the identical conversion certifying unit and the substitution certifying unit; and a decryption certifying unit for generating, based on the responses, a certificate certifying that the shuffle-decrypted texts are obtained through correct decryption of the shuffled encrypted texts using the secret keys. All of the certificates generated by the identical conversion certifying unit, the substitution certifying unit and the decryption certifying unit as well as the responses generated by the response generating unit are output as the shuffle-decryption certificates.

Another aspect of the invention is a shuffle-decryption verification device, of the present invention, for verifying whether or not shuffle-decryption of multiple encrypted texts

has taken place correctly by referring to shuffle-decryption certificates certifying that the shuffle-decryption has taken place correctly, where the shuffle-decryption certificates comprise: responses as references upon certification; and certificates, generated based on the responses, certifying that the shuffled encrypted texts, obtained by shuffling the order of the encrypted texts and encrypting them with public keys, have correctly been decrypted with the secret keys to give the shuffle-decrypted texts.

Moreover, the shuffle-decryption verification device of the invention comprises: an identical conversion verifying unit into which the shuffle-decryption certificates, the encrypted texts, the public keys and the shuffle-decrypted texts are input, and which verifies whether or not a generator of the certificates has information of the shuffling order and the content of conversion of the encrypted texts, generates challenge values, and, when each of the input encrypted texts consists of a plurality of integer elements, verifies whether or not the elements of each encrypted text have been shuffled in the same order and converted with the same random numbers so as the whole conversion to encryptions; a substitution verifying unit into which the shuffle-decryption certificates and the challenge values generated by the identical conversion verifying unit are input, and which verifies whether or not the encrypted texts has been correctly shuffled; and a decryption verifying unit into which the shuffle-decryption certificates and the challenge values generated by the identical conversion

verifying unit are input, and which verifies whether or not the shuffled encrypted texts have been correctly decrypted using the secret keys to give shuffle-decrypted texts. Only when judged "valid" in all of the identical conversion verifying unit, the substitution verifying unit and the decryption verifying unit, the encrypted texts are judged to have been shuffle-decrypted correctly.

Yet another aspect of the invention is a certified shuffle-decrypting method of the invention for shuffle-decrypting multiple encrypted texts to generate shuffle-decrypted texts and for generating shuffle-decryption certificates for certifying that the shuffle-decryption has correctly taken place, where: the order of the encrypted texts is shuffled and encrypted with public keys to obtain shuffled encrypted texts, which are then decrypted with secret keys to obtain the shuffle-decrypted texts; responses are generated as references for certifications; based on the response, certificates certifying validity of the shuffling of order, the encryption and the decryption for obtaining the shuffle-decrypted texts are generated; and the generated certificates and the response are output as shuffle-decryption certificates.

The certified shuffle-decrypting method of the invention, comprises the steps of: based on the inputs of the multiple encrypted texts and the public keys, shuffling the order of the multiple encrypted texts and encrypting them with the public keys, thereby generating multiple shuffled encrypted texts; based on the inputs of the multiple shuffled

encrypted texts and the secret keys, decrypting the shuffled encrypted texts with the secret keys, thereby generating multiple shuffle-decrypted texts; and based on the inputs of the multiple encrypted texts, the public keys and the secret keys, generating the shuffle-decryption certificates.

In the certified shuffle-decrypting method of the present invention, the certifying step comprises: an identical conversion certifying step for generating a certificate certifying that it knows the ordering relationship among the encrypted texts before and after the shuffling as well as random numbers used for encryption are known, and, when each of the input encrypted texts consists of multiple elements, that it knows that the elements of each encrypted text have been shuffled in the same order with the same random numbers; a substitution certifying step for generating a certificate certifying that the input encrypted texts have been correctly shuffled; a response generating step for generating responses for the identical conversion certifying step and the substitution certifying step; and a decryption certifying step for generating, based on the responses, a certificate certifying that the shuffle-decrypted texts are obtained through correct decryption of the shuffled encrypted texts using the secret keys. All of the certificates generated by the identical conversion certifying step, the substitution certifying step and the decryption certifying step as well as the responses generated by the response generating step are output as the shuffle-decryption certificates.

Yet another aspect of the invention is a shuffle-decryption verifying method, for verifying whether or not shuffle-decryption of multiple encrypted texts has taken place correctly by referring to shuffle-decryption certificates certifying that the shuffle-decryption has taken place correctly, in which the shuffle-decryption certificates comprise: responses as references upon certification; and certificates, generated based on the responses, certifying that the shuffled encrypted texts, obtained by shuffling the order of the encrypted texts and encrypting them with public keys, have correctly been decrypted with the secret keys to give the shuffle-decrypted texts.

The shuffle-decryption verifying method of present invention, comprises: an identical conversion verifying step where the shuffle-decryption certificates, the encrypted texts, the public keys and the shuffle-decrypted texts are input, where it is verified whether or not a generator of the certificates has information of the shuffling order and the content of conversion of the encrypted texts, where challenge values are generated, and, when each of the input encrypted texts consists of a plurality of elements, where it is verifies whether or not the elements of each encrypted text have been shuffled in the same order and converted with the same random numbers so as the whole conversion to encryptions; a substitution verifying step where the shuffle-decryption certificates and the challenge values generated by the identical conversion verifying step are input, and where it is verified whether or not the encrypted texts has been

correctly shuffled; and a decryption verifying step where the shuffle-decryption certificates and the challenge values generated by the identical conversion verifying step are input, and where it is verified whether or not the shuffled encrypted texts have been correctly decrypted using the secret keys to give shuffle-decrypted texts. Only when it is judged "valid" in all of the identical conversion verifying step, the substitution verifying step and the decryption verifying step, the encrypted texts are judged to have been shuffle-decrypted correctly.

