



(51) International Patent Classification:

H04L 9/08 (2006.01)

H04L 9/06 (2006.01)

(21) International Application Number:

PCT/KR2020/001687

(22) International Filing Date:

06 February 2020 (06.02.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/806,430

15 February 2019 (15.02.2019)

US

10-2019-0144484

12 November 2019 (12.11.2019)

KR

(71) Applicants: **CRYPTO LAB INC.** [KR/KR]; 27-404, 1, Gwanak-ro, Gwanak-gu, Seoul 08826 (KR). **SEOUL NATIONAL UNIVERSITY R&DB FOUNDATION** [KR/KR]; 1, Gwanak-ro, Gwanak-gu, Seoul 08826 (KR).

(72) Inventors: **CHEON, Jung Hee**; 1, Gwanak-ro, Gwanak-gu, Seoul 08826 (KR). **JEONG, Jinhyuck**; 27-441, 1, Gwanak-ro, Gwanak-gu, Seoul 08826 (KR). **YHEE, Donggeon**; 192-11, Jungang-ro, Jeongeup-si, Jeollabuk-do 56164 (KR). **CHO, Wonhee**; 404, 82, Seorim-gil, Gwanak-gu, Seoul 08837 (KR).

(74) Agent: **KIM, Tae-hun**; 9th Floor, Shinduk Bldg., 343, Gangnam-daero, Seocho-gu, Seoul 06626 (KR).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, 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,

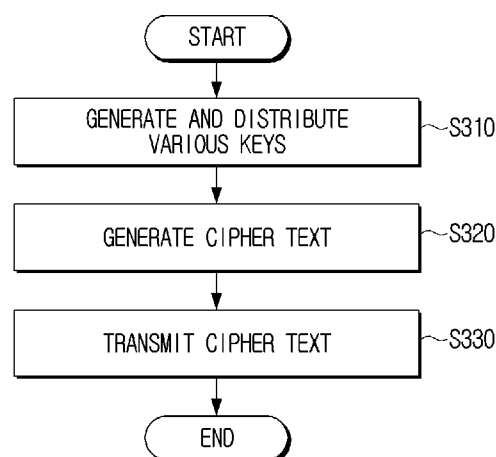
SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, 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))

(54) Title: APPARATUS FOR PERFORMING THRESHOLD DESIGN ON SECRET KEY AND METHOD THEREOF



(57) Abstract: An encryption method is disclosed. The encryption method includes calculating a secret key from a ring as a set closed for addition and multiplication defined between elements, generating a plurality of partial secret keys using the calculated secret key and a random matrix, and distributing the plurality of generated partial secret keys.

Description

Title of Invention: APPARATUS FOR PERFORMING THRESHOLD DESIGN ON SECRET KEY AND METHOD THEREOF

Technical Field

- [1] Apparatuses and methods consistent with the disclosure relate to an apparatus for performing threshold design on a secret key and a method thereof, and more particularly, to an apparatus for performing a threshold design on a secret key for an approximate cipher text and distributing the secret key, and a method thereof.

Background Art

- [2] As communication technologies have been developed and electronic devices have become actively prevalent, efforts have continuously been made to maintain communication security between electronic devices. Therefore, encryption/decryption technologies have been used in most communication environments.
- [3] Meanwhile, cipher text may be decrypted using secret keys, and recently, a threshold design (or a quorum design) is performed on the secret keys. Here, the threshold design is designed to distribute secret keys to everyone and to decrypt the cipher text only when a certain number of people gather.
- [4] In the related art, a Shamir secret key distribution scheme or $\{0, 1\}$ -linear secret sharing scheme (LSSS) has been used for the threshold design, but the related art scheme has a very large linear combination coefficient for recovering the secret keys, causing problems that a prime number q for decryption must satisfy certain conditions, and thus there are restrictions on q or the number of secret keys to be distributed to each person is very large.
- [5] In other words, a magnitude of prime numbers or the number of secret keys is restricted depending on a total number of people.

