



(51) International Patent Classification:

H04L 9/00 (2006.01)

G06F 17/16 (2006.01)

G06F 5/01 (2006.01)

(21) International Application Number:

PCT/KR2022/016242

(22) International Filing Date:

24 October 2022 (24.10.2022)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

10-2022-0061561 19 May 2022 (19.05.2022) KR

(71) Applicants: SEOUL NATIONAL UNIVERSITY R&DB FOUNDATION [KR/KR]; 1, Gwanak-ro, Gwanak-gu, Seoul 08826 (KR). INDUSTRY-ACADEMIC COOP-

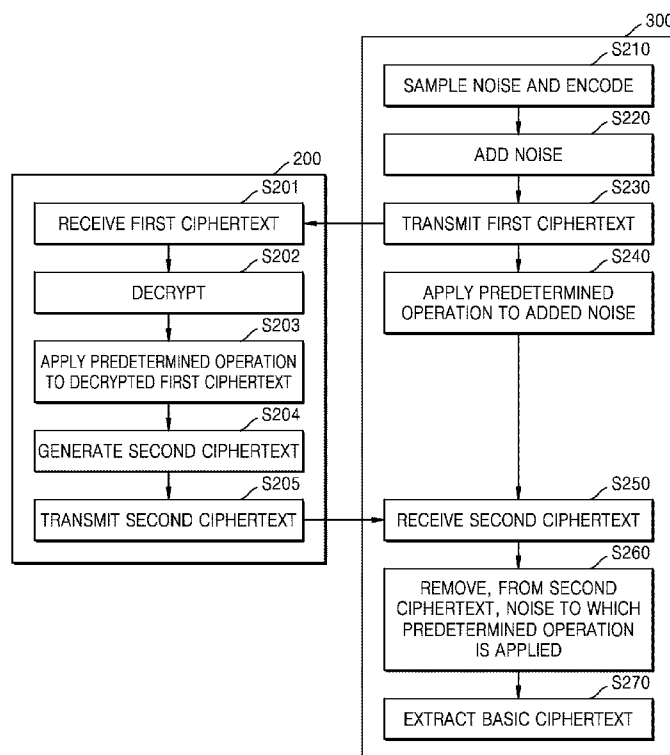
ERATION FOUNDATION, CHOSUN UNIVERSITY [KR/KR]; 309 Pilmun-daero, Dong-gu, Gwangju 61452 (KR).

(72) Inventors: LEE, Joon-Woo; Rm. 302, 31 Inheon 12da-gil, Gwanak-gu, Seoul 08797 (KR). NO, Jong-Seon; 207-803, 346-2 Sangdo-ro, Dongjak-gu, Seoul 07034 (KR). LEE, Yong-Woo; 107-101, 1 Bangbaeseonhaeng-gil, Seocho-gu, Seoul 06760 (KR). CHAE, Seung-Jae; F-3901, 57 Eonju-ro 30-gil, Gangnam-gu, Seoul 06293 (KR). KIM, Young-Sik; 201-1005, 66 Pungam 2-ro, Seo-gu, Gwangju 62067 (KR).

(74) Agent: Y.P.LEE, MOCK & PARTNERS; 12F Daelim Acrotel, 13 Eonju-ro 30-gil, Gangnam-Gu, Seoul 06292 (KR).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

(54) Title: METHOD AND DEVICE FOR PERFORMING HOMOMORPHIC PERMUTATION



(57) Abstract: A method of performing a homomorphic permutation via a terminal includes: generating, via a ciphertext generation portion, a first ciphertext, which is modified from a basic ciphertext by adding noise to the basic ciphertext; transmitting, via a transmission portion, the first ciphertext to a client; performing, via an operation portion, a predetermined operation on the noise; receiving, via a reception portion, a second ciphertext from the client; and extracting, via an extraction portion, the basic ciphertext on which the predetermined operation is performed, by removing, from the second ciphertext, the noise on which the predetermined operation is performed, wherein the second ciphertext is a ciphertext that is re-encrypted after decrypting the first ciphertext received from the client and then performing the predetermined operation on the decrypted first ciphertext.

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

Description

Title of Invention: METHOD AND DEVICE FOR PERFORMING HOMOMORPHIC PERMUTATION

Technical Field

- [1] One or more embodiments relate to mixing of homomorphic encryption and multilateral calculations. More particularly, one or more embodiments relate to a method of performing a homomorphic permutation from among multilateral calculations.

Background Art

- [2] Homomorphic rotation refers to an operation performed in an encrypted state to enable a cyclic shift on a vector in which a number of pieces of data are respectively moved with a fixed shift step in cyclic manner.

Disclosure of Invention

Technical Problem

- [3] However, it may take a long time to perform a homomorphic rotation in an encrypted state.
- [4] Also, a different arithmetic key is required for each rotation step of the homomorphic rotation operation. An arithmetic key occupies a memory of dozens to hundreds of megabytes. Thus, as the number of types of rotation steps increases, the number of arithmetic keys may increase too much, which makes it difficult to manage the memory.
- [5] Also, since there is no other permutation than homomorphic rotation, a required permutation has to be realized by synthesis of a number of homomorphic rotation operations. In this case, time required for processing a complex operation may significantly increase.

Solution to Problem

- [6] According to an embodiment of the disclosure, an operation time required when a cyclic shift is generated, by using communication, in an encrypted state for a homomorphic permutation may be reduced, and the homomorphic permutation may be performed without an arithmetic key. Also, a general permutation may be efficiently performed in an encrypted state without going through homomorphic rotation.
- [7] Additional aspects will be set forth in part in the description which follows and, in part, will be apparent from the description, or may be learned by practice of the presented embodiments of the disclosure.
- [8] [0001] According to one or more embodiments, a method of performing a homomorphic permutation by a server includes: generating, via a ciphertext generation portion, a first ciphertext by adding noise to the basic ciphertext; transmitting, via a

transmission portion, the first ciphertext to a client; performing, via an operation portion, a predetermined operation on the noise; receiving, via a reception portion, a second ciphertext from the client; and extracting, via an extraction portion, the basic ciphertext on which the predetermined operation is performed, by removing, from the second ciphertext, the noise, on which the predetermined operation is performed, wherein the second ciphertext is a ciphertext that is re-encrypted by the client after decrypting the first ciphertext and performing the predetermined operation on the decrypted first ciphertext. The terminal may include a server.