Yet still another aspect of the invention is a certified shuffle-decrypting system, for generating shuffle-decryption certificates certifying that multiple encrypted texts have been shuffle-decrypted correctly, and for verifying, based on the shuffle-decryption certificates, whether or not the shuffle-decryption has taken place correctly, wherein the system comprises: a certified shuffle-decryption device for shuffle-decrypting the multiple encrypted texts to generate the shuffle-decrypted texts, and for generating the shuffle-decryption certificates; and a shuffle-decryption verification device for verifying whether or not the shuffle-decryption has taken place correctly, by referring to the generated shuffle-decrypted texts and the shuffle-decryption certificates for the shuffle-decrypted texts. The certified shuffle-decryption device: decrypts, with the secret keys, the shuffled encrypted texts obtained by shuffling the order of the encrypted texts and encrypting them with public keys, thereby generating the shuffle

decrypted texts; generates responses as a reference for the certifications; generates certificates certifying, based on the responses, the validities of the shuffling of order, the encryption and the decryption for obtaining the shuffle-decrypted texts; and outputs the generated certificates and the responses as shuffle-decryption certificates.

In the certified shuffle-decrypting system of the present invention, the certified shuffle-decryption device comprises: a shuffling unit into which the multiple encrypted texts and the public keys are input and which shuffles the order of the multiple encrypted texts and encrypts them with the public keys, thereby generating multiple shuffled encrypted texts; a decrypting unit into which the multiple shuffled encrypted texts and the secret keys are input and which decrypts the shuffled encrypted texts with the secret keys, thereby generating multiple shuffle-decrypted texts; and a certifying unit into which the multiple encrypted texts, the public keys and the secret keys are input and which generates the shuffle-decryption certificates.

In the certified shuffle-decrypting system of the present invention, the certifying unit of the certified shuffle-decryption device comprises: an identical conversion certifying unit for generating a certificate certifying that it knows the ordering relationship among the encrypted texts before and after the shuffling as well as random numbers used for encryption are known, and, when each of the input encrypted texts consists of multiple elements, that it knows that the elements of each encrypted text have been shuffled

in the same order with the same random numbers; a substitution certifying unit for generating a certificate certifying that the input encrypted texts have been correctly shuffled; a response generating unit for generating responses for the identical conversion certifying unit and the substitution certifying unit; and a decryption certifying unit for generating, based on the responses, a certificate certifying that the shuffle-decrypted texts are obtained through correct decryption of the shuffled encrypted texts using the secret keys. All of the certificates generated by the identical conversion certifying unit, the substitution certifying unit and the decryption certifying unit as well as the responses generated by the response generating unit are output as the shuffle-decryption certificates.

In the certified shuffle-decrypting system of the present invention, the shuffle-decryption verification device comprises: an identical conversion verifying unit into which the shuffle-decryption certificates, the encrypted texts, the public keys and the shuffle-decrypted texts are input, and which verifies whether or not a generator of the certificates has information of the shuffling order and the content of conversion of the encrypted texts, generates challenge values, and, when each of the input encrypted texts consists of a plurality of elements, verifies whether or not the elements of each encrypted text have been shuffled in the same order and converted with the same random numbers so as the whole conversion to encryptions; a substitution verifying unit into which the shuffle-decryption certificates and the challenge

values generated by the identical conversion verifying unit are input, and which verifies whether or not the encrypted texts has been correctly shuffled; and a decryption verifying unit into which the shuffle-decryption certificates and the challenge values generated by the identical conversion verifying unit are input, and which verifies whether or not the shuffled encrypted texts have been correctly decrypted using the secret keys to give shuffle-decrypted texts. Only when it is judged "valid" in all of the identical conversion verifying unit, the substitution verifying unit and the decryption verifying unit, the encrypted texts are judged to have been shuffle-decrypted correctly.

Yet another aspect of the invention is a computer program product for certified shuffle-decrypting, which controls a computer for shuffle-decrypting multiple encrypted texts to generate shuffle-decrypted texts and for generating shuffle-decryption certificates for certifying that the shuffle-decryption has correctly taken place, wherein: the order of the encrypted texts is shuffled and encrypted with public keys to obtain shuffled encrypted texts, which are then decrypted with secret keys to obtain the shuffle-decrypted texts; responses are generated as references for certifications; based on the response, certificates certifying validity of the shuffling of order, the encryption and the decryption for obtaining the shuffle-decrypted texts are generated; and the generated certificates and the response are output as shuffle-decryption certificates.

Yet another aspect of the invention is a computer program product for shuffle-decryption verifying, which controls a computer for verifying whether or not shuffle-decryption of multiple encrypted texts has taken place correctly by referring to shuffle-decryption certificates certifying that the shuffle-decryption has taken place correctly, wherein the shuffle-decryption certificates comprise: responses as references upon certification; and certificates, generated based on the responses, certifying that the shuffled encrypted texts, obtained by shuffling the order of the encrypted texts and encrypting them with public keys, have correctly been decrypted with the secret keys to give the shuffle-decrypted texts.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram showing a configuration of a certified shuffle-decrypting system according to one embodiment of the present invention;

Figure 2 is a flowchart for illustrating operations by the certified shuffle-decrypting system according to one embodiment of the present invention;

Figure 3 is a diagram for illustrating certified shuffle-decryption according to one embodiment of the present invention;

Figure 4 is a diagram for illustrating shuffle-decryption verification according to one embodiment of the present invention;

Figure 5 is a flowchart for illustrating operations according to a conventional technique;

Figure 6 is a diagram for illustrating operations of conventional certified shuffling;

Figure 7 is a diagram for illustrating operations of conventional certified decryption; and

Figure 8 is a diagram showing a configuration of a combination of the conventional techniques shown in Figures 6 and 7.

DETAILED DESCRIPTION OF THE INVENTION

Hereinafter, embodiments of the present invention will be described in detail with reference to the drawings.

[Certified shuffle-decrypting method]

According to a certified shuffle-decryption technique of the present invention, first, encrypted texts, public keys and secret keys are input. Based on the encrypted texts and the public keys, shuffled encrypted texts are generated. Then, the shuffled encrypted texts are decrypted with the secret keys to give decrypted texts.

Next, a certified shuffling method (certified encryption shuffling method) is employed to generate the shuffled encrypted texts and shuffling certificates. The certified shuffling process may be carried out according to the conventional technique, for example, as described in Document 1. However, according to the present invention, the decrypted texts are used instead of the shuffled encrypted

texts in order to generate challenge values for generating the certificates.

Then, difference of the verification results which occurs for using the decrypted texts instead of the shuffled encrypted texts upon the verification procedure is obtained and added to the shuffling certificates.