Disclosure of Invention

Technical Problem

- [6] Embodiments of the disclosure overcome the above disadvantages and other disadvantages not described above. Also, the disclosure is not required to overcome the disadvantages described above, and an embodiment of the disclosure may not overcome any of the problems described above.

Solution to Problem

- [7] The disclosure provides an apparatus for performing threshold design on secret keys for an approximate cipher text and distributing the secret keys, and a method thereof.

- [8] According to an embodiment of the disclosure, an encryption method includes: calculating a secret key from a ring as a set closed for addition and multiplication defined between elements; generating a plurality of partial secret keys using the calculated secret key and a random matrix; and distributing the plurality of generated partial secret keys.
- [9] The random matrix may have a number of rows corresponding to a number of users and a number of columns corresponding to a threshold.
- [10] The random matrix may have a number of rows corresponding to a number of users and a number of secret keys to be distributed to each user and a number of columns corresponding to a threshold.
- [11] In the distributing, the plurality of distribution secret keys may be distributed to each user.
- [12] In the generating, a plurality of random values may be generated and the plurality of partial secret keys may be generated by applying a vector matrix including the plurality of random values and the secret key to the random matrix.
- [13] The encryption method may further include: generating a public key using the secret key; and generating a cipher text using the generated public key.
- [14] The encryption method may further include: collecting partial decipher texts each generated by applying the cipher text to a partial secret key equal to or greater than a threshold; and decrypting a plaintext for the cipher text using the partial decipher texts equal to or greater than the threshold.
- [15] The encryption method may further include: collecting partial secret keys equal to or greater than a threshold, among the plurality of partial secret keys; and recovering the secret key using the collected partial secret keys.
- [16] According to another embodiment of the disclosure, an arithmetic operation device includes: a memory configured to store at least one instruction; and a processor configured to execute the at least one instruction, wherein the processor is configured to, by executing the at least one instruction, calculate a secret key from a ring as a set closed for addition and multiplication defined between elements, generate a plurality of partial secret keys using the calculated secret key and a random matrix, and distribute the plurality of generated partial secret keys.
- [17] The processor may be configured to generate a plurality of random values and generate the plurality of partial secret keys by applying a vector matrix including the plurality of random values and the secret key to the random matrix.
- [18] The random matrix may have a number of rows corresponding to a number of users and a number of secret keys to be distributed for each user and a number of columns corresponding to a threshold, and the processor may be configured to distribute the plurality of partial secret keys to each user.

[19] The processor may be configured to generate a public key using the secret key and generate a cipher text using the generated public key.

[20] The processor may be configured to collect partial decipher texts each generated by applying the cipher text to a partial secret key equal to or greater than a threshold and decrypt a plain text for the cipher text using the partial decipher texts equal to or greater than the threshold.

[21] According to diverse embodiments of the disclosure as described above, when the threshold is satisfied using a random matrix, a secret key is distributed to enable decryption, thereby further reducing a magnitude of the linear combination coefficient.

[22] Additional and/or other aspects and advantages of the invention will be set forth in part in the description which follows and, in part, will be obvious from the description, or may be learned by practice of the invention.

[23]

Advantageous Effects of Invention

[24]

-

Brief Description of Drawings

[25] The above and/or other aspects of the disclosure will be more apparent by describing certain embodiments of the disclosure with reference to the accompanying drawings, in which:

[26] FIG. 1 is a view illustrating a structure of a network system according to an embodiment of the disclosure;

[27] FIG. 2 is a block diagram illustrating a configuration of an arithmetic operation device according to an embodiment of the disclosure;

[28] FIG. 3 is a flowchart illustrating an example of a method of generating a cipher text of the disclosure;

[29] FIG. 4 is a flowchart illustrating an example of a method of generating a partial secret key of the disclosure; and

[30] FIG. 5 is a flowchart illustrating a method of decrypting a cipher text using a plurality of partial secret keys.