- [9] The predetermined operation may be a permutation operation.
- [10] The predetermined operation may be a cyclic shift operation.
- [11] The basic ciphertext may be a ciphertext with respect to original data encrypted by using a homomorphic algorithm.
- [12] The noise may be in a form of a polynomial expression extracted from a predetermined uniform distribution.
- [13] A server and the client may perform wired or wireless communication with each other.
- [14] A server and the client may have a prior agreement with respect to the predetermined operation.
- [15] According to one or more embodiments, a method of performing a homomorphic permutation by a client includes: receiving, via a reception portion, a first ciphertext from a server; decrypting, via a decryption portion, the first ciphertext by using a secret key; performing, via an operation portion, a predetermined operation on the decrypted first ciphertext; generating, via a re-encryption portion, a second ciphertext by re-encrypting the first ciphertext on which the predetermined operation is performed; and transmitting, via a transmission portion, the second ciphertext to the server, wherein the first ciphertext is a ciphertext that is modified from a basic ciphertext by the server adding noise to the basic ciphertext.
- [16] The predetermined operation may be a permutation operation.
- [17] The predetermined operation may be a cyclic shift operation.

Advantageous Effects of Invention

- [18] According to an embodiment of the disclosure, an operation time taken when a cyclic shift occurs in an encrypted state may be reduced, with respect to homomorphic permutation, and without an arithmetic key required for each rotation operation with respect to homomorphic permutation, a cyclic shift or a permutation may be performed.
- [19] According to an embodiment of the disclosure, an arbitrary permutation may be performed through one time communication between a server and a client or between a

first terminal and a second terminal, and thus, a time for an operation may be reduced.

Brief Description of Drawings

- [20] The above and other aspects, features, and advantages of certain embodiments of the disclosure will be more apparent from the following description taken in conjunction with the accompanying drawings, in which:
- [21] FIG. 1 illustrates a system for performing a homomorphic rotation by using a communication network, according to an embodiment of the disclosure;
- [22] FIG. 2 is a flowchart of homomorphic rotation between two terminals, using a communication network, according to an embodiment of the disclosure;
- [23] FIG. 3 illustrates an example of a process of performing a permutation operation of a homomorphic permutation between a server and a client, according to an embodiment of the disclosure;
- [24] FIG. 4 illustrates an example of a process of performing a cyclic shift operation of a homomorphic permutation between a server and a client, according to an embodiment of the disclosure; and
- [25] FIG. 5 illustrates an example of a computing environment including a computing terminal, according to an embodiment of the disclosure.

Best Mode for Carrying out the Invention

- [26] According to one or more embodiments, a device for performing a homomorphic permutation includes at least one processor to implement: an ciphertext generation portion configured to generate a first ciphertext by adding noise to the basic ciphertext; a transmission portion configured to transmit the first ciphertext to a terminal; a reception portion configured to receive a second ciphertext from the terminal; an operation portion configured to perform a predetermined operation on the noise; and an extraction portion configured to extract the basic ciphertext on which the predetermined operation is performed, by removing, from the second ciphertext, the noise, on which the predetermined operation is performed; wherein the second ciphertext is a ciphertext that is re-encrypted by the terminal after decrypting the first ciphertext and performing the predetermined operation on the decrypted first ciphertext.

Mode for the Invention

- [27] Reference will now be made in detail to embodiments, examples of which are illustrated in the accompanying drawings, wherein like reference numerals refer to like elements throughout. In this regard, the present embodiments may have different forms and should not be construed as being limited to the descriptions set forth herein. Accordingly, the embodiments are merely described below, by referring to the figures, to explain aspects of the present description. As used herein, the term "and/or" includes any and all combinations of one or more of the associated listed items. Expressions

such as "at least one of," when preceding a list of elements, modify the entire list of elements and do not modify the individual elements of the list.

[28] Hereinafter, detailed embodiments of the disclosure are described with reference to the drawings. The descriptions in detail below are provided to help comprehensive understanding with respect to a method, a device, and/or a system described in this specification. However, the descriptions are only examples, and the disclosure is not limited thereto.

[29] While describing the embodiments of the disclosure, detailed descriptions about related well known arts are omitted, when it is determined that they may unnecessarily blur the points of the disclosure. The terms used below are defined by taking into account corresponding functions in the disclosure and may be different according to an intention of a user or an operator, a precedent, or the like. Therefore, the definitions of the terms have to be understood based on the general aspects throughout the specification. The terms used in the detailed description are merely used to describe embodiments of the disclosure and shall not be understood as restricting the embodiments. Unless clearly otherwise used, a singular expression denotes a meaning of a plural expression. In the description, it should be understood that the terms, such as "including" or "having," are intended to indicate the existence of the features, numbers, steps, actions, components, parts, or combinations thereof, and are not intended to preclude the possibility that one or more other features, numbers, steps, actions, components, parts, or combinations thereof may exist or may be added.

[30] FIG. 1 illustrates a system for performing a homomorphic rotation by using a communication network, according to an embodiment of the disclosure.

[31] The system 100 illustrated in FIG. 1 shows an example of performing a homomorphic permutation by using communication between two terminals, that is, a first terminal 200 and a second terminal 300. According to an embodiment of the disclosure, the first terminal 200 may be a client, and the second terminal 300 may be a server. According to another embodiment of the disclosure, the first terminal 200 may be, for example, a data provisioning device provisioning data without disclosing personal information. The second terminal 300 may be, for example, a data analyzing device or a data processing device analyzing or processing personal information received from the first terminal 200. According to another embodiment of the disclosure, the first terminal 200 refers to a device owning input data of an operation. The first terminal 200 has a secret key with respect to a ciphertext and does not attempt to disclose information about the secret key to the second terminal 300. The second terminal 300 refers to a device performing operations by using encrypted data of the first terminal 200. The second terminal 300 does not have a secret key with respect to a ciphertext and does not attempt to disclose a calculation process to the first terminal

200.