The certificates for validation of the obtained difference of the verification results are generated as decryption certificates. The shuffling certificates and the decryption certificates are added together as shuffle-decryption certificates. The decrypted texts and the shuffle-decryption certificate are output.

[Shuffle-decryption verifying method]

According to the shuffle-decryption verification of the invention, first, the encrypted texts, the public keys, the decrypted texts and the shuffle-decryption certificates are input. According to the present invention, the decrypted texts are input for the verification, instead of the shuffled encrypted texts used in the shuffle verification of Document 1. Difference of verification results caused upon using the decrypted texts in place of the shuffled encrypted texts upon the verification procedure, which is included in the shuffle-decryption certificates, is used for correcting the verification equation. Subsequently, validation of the difference of the verification results is verified. When the results of both of the verifications (i.e., shuffle verification using the decrypted texts and verification of the validation of the difference of the verification results)

are "valid", the verification result for the shuffle-decryption is output as "valid", otherwise output as "invalid".

Figure 1 is a block diagram showing a configuration of a certified shuffle-decrypting system according to one embodiment of the invention. Referring to Figure 1, the certified shuffle-decrypting system of the present embodiment is provided with a certified shuffle-decryption device 10 for generating certificates and a shuffle-decryption verification device 20 for verifying based on the certificates.

The certified shuffle-decryption device 10 is provided with a shuffling unit 11, a decrypting unit 12 and a certifying unit 13.

The shuffling unit 11 receives multiple encrypted texts and public keys, shuffles the order of the input multiple encrypted texts and encrypts the results with the public keys to give multiple shuffled encrypted texts.

The decrypting unit 12 receives the multiple shuffled encrypted texts generated by the shuffling unit 11 and secret keys, and decrypts the shuffled encrypted texts with the secret keys to generate and output multiple decrypted texts.

The certifying unit 13 generates certificates based on the multiple encrypted texts, the public keys and the secret keys. The certifying unit 13 is provided with an identical conversion certifying unit 13-1, a substitution certifying unit 13-2, a response generating unit 13-3 and a decryption certifying unit 13-4.

The identical conversion certifying unit 13-1 generates certificates which certify (which perform zero knowledge Interactive Proof) that they know the relationship of the orders before and after the shuffling by the shuffling unit 11 as well as the random numbers used for encryption. When each of the input encrypted texts consists of multiple integer elements, the identical conversion certifying unit 13-1 also generates certificates which certify that the elements of the encrypted texts are shuffled in the same order and processed with the same random number.

The substitution certifying unit 13-2 generates certificates that certify that shuffling has correctly taken place for the input encrypted texts. The response generating unit 13-3 generates responses for the identical conversion certifying unit 13-1 and the substitution certifying unit 13-2. The decryption certifying unit 13-4 generates certificate which certify that the shuffled encrypted texts have been correctly decrypted with the secret keys.

The certified shuffle-decryption device 10 outputs all of the certificates generated by the identical conversion certifying unit 13-1, the substitution certifying unit 13-2 and the decryption certifying unit 13-4 as well as the responses generated by the response generator 13-3, to give certificates for shuffle-decryption.

The shuffle-decryption verification device 20 is provided with an identical conversion verifying unit 21, a substitution verifying unit 22 and a decryption verifying unit 23.

The identical conversion verifying unit 21 accepts inputs of the shuffle-decryption certificates, the encrypted texts, the public keys and the decrypted texts to verify that the certificates contain the knowledge of the order of the shuffled input texts and the content of conversion for encryption. When each of the input encrypted texts consists of multiple elements, the identical conversion verifying unit 21 also verifies that the elements of each encrypted text are shuffled in the same order and converted with the same random numbers so as the whole conversion to encryptions. Then, the identical conversion verifying unit 21 outputs the result of the verification as "valid" or "invalid", and generates and outputs challenge values again.

The substitution verifying unit 22 receives inputs of the shuffle-decryption certificates as well as the challenge values generated by the identical conversion verifying unit 21, and verifies that the shuffling the order of the input encrypted texts has been done correctly and outputs the result as "valid" or "invalid".

The decryption verifying unit 23 receives inputs of the shuffle-decryption certificates as well as the challenge values generated by the identical conversion verifying unit 21, and verifies that the shuffled encrypted texts have been correctly decrypted with the secret keys to give decrypted texts, and outputs the result of verification as "valid" or "invalid".

When all of the verification results from the identical conversion verifying unit 21, the substitution verifying unit

22 and the decryption verifying unit 23 are "valid", the shuffle-decryption verification device 20 judges that the shuffled decrypted texts are the result of correct decryption of the input encrypted texts, and outputs a result of judgment as "valid". When at least one of the verification results is "invalid", the result of judgment is output as "invalid".

Hereinafter, the present invention will be described with reference to an example using ElGamal encryption. Followings are prior conditions of the present invention.

[ElGamal encryption system]

ElGamal encryption system belongs to a public-key cryptosystem. First, two prime numbers p and q that satisfy the relationship

$$P = kq + 1$$

are determined. These prime numbers are referred to as ElGamal domain parameters. Secret keys

$$x \in {}_R Z_q$$

are selected from elements of Z_q . Then, public keys

$$(g_0, m_0)$$

are selected from elements of Z_p^* of order q so as to satisfy the equation

$$m_0 = g_0^x \bmod p$$

In order to encrypt plain texts

$$P \in Z_p^*$$

which are elements of Z_p^* , random numbers

$$s \in {}_R Z_q$$

are secretly generated to obtain encrypted texts as

$$(G, M) = (g_0^s, m_0^s P) \bmod p$$

In order to decrypt this encrypted texts, the secret keys

x

are used to calculate as

$$P' = M/G^x \bmod p.$$

The decrypted texts P' correspond to the plain texts P .

Here, assume that the secret keys

x

are possessed separately. In other words, x is the sum of m number of x_j ($j = 1, \dots, m$) which are separately possessed, where

$$x = (x_1 + \dots + x_m) \bmod q$$

Herein, the x_j ($j = 1, \dots, m$) are referred to as secret keys used for decryption.