Best Mode for Carrying out the Invention

[31]

-

Mode for the Invention

[32] Hereinafter, the disclosure will be described in detail with reference to the accompanying drawings. Encryption/decryption may be applied to an information (data) transmission process performed in the disclosure, and expressions for describing the information (data) transmission process in the disclosure and claims should all be construed to include the case of encrypting/decrypting although not mentioned

separately. Expression in the form of "transmission (transfer) from A to B" or "reception by A from B" includes transmission (transfer) or reception by an intermediate medium and does not necessarily limited to only directly transmission (transfer) or reception from A to B.

- [33] In the description of the disclosure, the order of each step should be understood non-restrictively unless a preceding step must be performed before a subsequent step logically and temporally. That is, except for the exceptional case above, although a process described as a subsequent step is performed before a process described as a preceding step, it does not affect the essence of the disclosure and the scope of the disclosure should be defined regardless of order of steps. Also, description of "A or B" is defined to mean that both A and B are included, as well as selectively indicating any one of A and B. Also, the term "including" in this specification has a comprehensive meaning to further include another component in addition to elements enumerated to be included.
- [34] In this specification, only essential components necessary for the description of the disclosure are described and components not related to the essence of the disclosure are not mentioned. Also, only the mentioned components should not be construed to be included in an exclusive sense but should be construed in a non-exclusive sense to include any other component.
- [35] In this specification, the term "value" is defined as a concept including not only a scalar value but also a vector.
- [36] The mathematical operation and calculation of each step of the disclosure described hereinafter may be realized by a computer operation by a coding method known for corresponding operation or calculation and/or coding devised suitably for the disclosure.
- [37] Specific formulas described hereinafter are exemplarily described among various possible alternatives, and the scope of the disclosure should not be construed as being limited to the formulas mentioned in the disclosure.
- [38] For convenience of description, the following is assumed.
- [39] $a \leftarrow D$: Element a is selected according to distribution D .
- [40] $s_1, s_2 \in R$: Each of $S1$ and $S2$ is an element belonging to group R .
- [41] $\text{mod}(q)$: A modular operation is performed with element q .
- [42] $\lceil - \rceil$: The internal value is rounded off.
- [43] Hereinafter, various embodiments of the disclosure will be described in detail with reference to the accompanying drawings.
- [44] FIG. 1 is a view illustrating a configuration of a network system according to an embodiment of the disclosure.
- [45] Referring to FIG. 1, a network system may include a plurality of electronic devices

100-1 to 100-n, a first server device 200, and a second server device 300, and these components may be connected to each other via a network 10.

[46] The network 10 may be implemented in various types of wired/wireless communication networks, broadcast communication networks, optical communication networks, cloud networks, and the like, and each device may also be connected by a method such as Wi-Fi, Bluetooth, and near field communication (NFC), and the like, without a separate medium.

[47] In FIG. 1, a plurality of electronic devices 100-1 to 100-n are illustrated but the plurality of electronic devices may not necessarily be used and one device may be used. For example, the electronic devices 100-1 to 100-n may be implemented in various types of devices such as smartphones, tablets, game players, PCs, laptop PCs, home servers, secret kiosks, and the like, and may also be implemented in the form of a home appliance to which an IoT function is applied.

[48] A user may input various information through the electronic devices 100-1 to 100-n used by the user. The input information may be stored in the electronic devices 100-1 to 100-n but may be transmitted to and stored in an external device for the reason of storage capacity and security. In FIG. 1, the first server device 200 may serve to store such information, and the second server device 300 may serve to use some or all of the information stored in the first server device 200.

[49] Each of the electronic devices 100-1 to 100-n may homomorphically encrypt the input information and transmit the homomorphic cipher text to the first server device 200. For example, each of the electronic devices 100-1 to 100-n may homomorphically encrypt the input information using a public key and transmit a homomorphic cipher text to the first server device 200.