- [32] According to another embodiment of the disclosure, the second terminal 300 may provide an artificial intelligence service by analyzing or processing information provided by the first terminal 200 without disclosing the information to the outside. For example, the second terminal 300 may analyze health information of a user of the first terminal 200, by using DNA information of the user of the first terminal 200, without disclosing the DNA information to the outside.
- [33] The first and second terminals 200 and 300 may include devices capable of performing communication with external devices and performing encryption by using homomorphic encryption, such as a cellular phone, a smartphone, a smart watch, a hand-held device, a wearable device, a robot, a personal computer (PC), a notebook computer, a tablet PC, etc.
- [34] Homomorphic encryption denotes an encryption technique to perform operation on encrypted data. It is an encryption method for performing an arbitrary logical operation or arithmetic operation using encrypted data. When homomorphic encryption is used, data leakage and hacking damage may be prevented. When a plurality of pieces of data are encrypted in one ciphertext and a position of each piece of data has to be changed, a homomorphic permutation and homomorphic multiplication of homomorphic encryption are used. One ciphertext is composed of a number of slots, and each slot has a specified order and occupies a specified position in one ciphertext.
- [35] According to an embodiment of the disclosure, the first terminal 200 and the second terminal 300 may perform a homomorphic permutation by using wired or wireless communication.
- [36] Homomorphic rotation refers to an operation of performing a cyclic shift on an encrypted vector in which a number of pieces of data that are encrypted in one ciphertext are respectively moved with a fixed shift step in cyclic manner, in an encrypted state. When a general permutation operation, except for a cyclic shift, is performed on one ciphertext, a vector containing 0 and 1 is multiplied based on homomorphic multiplication, with respect to each of ciphertexts, on which a cyclic shift of all types of steps corresponding to a shift distance of data is performed. Here, the multiplication is performed by using the vector including 1 with respect to data positioned in an intended position and the vector including 0 with respect to data not positioned in an intended position. Thereafter, homomorphic addition is performed on all of the processed ciphertexts.
- [37] According to an embodiment of the disclosure, the first terminal 200 and the second terminal 300 may perform communication between each other in order to perform a homomorphic permutation. Referring to FIGS. 2 and 3, a method of performing a homomorphic permutation is described, based on an example in which the first terminal

200 is a client, and the second terminal 300 is a server.

[38] FIG. 2 is a flowchart of homomorphic rotation between the first terminal 200 and the second terminal 300, using a communication network, according to an embodiment of the disclosure.

[39] According to an embodiment of the disclosure, it is assumed that the first terminal 200 and the second terminal 300 have a prior agreement on a permutation operation.

[40] As shown in FIG. 1, the second terminal 300 may include a ciphertext generation portion 310, a transmission portion 320, a first operation portion 330, a reception portion 340, and an extraction portion 350. A process performed by the second terminal 300 for performing a homomorphic rotation is described first.

[41] Referring to FIG. 2, the ciphertext generation portion 310 may perform noise sampling and encoding of the sampled noise in operation S210. Thereafter, a first ciphertext may be generated by adding first noise to a basic ciphertext in operation S220. The basic ciphertext may refer to a ciphertext with respect to original data encrypted by using a homomorphic algorithm.

[42] The transmission portion 320 may transmit the first ciphertext to the first terminal 200 in operation S230.

[43] The first operation portion 330 may apply a predetermined operation to the noise added by the encryption generation portion 310, in operation S240.

[44] The reception portion 340 may receive a second ciphertext from the first terminal 200 in operation S250. The second ciphertext may refer to a ciphertext that is re-encrypted by the first terminal 200 after decrypting the first ciphertext received and then performing, on the decrypted first ciphertext, a predetermined operation previously agreed upon between the first terminal 200 and the second terminal 300.

[45] In operation S260, the extraction portion 350 may remove, from the received second ciphertext, second noise indicating the noise to which the predetermined operation has been applied by the first operation portion 300 in operation S240. Thereby, a basic ciphertext is extracted in operation S270.

[46] As shown in FIG. 1, the first terminal 200 may include a reception portion 210, a decryption portion 220, a second operation portion 230, a re-encryption portion 240, and a transmission portion 250. A process of performing a homomorphic rotation operation by the first terminal 200 is described below.

[47] Referring to FIG., 2, the reception portion 210 may receive a first ciphertext from the second terminal 300 in operation S201. The first ciphertext may refer to a ciphertext that is modified from a basic ciphertext by the second terminal 300 adding noise to the basic ciphertext. The decryption portion 220 may decrypt the received first ciphertext by using a secret key in operation S202.

[48] The second operation portion 230 may perform, on the decrypted first ciphertext, a

predetermined operation that is agreed upon between the first terminal 200 and the second terminal 300 in advance, in operation S203. The re-encryption portion 240 may generate a second ciphertext by re-encrypting the first ciphertext on which the predetermined operation is performed by the second operation portion 230, in operation S204. Then, the transmission portion 250 may transmit the second ciphertext to the second terminal 300.

[49] FIG. 3 illustrates an example of performing a permutation operation of a homomorphic permutation between a server and a client, according to an embodiment of the disclosure. FIG. 3 illustrates an example of performing the permutation operation of the homomorphic permutation by using homomorphic encryption. Homomorphic encryption may be homomorphic encryption of Cheon-Kim-Kim-Song (CKKS).

[50] The ciphertext generation portion 310 may generate a first ciphertext that is modified from a basic ciphertext by adding noise to the basic ciphertext in operations S310 and S320. The basic ciphertext may correspond to an input ciphertext on which a permutation is to be performed. Also, with respect to N which is one of the powers of 2, and Q which is a product of large prime numbers, R_Q may be a set of all polynomial expressions which may correspond to remaining ones after the polynomial expressions are sequentially divided by Q and $X^N + 1$. The basic ciphertext may be composed of two polynomial expressions R_Q^2 included in this set. All ciphertexts described hereinafter may be composed in this way. The basic ciphertext may be assumed as shown in Equation 1.

[51] [Equation 1]

$$[52] \quad ct = (b(X), a(X)) \in R_Q^2$$

[53] In the description below, a process of obtaining a polynomial expression $r(X)$ in the set R_Q by encoding a slot vector $(r_0, r_1, \dots, r_{(n-1)})$ may be frequently used. In this case, with respect to a complex number $\zeta = e^{2\pi i/N}$, a calculation is performed such that after obtaining an $n-1^{\text{th}}$ order polynomial expression $r'(X)$ of an only real number coefficient, satisfying $r'(\zeta^{5j}) = r_j$, with respect to $j=0, \dots, n-1$, $r(X) = [\Delta \cdot r'(X)] \in R_Q$ may be obtained with respect to a predetermined integer Δ . All the following encoding process is defined as below.

[54] The ciphertext generation portion 310 may sample noise in operation S310. The noise may have a form of a slot vector $(r_0, r_1, \dots, r_{(n-1)})$ and each r_j may be represented in the form of a polynomial expression extracted from a uniform distribution in the set Z_Q . Here, the set Z_Q refers to a set of remaining ones of an integer divided by Q . This may be encoded to generate a polynomial expression $r(X)$ of the noise.