In order to completely decrypt an encrypted text, decryption operation, in which M is successively divided by the results of the following Expression (1) calculated by using the respective secret keys for decryption, is repeated for all of x_j ($j = 1, \dots, m$). However, in the present example, only one secret key for decryption is used and referred to as x' .

$$G^{x_j} \bmod p \quad \dots (1)$$

[Encrypted texts]

n number of encrypted texts that are input are represented by Expression 2 below. Each element of each encrypted text is the element of Z_p^* of the order q .

$$(g_i, m_i) \quad i = 1, \dots, n \quad \dots (2)$$

[Decrypted texts]

n number of decrypted texts that are output are represented by Expression 3 below. Each element of each decrypted text is the element of Z_p^* of the order q .

$$(\tilde{g}_i, \tilde{m}_i) \quad i=1, \dots, n \quad \dots (3)$$

These are the results obtained by shuffling the order of the n number of encrypted texts represented by Expression 4 below and decrypting them with the secret keys,

$$(g_i, m_i) \quad i = 1, \dots, n \quad \dots (4)$$

[Challenge value generating function]

Hereinafter, a challenge value generating function will be described. Figure 5 is a flowchart showing an example of an interactive certifying protocol consisting of the following four steps.

First, a certifier sends a commitment referring to a certification to a verifier (Step A1). Next, the verifier sends a challenge value to the certifier (Step A2). Then, the certifier sends a response in response to the challenge value (Step A3). The verifier confirms authenticity of the certification based on the commitment, the challenge value and the content of the response (Step A4).

In such an interactive certifying protocol, the authenticity of a certification depends on whether or not the certifier can send an appropriate response to the verifier in response to any challenge value. In Step A2, a function for generating a challenge value may be used instead of the verifier, thereby converting the above-described interactive certifying protocol to a non-interactive protocol.

Specifically, as represented by a flowchart shown in Figure 2, first, the certifier generates a commitment referring to a certification to the verifier (Step B1). Then, the commitment and content of the certification are input into the above-mentioned function to obtain the output as a challenge value (Step B2). The certifier generates a response to the challenge value and sends each of the generated data to the verifier (Step B3). The verifier confirms the authenticity of the certification based on the commitment, the challenge value and the content of the response (Step B4).

As described above, according to the certification protocol of the invention, the certifier can perform certification without interacting with the verifier.

The above-mentioned function for generating a challenge value is referred to as a challenge value generating function, which is expressed by the following Expression (5).

$$H_i(*) \quad i = 1, \dots, n \quad \dots (5)$$

The output of the challenge value generating function is n number of integers that is less than q but not "1" or "0". This function does not allow parameters to be derived intentionally through calculation with respect to the relationship between the input and output or the relationship between different components of the output.

A specific challenge value generating function may be expressed, for example, by the following Equation (6).

$$H_i(x) = \text{Hash}(\text{Hash}(x))^i \bmod q \bmod q$$

[Substitution Matrix]

Hereinafter, a substitution matrix will be described. Herein, the "substitution matrix" is defined as an $n \times n$ (row $\times$ column) square matrix having a single unique component "1" on Z_q in each row and each column, and other components are all "0" on Z_q . An exemplary matrix include the following matrix (7).

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad \dots (7)$$

[Shuffle Matrix]

A shuffle matrix is defined as an $(n + 1) \times (n + 1)$ (row $\times$ column) matrix

$$\{A_{\mu, \nu}\} \quad (\mu, \nu = 0, \dots, n)$$

where the components thereof form a substitution matrix of

$$\{A_{i, j}\} \quad (i, j = 1, \dots, n): n \times n \text{ (row } \times \text{ column)}$$

$$A_{0, j}, A_{i, 0}, A_{0, 0} \in {}_R Z_q \quad (i, j = 1, \dots, n)$$

[Certified Shuffle-decryption]

Hereinafter, a certified shuffle-decrypting method according to one example of the invention will be described with reference to Figure 8.

[Shuffling step 402]

Encrypted texts/public keys 401

$$(g_i, m_i), (g_0, m_0): (i = 1, \dots, n)$$

are input.

Next, in shuffling step 402, shuffling information 403

$$A_{0,j} \in {}_{\mathbb{R}}Z_q \quad (j = 1, \dots, n)$$

$$A_{1,j} : \text{Substitution matrix } (i, j = 1, \dots, n)$$

is prepared.

Then, variables of the following Expression (8) as the shuffled encrypted texts 404 are calculated according to Equations (9) as follows. Then, the shuffling step 402 outputs the shuffling information 403 as well as the shuffled encrypted texts 404.

$$(\bar{g}_i, \bar{m}_i) \quad i=1, \dots, n \quad \dots (8)$$

$$\begin{aligned} \bar{g}_i &= \prod_{v=0}^n g_v^{A_{vi}} \bmod p \quad i=1, \dots, n \\ \bar{m}_i &= \prod_{v=0}^n m_v^{A_{vi}} \bmod p \quad i=1, \dots, n \end{aligned} \quad \dots (9)$$

[Decrypting step 405]

The shuffled encrypted texts 404 and the secret keys 400 for decryption are input. Then, the decrypted texts 406 are calculated according to Equations (10) and output.

$$\begin{aligned} \tilde{g}_i &= \bar{g}_i \bmod p \quad i=1, \dots, n \\ \tilde{m}_i &= \bar{g}_i^{-x'} \bar{m}_i \bmod p \quad i=1, \dots, n \end{aligned} \quad \dots (10)$$

[identical conversion certifying step 407]

The shuffling information 403 and the encrypted texts/public keys 401 are input. Then, a random number 408

$$A_{\mu,0} \in {}_{\mathbb{R}}Z_q \quad (\mu = 0, \dots, n)$$

is prepared to calculate each of the variables as a part of the commitment expressed by the following Expression (11)

according to the following Equations (12) and to output the result as an identical conversion certificate 409.

$$(\tilde{g}_0, \tilde{m}_0) \quad \dots (11)$$

$$\begin{aligned} \tilde{g}_0 &= \prod_{v=0}^n g_v^{A_{v0}} \bmod p \\ \tilde{m}_0 &= \prod_{v=0}^n m_v^{A_{v0}} \bmod p \end{aligned} \quad \dots (12)$$

[Substitution certifying step 410]

A shuffle matrix

$$A_{\mu, \nu} \bmod q \quad (\mu, \nu = 0, \dots, n)$$

which is obtained based on the shuffling information 403 generated in the shuffling step 402 and the random numbers 408 generated in the identical conversion certifying step 407 is input.