[50] In this case, each of the electronic devices 100-1 to 100-n may include encryption noise, i.e., an error, calculated in the process of performing the homomorphic encryption, in the cipher text. Accordingly, the homomorphic cipher text generated by each of the electronic devices 100-1 to 100-n may be generated in a form in which a resultant value including a message and an error value is restored when decrypted later using a secret key.

[51] For example, the homomorphic cipher text generated by the electronic devices 100-1 to 100-n may be generated in a form satisfying the following properties when decrypted using a secret key.

[52] [Equation 1]

[53] $\text{Dec}(\text{ct}, \text{sk}) = \langle \text{ct}, \text{sk} \rangle = M + e \pmod{q}$

[54] Here, $\langle, \rangle$ are usual inner products, ct is cipher text, sk is secret key, M is plaintext message, e is an encryption error value, and mod q is Modulus of cipher text. q should be chosen to be greater than a resultant value M obtained by multiplying the message

by a scaling factor Δ . If an absolute value of the error value e is smaller enough than M , then a decrypted value $M+e$ of the cipher text is a value that may replace an original message with the same precision in significant digit arithmetic operation. Among the decrypted data, an error may be disposed on the least significant bit s (LSB) side and M may be disposed on a second LSB side.

- [55] If a size of the message is too small or too large, the size of the message may be adjusted using a scaling factor. When the scaling factor is used, even a message in the form of a real number, as well as the form of an integer, may be encrypted, utilization may be significantly increased. In addition, by adjusting the size of the message using the scaling factor, a size of an area in which the messages exist, that is, an effective area, in the cipher text after the arithmetic operation is performed may also be adjusted.
- [56] According to an embodiment, the cipher text modulus q may be set and used in various forms. For example, the modulus of the cipher text may be set in the form of an exponential power $q=\Delta^L$ of the scaling factor Δ . If Δ is 2, q may be set to a value such as $q=2^{10}$.
- [57] The first server device 200 may store the received homomorphic cipher text in the cipher text form, without decrypting the received homomorphic cipher text.
- [58] The first server device 200 may generate a secret key and a public key for encryption and provide the generated public key to the plurality of electronic devices 100-1 to 100-n. Here, the first server device 200 may generate a plurality of partial secret keys for the secret key and provide the plurality of generated partial secret keys to the plurality of devices for stability.
- [59] For example, the first server device 200 may generate a plurality of partial secret keys having a threshold for the secret key described above. The first server device 200 may distribute the generated partial secret keys to the plurality of electronic devices 100-1 to 100-n. When the partial secret keys are used as described above, each of the plurality of electronic devices 100-1 to 100-n cannot perform decryption on the cipher text using only the partial secret keys of its own, and may perform decryption only when partial secret keys equal to or greater than a designed threshold gather (or only when the partial decipher texts equal to or greater than the threshold gather).
- [60] The second server device 300 may request a specific processing result for the homomorphic cipher text from the first server device 200. The first server device 200 may perform a specific arithmetic operation according to a request from the second server device 300, and then transmit a result to the second server device 300. As described above, the first server device 200 may be referred to as an arithmetic operation device in that it may perform an arithmetic operation.
- [61] For example, when the cipher texts $ct1$ and $ct2$ transmitted from the two electronic devices 100-1 and 100-2 are stored in the first server device 200, the second server

device 300 may request the sum of the information provided from the electronic devices 100-1 and 100-2, from the first server device 200. The first server device 200 may perform an arithmetic operation of summing the two cipher texts according to the request, and then transmit a resultant value $ct1+ct2$ to the second server device 300.

[62] In terms of the nature of the homomorphic cipher text, the first server device 200 may perform an arithmetic operation without decryption, and the resultant value is also in the cipher text form. In the disclosure, the resultant value obtained by the arithmetic operation is referred to as an arithmetic operation result cipher text.