- [55] Also, the polynomial expression $r(X)$ of the noise may be added to a first polynomial expression $b(X)$ of two polynomial expressions included in the basic ciphertext, as shown in Equation 2.
- [56] [Equation 2]
- [57] $b'(X) = b(X) + r(X)$
- [58] Thereafter, a first ciphertext, which is modified from the basic ciphertext by adding noise thereto, may be generated in operation S320. The first ciphertext is defined as Equation 3.
- [59] [Equation 3]
- [60] $ct' = (b'(X), a(X)) \in R_Q^2$
- [61] The transmission portion 320 may transmit the first ciphertext $ct' = (b'(X), a(X)) \in R_Q^2$ generated by the ciphertext generation portion 310 to the first terminal 200 in operation S330.
- [62] The first operation portion 330 may obtain $(r_{(\sigma(0))}, r_{(\sigma(1))}, \dots, r_{(\sigma(n-1))})$ by applying a permutation function σ to the slot vector $(r_0, r_1, \dots, r_{(n-1)})$ obtained from the ciphertext generation portion 310. Then, second noise $r'(X)$ may be obtained by encoding $(r_{(\sigma(0))}, r_{(\sigma(1))}, \dots, r_{(\sigma(n-1))})$ based on a polynomial expression in R_Q in operation S340. That is, the first operation portion 330 may apply a predetermined operation previously agreed upon between the first terminal 200 and the second terminal 300 to the noise added to the basic ciphertext by the ciphertext generation portion 310.
- [63] The reception portion 340 may receive a second ciphertext from the client 200 in operation S350. The second ciphertext may indicate a ciphertext that is re-encrypted by the first terminal 200 after decrypting the first ciphertext and then performing, on the decrypted first ciphertext, the predetermined operation previously agreed upon between the first terminal 200 and the second terminal 300. The second ciphertext may be defined as Equation 4.
- [64] The extraction portion 350 may extract the basic ciphertext by removing, from the received second ciphertext, the noise to which the predetermined operation is applied, in operation S360. When the second ciphertext $ct'' = (b''(X), a''(X))$ is received from the first terminal 200, second noise $r'(X)$ may be calculated by the first operation portion 330 and may be removed from a first element $b''(X)$ of the second ciphertext, to obtain $\bar{b}(X) = b''(X) - r'(X)$ and compose $\bar{ct} = (\bar{b}(X), a''(X)) \in R_Q^2$. A vector of $(v_0, v_1, \dots, v_{(n-1)})$ is derived when $m(X)$ decoding is performed by decrypting the basic ciphertext owned by the server 300. Specifically, a vector of $(v_{(\sigma(0))}, v_{(\sigma(1))}, \dots, v_{(\sigma(n-1))})$, which is permuted from the vector of $(v_0, v_1, \dots, v_{(n-1)})$

via the permutation function σ , may be derived, when the extraction portion 350 decrypts and decodes the extracted basic ciphertext.

[65] According to an embodiment of the disclosure, the client 200 may include the reception portion 210, the decryption portion 220, the second operation portion 230, the re-encryption portion 240, and the transmission portion 250.

[66] Referring to FIG. 3, the client 200 may receive a first ciphertext from the server 300 in operation S301. The first ciphertext may be represented by Equation 3. The decryption portion 220 of the client 200 may decrypt the first ciphertext by using a secret key $s(X)$ to calculate $b'(x)+a(x)s(x)=m(X)+r(X)=m'(X)$ in operation S302. Here, $m(X)$ denotes a polynomial expression obtained by encoding a slot vector $(v_0, v_1, \dots, v_{(n-1)})$ encrypted in an input basic ciphertext.

[67] The decryption portion 220 may obtain a slot vector $(m'_0, m'_1, \dots, m'_{n-1})$ by decoding the calculated $m'(X)$, in operation S303.

[68] The second operation portion 230 may obtain $(m'_{\sigma(0)}, m'_{\sigma(1)}, \dots, m'_{\sigma(n-1)})$ from $(m'_0, m'_1, \dots, m'_{n-1})$ by applying a predetermined permutation to the decrypted first ciphertext and may encode $(m'_{\sigma(0)}, m'_{\sigma(1)}, \dots, m'_{\sigma(n-1)})$ to obtain $m''(X)$ in operation S304.

[69] $(m'_{\sigma(0)}, m'_{\sigma(1)}, \dots, m'_{\sigma(n-1)})$ may maintain an encrypted state by the slot vector $(r_0, r_1, \dots, r_{(n-1)})$ obtained by the encryption generation portion 310 of the server 300, and thus, the client 200 may not know information of the server 300 after decryption and decoding.

[70] The re-encryption portion 240 may encrypt $m''(X)$ to generate a second ciphertext as shown in Equation 4, in operation S304. The transmission portion 250 may transmit the second cryptogram to the server 300 in operation S305.

[71] [Equation 4]

$$ct'' = (b''(X), a''(X)) \in R_Q^2,$$

[73] FIG. 4 is an example of performing, via the first terminal 200 and the second terminal 300, a cyclic shift operation of a homomorphic permutation, according to another embodiment of the disclosure. According to an embodiment of the disclosure, when a vector of $(v_0, v_1, \dots, v_{(n-1)})$ is encrypted by the server 300 in a basic ciphertext, the server 300 may, through communication with the client 200, attempt to obtain a ciphertext in which a vector $(v_k, v_{k+1}, \dots, v_{n-1}, v_0, \dots, v_{k-1})$, which is cyclically shifted by k , is encrypted. FIG. 4 illustrates a case of using homomorphic encryption of CKKS, according to an embodiment.

[74] For descriptions of homomorphic permutation of FIG. 4 that are substantially the

same as those of homomorphic permutation of FIG. 3 will be omitted.

- [75] In operation S403, the second operation portion 230 of the client 200 may obtain $m'(X^{s^*})$ by applying a cyclic shift operation by substituting X^{s^*} for X in $m'(X)$. Also, in operation S440, the first operation portion 330 of the server 300 may obtain $r(X^{s^*})$ by substituting X^{s^*} rather than X for $r(x)$, which is a noise element added to a basic ciphertext (S420). Also, this may be converted to an element of R_Q^2 , which is a space of a new ciphertext. In S450, the server 200 receives a second ciphertext from the client. In operation S460, noise to which the cyclic shift operation is applied may be removed from the second ciphertext. As a result, a basic ciphertext which is generated by encrypting a cyclic shift vector may be extracted. In detail, when the second ciphertext ct'' is received from the client, $r(X^{s^*})$ may be subtracted from $b''(X)$, which is a first element of the second ciphertext, to obtain $\overline{b}(X) = b''(X) - r(X^{s^*})$ and compose $\overline{ct} = (\overline{b}(X), a''(X)) \in R_Q^2$.

- [76] FIG. 5 illustrates an example of a computing environment including a computing terminal 12, according to an embodiment of the disclosure. In the embodiment illustrated in FIG. 5, each component may have different functions and capabilities from those described hereinafter. Also, in addition to the descriptions below, additional components may be included.