Then, random numbers (not 0 nor 1)

$$\sigma, \rho', \rho, \lambda_{\mu} \in {}_R Z_q \quad (\mu = 0, \dots, n)$$

$$g = g_0$$

are prepared to calculate the following Equations (13)

$$\begin{aligned}
\phi_i &= \sum_{j=1}^n (3A_{j0} + \rho'\lambda_j) A_{ji} \bmod q \quad i=1, \dots, n \\
\phi_i &= \sum_{j=1}^n (3A_{j0} + 2\rho'\lambda_j) A_{j0} A_{ji} + \rho A_{0i} \bmod q \quad i=1, \dots, n \\
\phi_0 &= \sum_{j=1}^n (A_{j0} + \rho'\lambda_j) A_{j0} A_{j0} + \rho'\lambda_0 + \rho A_{00} \bmod q \\
\psi_i &= \sum_{j=1}^n 2A_{j0} A_{ji} + \sigma A_{0i} \bmod q \quad i=1, \dots, n \\
\psi_0 &= \sum_{j=1}^n A_{j0} A_{j0} + \sigma A_{00} \bmod q \\
v &= g^\rho, v' = g^{\rho'}, \dot{v}_0 = g^{\phi_0}, \dot{v}_i = g^{\phi_i}, \\
w &= g^\sigma, \dot{w}_0 = g^{\psi_0}, \dot{w}_i = g^{\psi_i}, \\
\dot{u}_i &= g^{\phi_i}, u_0 = g^{\lambda_0}, u_i = g^{\lambda_i} \bmod p \quad i=1, \dots, n \quad \dots (13)
\end{aligned}$$

Here, each of the variables represented as Expressions 14 is output as a substitution certificate 411.

$$v, \dot{v}_0, \dot{v}_i, w, \dot{w}_0, \dot{w}_i, v', \dot{u}_i, u_0, u_i \quad i=1, \dots, n \quad \dots (14)$$

[Response generating step 412]

The encrypted texts/public keys 401, the identical conversion certificates 409, the substitution certificates 411 and the decrypted texts 406 are input to calculate challenge value according to Equation (15).

$$\begin{aligned}
c_i &= H_i(g_0, g_j, m_0, m_j, \tilde{g}_0, \tilde{g}_j, \tilde{m}_0, \tilde{m}_j, \\
&\quad v, \dot{v}_0, \dot{v}_j, w, \dot{w}_0, \dot{w}_j, v', \dot{u}_j, u_0, u_j \\
&\quad j=1, \dots, n) \quad , \quad i=1, \dots, n \quad \dots (15)
\end{aligned}$$

Then, responses are calculated according to Equations (16).

$$r_\mu = \sum_{v=0}^n A_{\mu v} c_v \bmod q \quad \mu = 0, \dots, n$$

$$\lambda = \lambda_0 + \sum_{i=1}^n \lambda_i r_i \bmod q$$

... (16)

Finally, the identical conversion certificates, the substitution certificates and the responses are output as shuffling certificates 413.

[Decryption certifying step 417]

The decrypted texts 406, the secret keys 400 for decryption, and the challenge values 414 generated in the response generating step are input. An arbitrary value

$$\beta \in_{\mathbb{R}} \bmod q$$

is selected to calculate Equations (17).

$$\zeta = \prod_{i=1}^n \tilde{g}_i^{\alpha_i} \bmod p$$

$$\eta = \zeta^{x'} \bmod p$$

$$\eta' = \zeta^{\beta} \bmod p$$

$$m'_0 = g_0^{\beta} \bmod p$$

... (17)

Next, the challenge values for decryption certification are calculated according to Equation (18).

$$c' = H_0(\zeta, \eta, \eta', g_0, m'_0, m''_0) \quad \dots (18)$$

Next, the responses for decryption certification are calculated as:

$$r' = c' x' + \beta \bmod q$$

Finally,

$$\eta, \eta', m_0'', r'$$

are output as decryption certificates 415.

[Certificates]

The identical conversion certificates, the substitution certificates, the responses and the decryption certificates are output as certificates for shuffle-decryption.

[Verification of Shuffle-decryption]

Hereinafter, a method for verifying shuffle-decryption according to the present embodiment of the invention will be described with reference to Figure 4.

[identical conversion Verifying Step]

The shuffle-decryption certificates 316, the encrypted texts/public keys 401 and the decrypted texts are input. Challenge values 500 are calculated according to the following Equation (19).

$$c_i = H_i(g_0, g_j, m_0, m_j, \tilde{g}_0, \tilde{g}_j, \tilde{m}_0, \tilde{m}_j, v, \hat{v}_0, \hat{v}_j, w, \hat{w}_0, \hat{w}_j, v', \hat{u}_j, u_0, u_j, j=1, \dots, n) \quad i=1, \dots, n \quad \dots (19)$$

Then, if the following Equations (20) are true then "valid", if not then "invalid" is output as an output 501.

$$\prod_{\mu=0}^n g_{\mu}^{e_{\mu}} = \prod_{v=0}^n \tilde{g}_v^{e_v} \mod p$$

$$\prod_{\mu=0}^n m_{\mu}^{e_{\mu}} = \eta \prod_{v=0}^n \tilde{m}_v^{e_v} \mod p \quad \dots (20)$$

[Substitution Verifying Step]

The shuffle-decryption certificates and the challenge values 500 obtained in the identical conversion verifying step are input. Then, if the following Equations (21) are

true, then "valid", if not, then "invalid" is output as an output 502.