[63] The second server device 300 may decrypt the received arithmetic operation result cipher text to obtain an arithmetic operation resultant value of data included in each homomorphic cipher text. Here, if the second server device 300 has a secret key, the second server 300 may immediately decrypt the received arithmetic operation result cipher text. However, if the second server device 300 has a partial secret key, the second server device 300 may perform decryption after restoring the secret key by collecting other partial secret keys equal to or greater than the threshold from other devices. Alternatively, the second server device 300 may collect partial decipher texts which is a decryption result using the partial secret key for the arithmetic operation result and may perform decryption using the partial decipher texts when the collected partial decipher texts are equal to or greater than the threshold. As described above, the second server device 300 may also be referred to as an arithmetic operation device in that it performs an arithmetic operation such as decryption on the cipher text.

[64] Meanwhile, although FIG. 1 illustrates a case that the first electronic device and the second electronic device perform encryption and the second server device performs decryption, the disclosure is not limited thereto.

[65] FIG. 2 is a block diagram illustrating a configuration of an arithmetic operation device according to an embodiment of the disclosure.

[66] In detail, in the system of FIG. 1, the devices that perform homomorphic encryption, such as the first electronic device and the second electronic device, the device that arithmetically operates the homomorphic cipher text, such as the first server device or the like, the device that decrypts the homomorphic cipher text, such as the second server device, and the like may be referred to as arithmetic operation devices. The arithmetic operation devices may include various devices such as a personal computer, a notebook computer, a smartphone, a tablet, a server, and the like.

[67] Referring to FIG. 2, the arithmetic operation device 400 may include a communication device 410, a memory 420, a display 430, an operation input device 440, and a processor 450.

[68] The communication device 410 is provided to connect the arithmetic operation device 400 to an external device (not shown), and here, the communication device 410

may be connected to an external device via a local area network (LAN) and the internet or may be connected to the external device through a universal serial bus (USB) port or a wireless communication (e.g., Wi-Fi 802.11a/b/g/n, NFC, Bluetooth) port. The communication device 410 may also be referred to as a transceiver.

- [69] The communication device 410 may receive a public key from an external device and transmit a public key generated by the arithmetic operation device 400 itself to the external device.
- [70] In addition, the communication device 410 may transmit a secret key or a partial secret key generated by the arithmetic operation device 400 itself to an external device. Alternatively, the communication device 410 may receive a partial secret key from an external device.
- [71] The communication device 410 may receive a message from an external device and transmit a generated homomorphic cipher text to the external device. The communication device 410 may receive a partial decipher text decrypted with a partial secret key from the external device or transmit a partial decipher text decrypted with the partial secret key stored by the arithmetic operation device 400 to the external device.
- [72] In addition, the communication device 410 may receive various parameters necessary for generating a cipher text from an external device. Meanwhile, in the implementation, various parameters may be directly input from the user through the operation input device 440 to be described later.
- [73] In addition, the communication device 410 may receive a request for an arithmetic operation on the homomorphic cipher text from the external device and transmit a calculated result to the external device.
- [74] At least one instruction regarding the arithmetic operation device 400 may be stored in the memory 420. In detail, various programs (or software) for the arithmetic operation device 400 to operate may be stored in the memory 420 according to various embodiments of the disclosure.
- [75] The memory 420 may be implemented in various forms such as a random access memory (RAM), a read-only memory (ROM), a flash memory, a hard disk drive (HDD), an external memory, a memory card, and the like, but is not limited thereto.
- [76] The memory 420 may store a message to be encrypted. Here, the message may be various credit information, personal information, and the like quoted by the user or may be information related to a usage history such as location information and Internet usage time information used in the arithmetic operation device 400.
- [77] The memory 420 may store a public key. If the arithmetic operation device 400 is a device that directly generates a public key, the memory 420 may store various parameters necessary for generating a public key and a secret key, as well as the secret key.