- [77] The computing terminal 12 may include at least one processor 14, a computer-readable storage medium 16, and a communication bus 18. The processor 14 may enable the computing terminal 12 to operate according to example embodiments described above. For example, the processor 14 may execute one or more programs stored in the computer-readable storage medium 16. The one or more programs may include one or more computer-executable instructions, and when the computer-executable instructions are executed by the processor 14, the computing terminal 12 may perform operations according to the example embodiments.

- [78] The computer-readable storage medium 16 may be configured to store computer-executable instructions or program codes, program data, and/or other appropriate type information. A program 20 stored in the computer-readable storage medium 16 may include a set of instructions executable by the processor 14. According to an embodiment, the computer-readable storage medium 16 may include a memory (a volatile memory such as random-access memory, a non-volatile memory, or an appropriate combination thereof), one or more magnetic disk storage devices, optical disk storage devices, flash memory devices, other types of storage media accessed by the computing terminal 12 and capable of storing desired information, or an appropriate combination thereof.

- [79] The communication bus 18 may connect various components of the computing terminal 12, including the processor 14 and the computer-readable storage medium 16, to one another. The computing terminal 12 may also include one or more input and output interfaces 22 providing an interface for one or more input and output devices 24 and one or more network communication interfaces 26. The one or more input and output interfaces 22 and the one or more network communication interfaces 26 may be connected to the communication bus 18. The one or more input and output devices 24 may be connected to other components of the computing terminal 12 through the one or more input and output interfaces 22. Examples of the input and output devices 24 may include a pointing device (a mouse, a track pad, or the like), an input device, such as a keyboard, a touch input device (a touch pad, a touch screen, or the like), a voice or sound input device, various types of sensor devices and/or capturing devices, and/or an output device, such as a display, a printer, a speaker, and/or a network card. The examples of the input and output devices 24 may be included in the computing terminal 12 as a component included in the computing terminal 12 or may be connected to the computing terminal 12 as a separate device from the computing device 12.
- [80] At least one of the components, elements or units (collectively "components" in this paragraph) represented by a block in the drawings, such as the first and second terminals 200 and 300 and their components illustrated in FIG. 1, may be embodied as various numbers of hardware, software and/or firmware structures that execute respective functions described above, according to embodiments. For example, at least one of these components may use a direct circuit structure, such as a memory, processing, logic, a look-up table, etc. that may execute the respective functions through controls of one or more microprocessors or other control apparatuses. Also, at least one of these components may be specifically embodied by a module, a program, or a part of code, which contains one or more executable instructions for performing specified logic functions. Also, at least one of these components may further include a processor such as a central processing unit (CPU) that performs the respective functions, a microprocessor, or the like. Functional aspects of the above exemplary embodiments may be implemented in algorithms that execute on one or more processors. Furthermore, the components represented by a block or processing steps may employ any number of related art techniques for electronics configuration, signal processing and/or control, data processing and the like.
- [81] It should be understood that embodiments described herein should be considered in a descriptive sense only and not for purposes of limitation. Descriptions of features or aspects within each embodiment should typically be considered as available for other similar features or aspects in other embodiments. While one or more embodiments

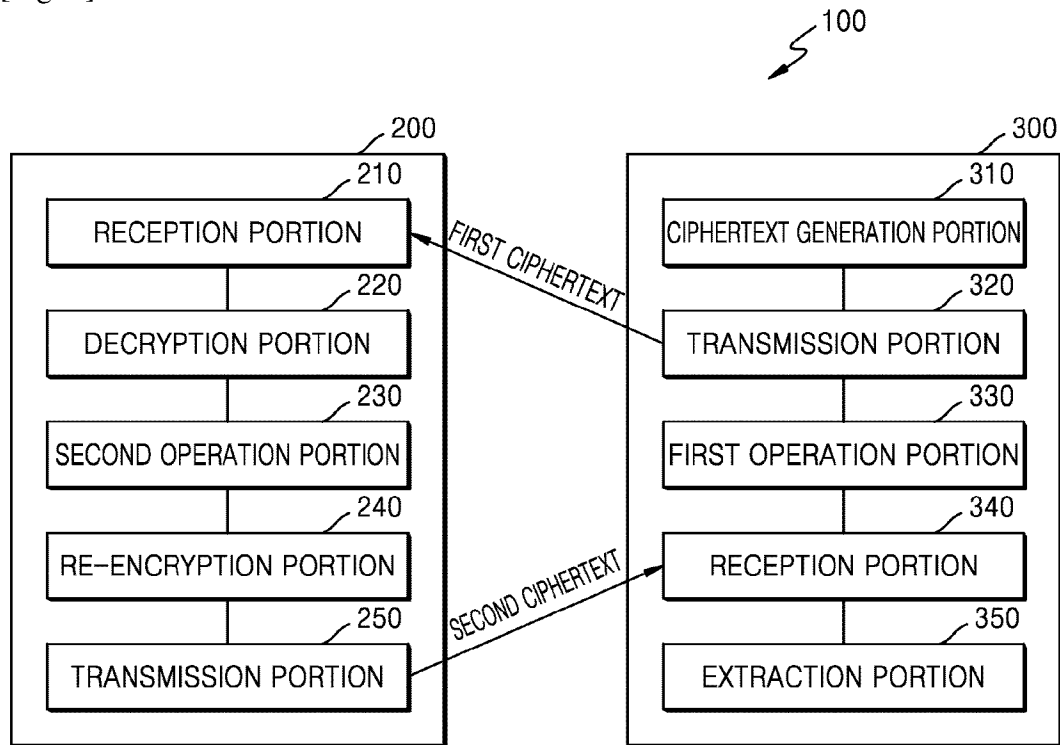
have been described with reference to the figures, it will be understood by those of ordinary skill in the art that various changes in form and details may be made therein without departing from the spirit and scope as defined by the following claims.