$$\begin{aligned}
 u^\lambda &= \dot{u}_0 \prod_{i=1}^n \dot{u}_i^{r_i r_i} \bmod p \\
 v^{r\lambda} v^{r0} g^{\sum_{i=1}^n (r_i^3 - c_i^3)} &= \dot{v}_0 \prod_{i=1}^n \dot{u}_i^{s_i^2} \prod_{i=1}^n \dot{v}_i^{c_i} \bmod p \\
 w^{r0} g^{\sum_{i=1}^n (r_i^2 - c_i^2)} &= \dot{w}_0 \prod_{i=0}^n \dot{w}_i^{c_i} \bmod p
 \end{aligned}
 \dots (21)$$

[Decryption Verifying Step]

The shuffle-decryption certificates and the challenge values 500 obtained in the identical conversion verifying step are input. Then, the auxiliary challenge values are calculated according to the following Equation (22).

$$c' = H_0(\zeta, \eta, \eta', g_0, m'_0, m''_0) \dots (22)$$

Next, if the following Equations (23) are true then "valid", if not then "invalid" is output as an output 503.

$$\begin{aligned}
 g_0^{r'} &= m'_0{}^{c'} m''_0 \bmod p \\
 \left(\prod_{i=1}^n \tilde{g}_i^{c_i} \right)^{r'} &= \eta^{c'} \eta' \bmod p
 \end{aligned}
 \dots (23)$$

If all of the outputs in the identical conversion verifying step, the substitution verifying step and the decryption verifying step are valid then "valid", if any one of them is invalid then "invalid" is output as a shuffle-decryption verification output 504.

In the certified shuffle-decrypting system according to the present embodiment, functions of the shuffling unit 11,

the decrypting unit 12, the certifying unit 13, the identical conversion certifying unit 13-1, the substitution certifying unit 13-2, the response generating unit 13-3 and the decryption certifying unit 13-4 of the certified shuffle-decryption device 10, functions of the identical conversion verifying unit 21, the substitution verifying unit 22 and the decryption verifying unit 23 of the shuffle-decryption verification device 20, and other functions may also be realized as a hardware. Computer programs provided with the above-mentioned functions, namely a certified shuffle-decryption program and a shuffle-decryption verification program, can also be realized by being loaded to a memory of a computer processor. The certified shuffle-decryption program and the shuffle-decryption verification program may be stored in a magnetic disk, a semiconductor memory or other storage media 80 and 90 to be loaded to the computer processor to control the operations thereof, thereby realizing the above-mentioned functions.

The present invention has been described by way of preferred embodiments and examples. The present invention, however, is not limited to the above-described embodiments or examples and may be modified in various ways without departing from the scope of the technical spirit of the invention.

According to the present invention, an amount of calculation required for a combination of certified decryption and certified shuffling can greatly be minimized compared to conventional techniques.

For example, assume that the number of the input encrypted texts is n . When the certified decryption is combined with the certified shuffling according to the conventional technique of Document 2, $3n$ number of modular exponentiations are required. On the other hand, the present invention requires only $(n + 3)$ number of modular exponentiations, which is far less than the amount of calculation required by the conventional techniques.

Since the modular exponentiations according to the present invention are not performed individually but are carried out as a multiplication of the modular exponentiations, much less amount of calculation is required and thus further high-speed processing can be realized.

The invention may be embodied in other specific forms without departing from the spirit or essential characteristic thereof. The present embodiments are therefore to be considered in all respects as illustrative and not restrictive, the scope of the invention being indicated by the appended Claims rather than by the foregoing description and all changes which come within the meaning and range of equivalency of the Claims are therefore intended to be embraced therein.

WHAT IS TO BE CLAIMED:

1. A certified shuffle-decryption device for shuffle-decrypting multiple encrypted texts to generate shuffle-decrypted texts and for generating shuffle-decryption certificates for certifying that the shuffle-decryption has correctly taken place, wherein:

the order of the encrypted texts is shuffled and encrypted with public keys to obtain shuffled encrypted texts, which are then decrypted with secret keys to obtain the shuffle-decrypted texts,

responses are generated as references for certifications;

based on the responses, certificates certifying validity of the shuffling of order, the encryption and the decryption for obtaining the shuffle-decrypted texts are generated; and

the generated certificates and the response are output as shuffle-decryption certificates.

2. A certified shuffle-decryption device according to claim 1, comprising:

a shuffling unit into which the multiple encrypted texts and the public keys are input and which shuffles the order of the multiple encrypted texts and encrypts them with the public keys, thereby generating multiple shuffled encrypted texts;

a decrypting unit into which the multiple shuffled encrypted texts and the secret keys are input and which

decrypts the shuffled encrypted texts with the secret keys, thereby generating multiple shuffle-decrypted texts; and

a certifying unit into which the multiple encrypted texts, the public keys and the secret keys are input and which generates the shuffle-decryption certificates.

3. A certified shuffle-decryption device according to claim 2,

wherein the certifying unit comprises:

an identical conversion certifying unit for generating a certificate certifying that it knows the ordering relationship among the encrypted texts before and after the shuffling as well as random numbers used for encryption are known, and, when each of the input encrypted texts consists of multiple integer elements, that it knows that the elements of each encrypted text have been shuffled in the same order and converted with the same random numbers so as the whole conversion to be encryptions;

a substitution certifying unit for generating a certificate certifying that the input encrypted texts have been correctly shuffled;

a response generating unit for generating responses for the identical conversion certifying unit and the substitution certifying unit; and

a decryption certifying unit for generating, based on the responses, a certificate certifying that the shuffle-decrypted texts are obtained through correct decryption of the shuffled encrypted texts using the secret keys, and

wherein all of the certificates generated by the identical conversion certifying unit, the substitution certifying unit and the decryption certifying unit as well as the responses generated by the response generating unit are output as the shuffle-decryption certificates.

4. A shuffle-decryption verification device for verifying whether or not shuffle-decryption of multiple encrypted texts has taken place correctly by referring to shuffle-decryption certificates certifying that the shuffle-decryption has taken place correctly,

wherein the shuffle-decryption certificates comprise:
responses as references upon certification; and
certificates, generated based on the responses,
certifying that the shuffled encrypted texts, obtained by shuffling the order of the encrypted texts and encrypting them with public keys, have correctly been decrypted with the secret keys to give the shuffle-decrypted texts.