- [78] In addition, if the arithmetic operation device 400 directly performs a threshold design, the memory 420 may store a plurality of partial secret keys for a secret key and store a partial secret key received from an external device. Meanwhile, according to an embodiment, one arithmetic operation device 400 may store a predetermined number of partial secret keys.
- [79] In addition, the memory 420 may store a homomorphic cipher text generated in a process to be described later. The memory 420 may store a homomorphic cipher text transmitted from an external device. In addition, the memory 420 may store an arithmetic operation result cipher text which is a result of the arithmetic operation as described later.
- [80] The memory 420 may store a partial decipher text decrypted using the partial secret key or store a partial decipher text received from an external device.
- [81] The display 430 displays a user interface window for selecting a function supported by the arithmetic operation device 400. Specifically, the display 430 may display a user interface window for selecting various functions provided by the arithmetic operation device 400. The display 430 may be a monitor such as a liquid crystal display (LCD), an organic light emitting diode (OLED), or the like or may be implemented as a touch screen capable of simultaneously performing a function of the operation input device 440 to be described later.
- [82] The display 430 may display a message requesting input of a parameter required for generating a secret key and a public key. In addition, the display 430 may display a message requesting input of a parameter required for threshold design. Here, the parameter required for the threshold design may be the number of users who are to be provided with the partial secret key, the number of partial secret keys to be provided to each user, and the threshold (i.e., a predetermined number of decryptable partial secret keys).
- [83] In addition, the display 430 may display a message in which an encryption target selects a message. Meanwhile, when implemented, the encryption target may be directly selected by the user or may be automatically selected. That is, personal information requiring encryption may be automatically set even if the user does not directly select a message.
- [84] The operation input device 440 may receive selection of a function of the arithmetic operation device 400 and a control command for the corresponding function from the user. Specifically, the operation input device 440 may receive a parameter required for generating a secret key and a public key from the user. In addition, the operation input device 440 may receive a parameter for threshold design from the user. In addition, the operation input device 440 may receive a message to be encrypted from the user.
- [85] The processor 450 controls an overall operation of the arithmetic operation device

400. Specifically, the processor 450 may control the overall operation of the arithmetic operation device 400 by executing at least one instruction stored in the memory 420. The processor 450 may be configured as a single device such as a central processing unit (CPU) or an application-specific integrated circuit (ASIC) or may include a plurality of devices such as the CPU and a graphics processing unit (GPU).

[86] When a message to be transmitted is input, the processor 450 may store the message in the memory 420. The processor 450 may homomorphically encrypt the message using various set values and programs stored in the memory 420. In this case, the public key may be used.

[87] The processor 450 may generate a public key required for performing encryption by itself and use the public key or may receive the public key from an external device and use the same. For example, the second server device 300 that performs decryption may distribute the public key to other devices.

[88] When generating a secret key by itself, the processor 450 may generate the public key using a Ring-LWE technique. Specifically, the processor 450 may first set various parameters and rings and store the set parameters and rings in the memory 420. Examples of parameters may include a length of bits of a plain text, sizes of the public key and the secret key, and the like.

[89] The ring may be expressed by the following equation.

[90] [Equation 2]

$$[91] \quad R = \mathbb{Z}_q[x]/(f(x))$$

[92] Here R denotes a ring, $\mathbb{Z}_q$ denotes a coefficient, and $f(x)$ is an nth order polynomial.

[93] The ring, as a set of polynomials with predetermined coefficients, refers to set in which addition and multiplication are defined between elements and which is closed for addition and multiplication. Such a ring may be referred to as a ring.

[94] As an example, the ring refers to a set of n-th polynomials whose coefficient is $\mathbb{Z}_q$. Specifically, the ring refers to N-th cyclotomic polynomial when n is $\Phi(N)$. $(f(x))$ denotes an ideal of $\mathbb{Z}_q[x]$ produced by (x) . The Euler's totient function $\Phi(N)$ refers to the number of natural numbers which are relatively prime with N and smaller than N. If $\Phi_N(x)$ is defined as the N-th cyclotomic polynomial, the ring may also be expressed as Equation 3 below.