Claims

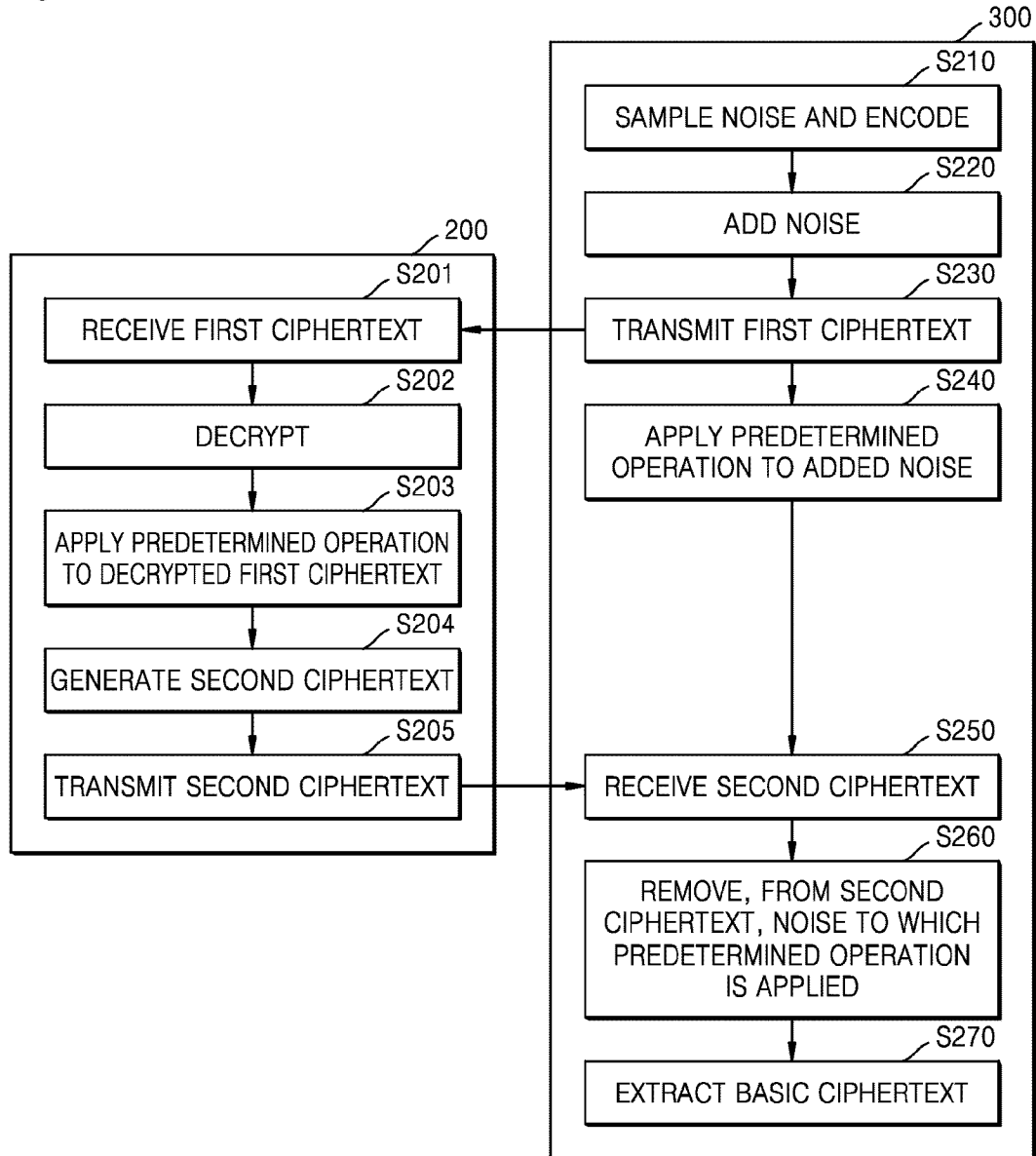
- [Claim 1] A method of performing a homomorphic permutation by a server, the method comprising:
generating, via a ciphertext generation portion, a first ciphertext by adding noise to a basic ciphertext;
transmitting, via a transmission portion, the first ciphertext to a client;
performing, via an operation portion, a predetermined operation on the noise;
receiving, via a reception portion, a second ciphertext from the client;
and
extracting, via an extraction portion, the basic ciphertext on which the predetermined operation is performed, by removing, from the second ciphertext, the noise on which the predetermined operation is performed,
wherein the second ciphertext is a ciphertext that is re-encrypted by the client after decrypting the first ciphertext and performing the predetermined operation on the decrypted first ciphertext.
- [Claim 2] The method of claim 1, wherein the predetermined operation is a permutation operation.
- [Claim 3] The method of claim 1, wherein the predetermined operation is a cyclic shift operation.
- [Claim 4] The method of claim 1, wherein the basic ciphertext is a ciphertext with respect to original data encrypted by using a homomorphic algorithm.
- [Claim 5] The method of claim 1, wherein the noise is in a form of a polynomial expression extracted from a predetermined uniform distribution.
- [Claim 6] The method of claim 1, wherein the server and the client perform wired or wireless communication with each other.
- [Claim 7] The method of claim 1, wherein the server and the client have a prior agreement with respect to the predetermined operation.
- [Claim 8] A method of performing a homomorphic permutation by a client, the method comprising:
receiving, via a reception portion, a first ciphertext from a server;
decrypting, via a decryption portion, the first ciphertext by using a secret key;
performing, via an operation portion, a predetermined operation on the decrypted first ciphertext;
generating, via a re-encryption portion, a second ciphertext by re-

- encrypting the first ciphertext on which the predetermined operation is performed; and
transmitting, via a transmission portion, the second ciphertext to the server,
wherein the first ciphertext is a ciphertext that is modified from a basic ciphertext by the server adding noise to the basic ciphertext.
- [Claim 9] The method of claim 8, wherein the predetermined operation is a permutation operation.
- [Claim 10] The method of claim 8, wherein the predetermined operation is a cyclic shift operation.
- [Claim 11] A device for performing a homomorphic permutation, the device comprising at least one processor to implement:
a ciphertext generation portion configured to generate a first ciphertext by adding noise to the basic ciphertext;
a transmission portion configured to transmit the first ciphertext to a terminal;
a reception portion configured to receive a second ciphertext from the terminal;
an operation portion configured to perform a predetermined operation on the noise; and
an extraction portion configured to extract the basic ciphertext on which the predetermined operation is performed, by removing, from the second ciphertext, the noise on which the predetermined operation is performed,
wherein the second ciphertext is a ciphertext that is re-encrypted by the terminal after decrypting the first ciphertext and performing the predetermined operation on the decrypted first ciphertext.
- [Claim 12] The device of claim 11, wherein the predetermined operation is a permutation operation.
- [Claim 13] The device of claim 11, wherein the predetermined operation is a cyclic shift operation.
- [Claim 14] The device of claim 11, wherein the basic ciphertext is a ciphertext with respect to original data encrypted by using a homomorphic algorithm.
- [Claim 15] A non-transitory computer-readable recording medium having stored thereon a program for executing the method of performing a homomorphic permutation of claim 1.