5. A shuffle-decryption verification device according to claim 4, comprising:

an identical conversion verifying unit into which the shuffle-decryption certificates, the encrypted texts, the public keys and the shuffle-decrypted texts are input, and which verifies whether or not a generator of the certificates has information of the shuffling order and the content of conversion of the encrypted texts, generates challenge values, and, when each of the input encrypted texts consists of a

plurality of integer elements, verifies whether or not the elements of each encrypted text have been converted with the same random numbers so as the whole conversion to be encryptions;

a substitution verifying unit into which the shuffle-decryption certificates and the challenge values generated by the identical conversion verifying unit are input, and which verifies whether or not the encrypted texts has been correctly shuffled; and

a decryption verifying unit into which the shuffle-decryption certificates and the challenge values generated by the identical conversion verifying unit are input, and which verifies whether or not the shuffled encrypted texts have been correctly decrypted using the secret keys to give shuffle-decrypted texts, and

wherein only when judged "valid" in all of the identical conversion verifying unit, the substitution verifying unit and the decryption verifying unit, the encrypted texts are judged to have been shuffle-decrypted correctly.

6. A certified shuffle-decrypting method for shuffle-decrypting multiple encrypted texts to generate shuffle-decrypted texts and for generating shuffle-decryption certificates for certifying that the shuffle-decryption has correctly taken place, wherein:

the order of the encrypted texts is shuffled and encrypted with public keys to obtain shuffled encrypted texts,

which are then decrypted with secret keys to obtain the shuffle-decrypted texts;

responses are generated as references for certifications;

based on the response, certificates certifying validity of the shuffling of order, the encryption and the decryption for obtaining the shuffle-decrypted texts are generated; and the generated certificates and the response are output as shuffle-decryption certificates.

7. A certified shuffle-decrypting method according to claim 6, comprising the steps of:

based on the inputs of the multiple encrypted texts and the public keys, shuffling the order of the multiple encrypted texts and encrypting them with the public keys, thereby generating multiple shuffled encrypted texts;

based on the inputs of the multiple shuffled encrypted texts and the secret keys, decrypting the shuffled encrypted texts with the secret keys, thereby generating multiple shuffle-decrypted texts; and

based on the inputs of the multiple encrypted texts, the public keys and the secret keys, generating the shuffle-decryption certificates.

8. A certified shuffle-decrypting method according to claim 7, wherein the certifying step comprises:

an identical conversion certifying step for generating a certificate certifying that it knows the ordering

relationship among the encrypted texts before and after the shuffling as well as random numbers used for encryption are known, and, when each of the input encrypted texts consists of multiple elements, that it knows that the elements of each encrypted text have been shuffled in the same order and converted with the same random numbers so as the whole conversion to be encryptions;

a substitution certifying step for generating a certificate certifying that the input encrypted texts have been correctly shuffled;

a response generating step for generating responses for the identical conversion certifying step and the substitution certifying step; and

a decryption certifying step for generating, based on the responses, a certificate certifying that the shuffle-decrypted texts are obtained through correct decryption of the shuffled encrypted texts using the secret keys, and

wherein all of the certificates generated by the identical conversion certifying step, the substitution certifying step and the decryption certifying step as well as the responses generated by the response generating step are output as the shuffle-decryption certificates.

9. A shuffle-decryption verifying method for verifying whether or not shuffle-decryption of multiple encrypted texts has taken place correctly by referring to shuffle-decryption certificates certifying that the shuffle-decryption has taken place correctly,

wherein the shuffle-decryption certificates comprise:
responses as references upon certification; and
certificates, generated based on the responses,
certifying that the shuffled encrypted texts, obtained by
shuffling the order of the encrypted texts and encrypting
them with public keys, have correctly been decrypted with the
secret keys to give the shuffle-decrypted texts.

10. A shuffle-decryption verifying method according
to claim 9, comprising:

an identical conversion verifying step where the
shuffle-decryption certificates, the encrypted texts, the
public keys and the shuffle-decrypted texts are input, where
it is verified whether or not a generator of the certificates
has information of the shuffling order and the content of
conversion of the encrypted texts, where challenge values are
generated, and, when each of the input encrypted texts
consists of a plurality of elements, where it is verifies
whether or not the elements of each encrypted text have been
shuffled in the same order and converted with the same random
numbers so as the whole conversion to be encryptions;

a substitution verifying step where the shuffle-
decryption certificates and the challenge values generated by
the identical conversion verifying step are input, and where
it is verified whether or not the encrypted texts has been
correctly shuffled; and

a decryption verifying step where the shuffle-
decryption certificates and the challenge values generated by

the identical conversion verifying step are input, and where it is verified whether or not the shuffled encrypted texts have been correctly decrypted using the secret keys to give shuffle-decrypted texts, and

wherein only when judged "valid" in all of the identical conversion verifying step, the substitution verifying step and the decryption verifying step, the encrypted texts are judged to have been shuffle-decrypted correctly.

11. A certified shuffle-decrypting system for generating shuffle-decryption certificates certifying that multiple encrypted texts have been shuffle-decrypted correctly, and for verifying, based on the shuffle-decryption certificates, whether or not the shuffle-decryption has taken place correctly,

wherein the system comprises: a certified shuffle-decryption device for shuffle-decrypting the multiple encrypted texts to generate the shuffle-decrypted texts, and for generating the shuffle-decryption certificates; and a shuffle-decryption verification device for verifying whether or not the shuffle-decryption has taken place correctly, by referring to the generated shuffle-decrypted texts and the shuffle-decryption certificates for the shuffle-decrypted texts, and

wherein the certified shuffle-decryption device: decrypts, with the secret keys, the shuffled encrypted texts obtained by shuffling the order of the encrypted texts and

encrypting them with public keys, thereby generating the shuffle decrypted texts; generates responses as a reference for the certifications; generates certificates certifying, based on the responses, the validities of the shuffling of order, the encryption and the decryption for obtaining the shuffle-decrypted texts; and outputs the generated certificates and the responses as shuffle-decryption certificates.

12. A certified shuffle-decrypting system according to claim 11, wherein the certified shuffle-decryption device comprises:

a shuffling unit into which the multiple encrypted texts and the public keys are input and which shuffles the order of the multiple encrypted texts and encrypts them with the public keys, thereby generating multiple shuffled encrypted texts;

a decrypting unit into which the multiple shuffled encrypted texts and the secret keys are input and which decrypts the shuffled encrypted texts with the secret keys, thereby generating multiple shuffle-decrypted texts; and

a certifying unit into which the multiple encrypted texts, the public keys and the secret keys are input and which generates the shuffle-decryption certificates.

13. A certified shuffle-decrypting system according to claim 12, wherein the certifying unit of the certified shuffle-decryption device comprises:

an identical conversion certifying unit for generating a certificate certifying that it knows the ordering relationship among the encrypted texts before and after the shuffling as well as random numbers used for encryption are known, and, when each of the input encrypted texts consists of multiple elements, that it knows that the elements of each encrypted text have been shuffled in the same order with the same random numbers;

a substitution certifying unit for generating a certificate certifying that the input encrypted texts have been correctly shuffled;

a response generating unit for generating responses for the identical conversion certifying unit and the substitution certifying unit; and

a decryption certifying unit for generating, based on the responses, a certificate certifying that the shuffle-decrypted texts are obtained through correct decryption of the shuffled encrypted texts using the secret keys, and

wherein all of the certificates generated by the identical conversion certifying unit, the substitution certifying unit and the decryption certifying unit as well as the responses generated by the response generating unit are output as the shuffle-decryption certificates.

14. A certified shuffle-decrypting system according to any one of claims 11 to 13, wherein the shuffle-decryption verification device comprises:

an identical conversion verifying unit into which the shuffle-decryption certificates, the encrypted texts, the public keys and the shuffle-decrypted texts are input, and which verifies whether or not a generator of the certificates has information of the shuffling order and the content of conversion of the encrypted texts, generates challenge values, and, when each of the input encrypted texts consists of a plurality of elements, verifies whether or not the elements of each encrypted text have been shuffled in the same order and converted with the same random numbers so as the whole conversion to encryptions;

a substitution verifying unit into which the shuffle-decryption certificates and the challenge values generated by the identical conversion verifying unit are input, and which verifies whether or not the encrypted texts has been correctly shuffled; and

a decryption verifying unit into which the shuffle-decryption certificates and the challenge values generated by the identical conversion verifying unit are input, and which verifies whether or not the shuffled encrypted texts have been correctly decrypted using the secret keys to give shuffle-decrypted texts, and

wherein only when judged "valid" in all of the identical conversion verifying unit, the substitution verifying unit and the decryption verifying unit, the encrypted texts are judged to have been shuffle-decrypted correctly.

15. A computer program product for certified shuffle-decrypting which controls a computer for shuffle-decrypting multiple encrypted texts to generate shuffle-decrypting texts and for generating shuffle-decryption certificates for certifying that the shuffle-decryption has correctly taken place, wherein:

the order of the encrypted texts is shuffled and encrypted with public keys to obtain shuffled encrypted texts, which are then decrypted with secret keys to obtain the shuffle-decrypting texts;

responses are generated as references for certifications;

based on the response, certificates certifying validity of the shuffling of order, the encryption and the decryption for obtaining the shuffle-decrypting texts are generated; and the generated certificates and the response are output as shuffle-decryption certificates.

16. A computer program product according to claim 15, comprising:

a shuffling process where the multiple encrypted texts and the public keys are input and where the order of the multiple encrypted texts are shuffled and encrypted with the public keys, thereby generating multiple shuffled encrypted texts;

a decrypting process where the multiple shuffled encrypted texts and the secret keys are input and where the

shuffled encrypted texts are decrypted with the secret keys, thereby generating multiple shuffle-decrypted texts; and

a certifying process where the multiple encrypted texts, the public keys and the secret keys are input and where the shuffle-decryption certificates are generated.

17. A computer program product according to claim 16, wherein the certifying process comprises:

an identical conversion certifying process for generating a certificate certifying that it knows the ordering relationship among the encrypted texts before and after the shuffling as well as random numbers used for encryption are known, and, when each of the input encrypted texts consists of multiple elements, that it knows that the elements of each encrypted text have been shuffled in the same order with the same random numbers;

a substitution certifying process for generating a certificate certifying that the input encrypted texts have been correctly shuffled;

a response generating process for generating responses for the identical conversion certifying process and the substitution certifying process; and

a decryption certifying process for generating, based on the responses, a certificate certifying that the shuffle-decrypted texts are obtained through correct decryption of the shuffled encrypted texts using the secret keys, and

wherein all of the certificates generated through the identical conversion certifying process, the substitution

certifying process and the decryption certifying process as well as the responses generated by the response generating process are output as the shuffle-decryption certificates.

18. A computer program product for shuffle-decryption verifying which controls a computer for verifying whether or not shuffle-decryption of multiple encrypted texts has taken place correctly by referring to shuffle-decryption certificates certifying that the shuffle-decryption has taken place correctly,

wherein the shuffle-decryption certificates comprise:
responses as references upon certification; and
certificates, generated based on the responses,
certifying that the shuffled encrypted texts, obtained by shuffling the order of the encrypted texts and encrypting them with public keys, have correctly been decrypted with the secret keys to give the shuffle-decrypted texts.

19. A computer program product according to claim 18, comprising:

an identical conversion verifying process where the shuffle-decryption certificates, the encrypted texts, the public keys and the shuffle-decrypted texts are input, where it is verified whether or not a generator of the certificates has information of the shuffling order and the content of conversion of the encrypted texts, where challenge values are generated, and, when each of the input encrypted texts consists of a plurality of elements, where it is verifies

whether or not the elements of each encrypted text have been shuffled in the same order and converted with the same random numbers so as the whole conversion to be encryptions;

a substitution verifying process where the shuffle-decryption certificates and the challenge values generated by the identical conversion verifying process are input, and where it is verified whether or not the encrypted texts has been correctly shuffled; and

a decryption verifying process where the shuffle-decryption certificates and the challenge values generated by the identical conversion verifying process are input, and where it is verified whether or not the shuffled encrypted texts have been correctly decrypted using the secret keys to give shuffle-decrypted texts, and

wherein only when judged "valid" in all of the identical conversion verifying process, the substitution verifying process and the decryption verifying process, the encrypted texts are judged to have been shuffle-decrypted correctly.