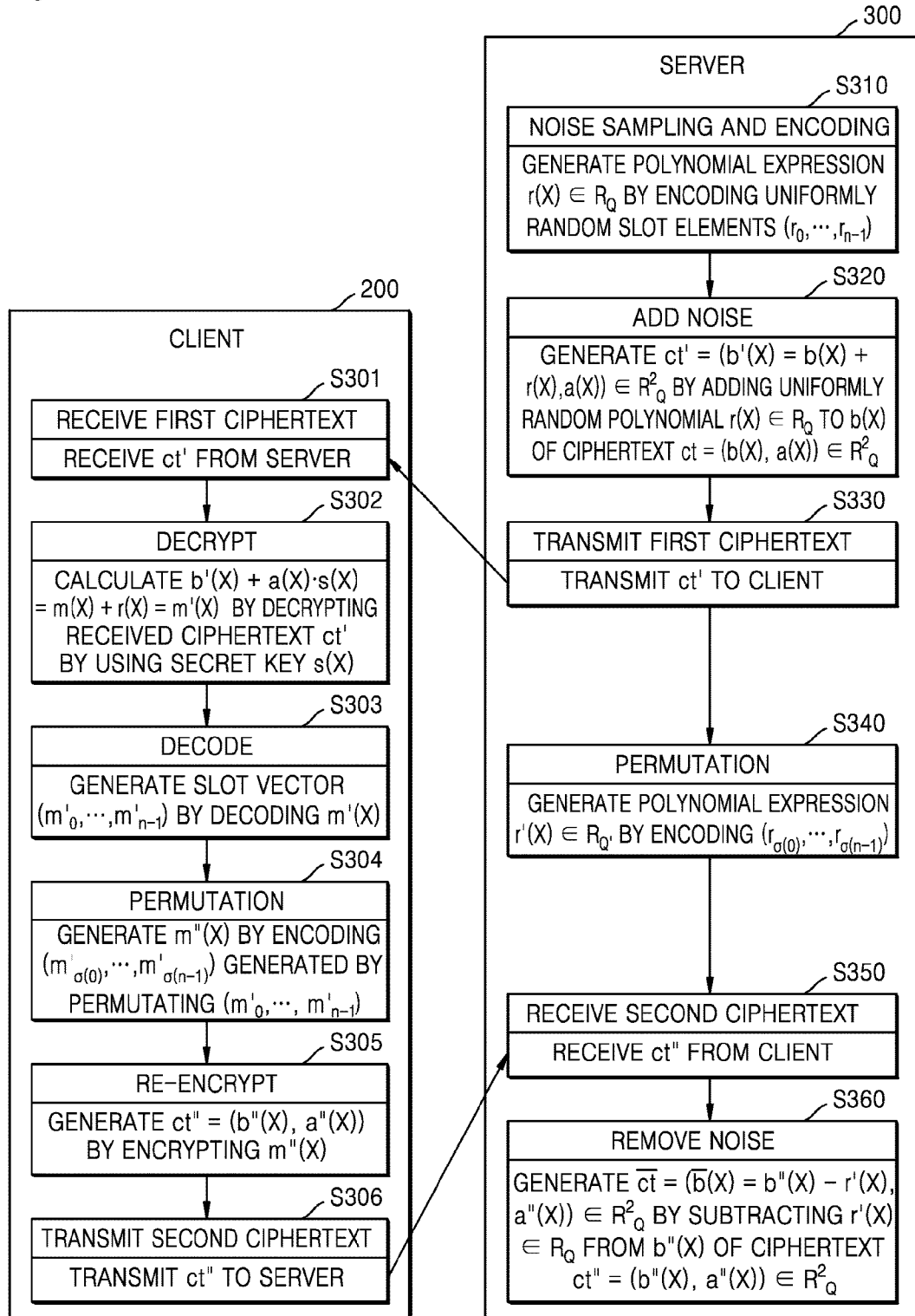
[Fig. 1]



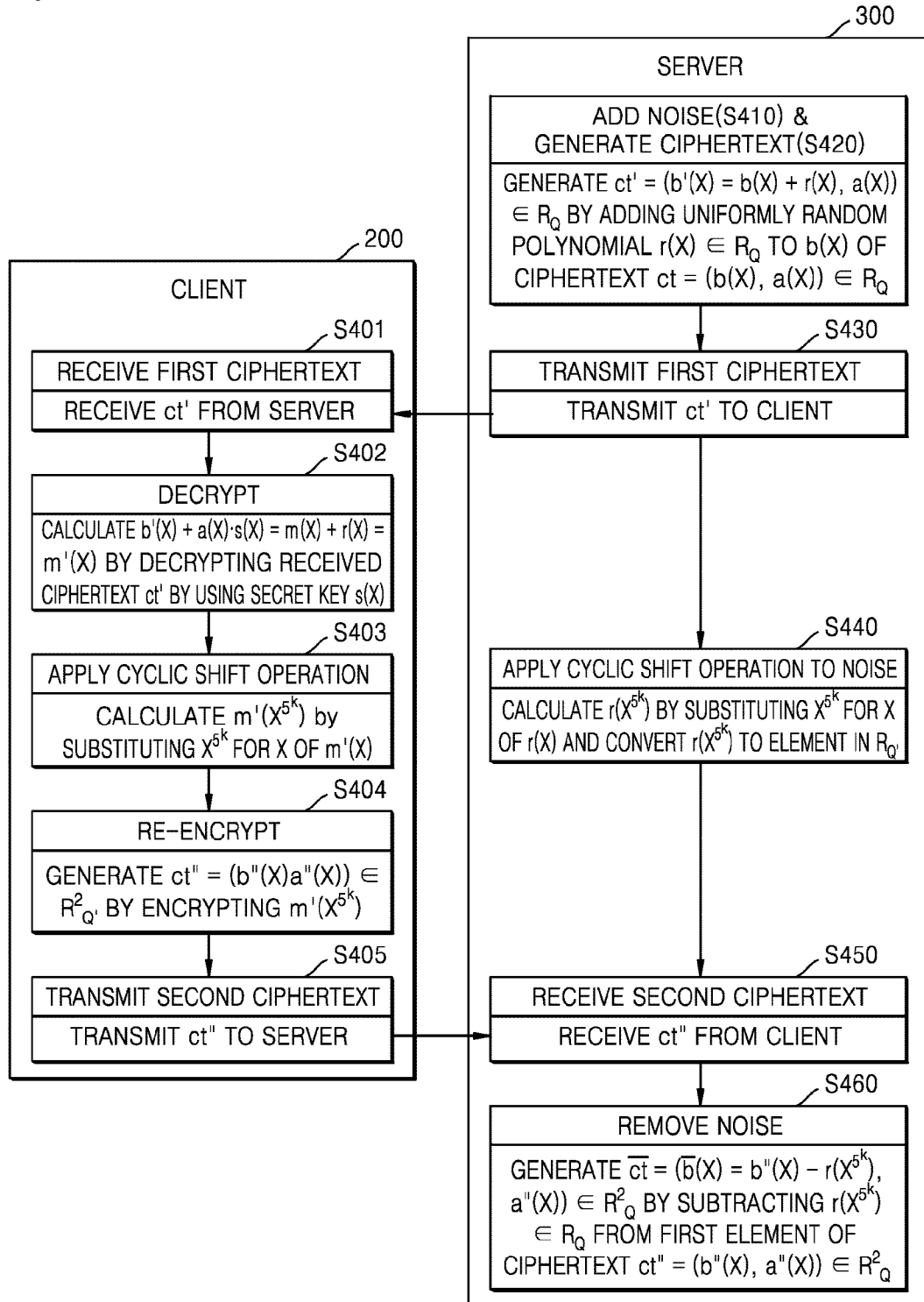
[Fig. 2]



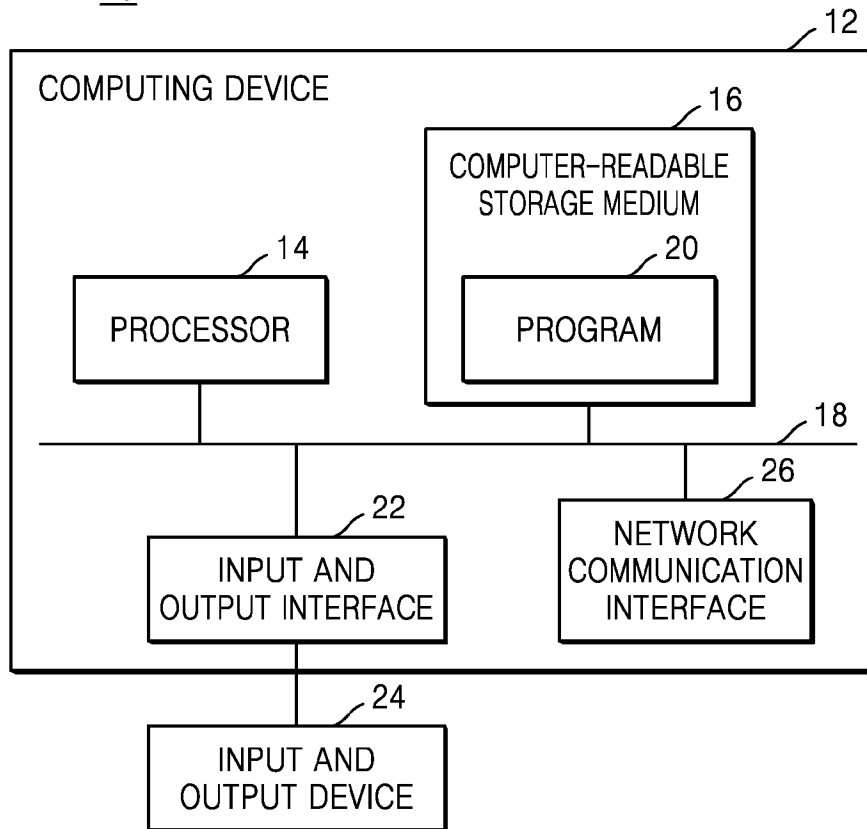
[Fig. 3]



[Fig. 4]



[Fig. 5]

10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2022/016242

A. CLASSIFICATION OF SUBJECT MATTER**H04L 9/00**(2006.01)i; **G06F 5/01**(2006.01)i; **G06F 17/16**(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/00(2006.01); G06F 21/60(2013.01); G06F 21/62(2013.01); H04L 9/30(2006.01)

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: homomorphic permutation, ciphertext, noise, re-encrypting, decrypt

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WEI WU et al., 'Secure and Efficient Outsourced k-Means Clustering using Fully Homomorphic Encryption With Ciphertext Packing Technique', IEEE Transactions on Knowledge and Data Engineering, Volume: 33, Issue: 10, 27 January 2020 sections 2.1, 2.3.2, 4.2, 4.4; table 1; and figure 1	1-15
Y	US 2020-0252199 A1 (CRYPTO LAB INC.) 06 August 2020 (2020-08-06) paragraphs [0018], [0122], [0131]-[0134], [0138]; and figures 4-5	1-15
A	US 2015-0124962 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 07 May 2015 (2015-05-07) paragraphs [0286]-[0302]; and figures 7-8	1-15
A	US 2020-0327250 A1 (NOVO VIVO INC.) 15 October 2020 (2020-10-15) paragraphs [0432]-[0436]; and figure 30	1-15
A	US 2016-0191233 A1 (MICROSOFT TECHNOLOGY LICENSING, LLC) 30 June 2016 (2016-06-30) paragraphs [0032]-[0074]; and figures 2-4	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

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

"D" document cited by the applicant in the international application

"E" earlier application or patent but published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

14 February 2023

Date of mailing of the international search report

16 February 2023

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon
35208, Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

BYUN, Sung Cheal

Telephone No. +82-42-481-8262

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2022/016242

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2020-0252199	A1	06 August 2020	CN	110214433	A	06 September 2019
				CN	115134068	A	30 September 2022
				EP	3553995	A1	16 October 2019
				EP	3553995	B1	23 June 2021
				EP	3793127	A1	17 March 2021
				JP	2020-528232	A	17 September 2020
				JP	2022-059027	A	12 April 2022
				JP	7049374	B2	06 April 2022
				KR	10-1965628	B1	04 April 2019
				KR	10-2040106	B1	27 November 2019
				SG	10202100111	A	25 February 2021
				SG	11202001984	A	29 April 2020
				US	10778409	B2	15 September 2020
				US	11101976	B2	24 August 2021
				US	11115183	B2	07 September 2021
				US	2019-0363871	A1	28 November 2019
				US	2020-0162235	A1	21 May 2020
				WO	2019-117694	A1	20 June 2019
US	2015-0124962	A1	07 May 2015	US	10177905	B2	08 January 2019
				US	2012-0039463	A1	16 February 2012
				US	2012-0039465	A1	16 February 2012
				US	2012-0039473	A1	16 February 2012
				US	2013-0315390	A1	28 November 2013
				US	8532289	B2	10 September 2013
				US	8565435	B2	22 October 2013
				US	8903083	B2	02 December 2014
US	2020-0327250	A1	15 October 2020	US	8958555	B2	17 February 2015
				CN	113169957	A	23 July 2021
				US	11003791	B2	11 May 2021
US	2016-0191233	A1	30 June 2016	WO	2020-206695	A1	15 October 2020
				CN	105122721	A	02 December 2015
				CN	105122721	B	06 November 2018
				EP	2936731	A2	28 October 2015
				EP	2936731	B1	20 July 2016
				ES	2598298	T3	26 January 2017
				US	10211975	B2	19 February 2019
				US	2014-0177828	A1	26 June 2014
				US	9306738	B2	05 April 2016
				WO	2014-100788	A2	26 June 2014
				WO	2014-100788	A3	21 August 2014