[95] [Equation 3]

$$[96] \quad R = \mathbb{Z}_q[x]/(\Phi_N(x))$$

[97] Meanwhile, the ring of Equation 3 described above has a complex number in a plain text space. Meanwhile, in order to improve an arithmetic operation speed for the homomorphic cipher text, only a set in which the plain text space is a real number, in the set of the ring described above, may also be used.

- [98] When such a ring is established, the processor 450 may calculate a secret key sk from the ring.
- [99] [Equation 4]
- [100] $sk \leftarrow (1, s(x)), s(x) \in R$
- [101] Here, $s(x)$ denotes a polynomial generated randomly with a small coefficient.
- [102] The processor 450 calculates a first random polynomial $a(x)$ from the ring. The first random polynomial may be expressed as follows.
- [103] [Equation 5]
- [104] $a(x) \leftarrow R$
- [105] In addition, the processor 450 may calculate an error. Specifically, the processor 450 may extract an error from a discrete Gaussian distribution or a distribution having a statistical distance close thereto. This error may be expressed as follows.
- [106] [Equation 6]
- [107] $e(x) \leftarrow D_{\alpha q}^n$
- [108] When the error is calculated, the processor 450 may calculate a second random polynomial by performing a modular operation on the first random polynomial and the secret key error. The second random polynomial may be expressed as follows.
- [109] [Equation 7]
- [110] $b(x) = -a(x)s(x) + e(x) \pmod{q}$
- [111] Finally, the public key pk is set in a form including the first random polynomial and the second random polynomial as follows.
- [112] [Equation 8]
- [113] $pk = (b(x), a(x))$
- [114] The method of generating the secret key described above is merely an example, and thus the disclosure is not limited there and the public key and the secret key may be generated in other ways.
- [115] Meanwhile, in case of only one secret key, leakage of the secret key may cause a big security problem. Therefore, there is a need to improve security by allowing a plurality of users or a plurality of devices, instead of one user (or one device), to store the secret key separately.
- [116] In case of using the public key encryption (PKE)-based learning with error (LWE) as described above, the cipher text (c) is a vector in $\mathbb{Z}_q^{m+1}$ and the secret key (sk) is also a vector in $\mathbb{Z}_q^m$ having a decoding structure ($\langle c, sk \rangle = m \cdot \left\lfloor \frac{q}{2} \right\rfloor + e^*$).
- [117] If $\langle c, sk \rangle$ is small enough, a decryption output value may be 0, otherwise it may have a value of 1.

[118] Meanwhile, if a set of participants is assumed to be $P=(P_1, \dots, P_N)$ and a linear secret key sharing scheme is applied to the secret key (sk), then secret keys $sk_1, \dots, sk_N$ may be distributed to N people. For convenience of description, hereinafter, the secret keys $sk_1, \dots, sk_N$ generated according to the application of the linear secret key sharing scheme will be referred to as partial secret keys.

[119] In this case, when a combiner calculates recovery coefficients $\lambda=(\lambda_i)_{i \in I}$, a subset $I \subset |N|$ greater than t is expressed by Equation 9 below. Here, t is a threshold.

[120] [Equation 9]

$$[121] \quad \langle c, sk \rangle = \langle c, \sum_{i \in I} \lambda_i sk_i \rangle = \sum_{i \in I} \lambda_i \cdot \langle c, sk_i \rangle$$

[122] Accordingly, each user may perform partial decryption ($p_i = \langle c, sk_i \rangle + e_i$) with an error.

[123] Therefore, the sum of the decryption result using the partial secret key may be expressed as in Equation 10 below.

[124] [Equation 10]

$$[125] \quad \begin{aligned} \sum_{i \in I} \lambda_i P_i &= \langle c, sk \rangle + \sum_{i \in I} \lambda_i e_i \\ &= m \cdot \left\lfloor \frac{q}{2} \right\rfloor + e^* + \sum_{i \in I} \lambda_i e_i \end{aligned}$$

[126] Therefore, referring to Equation 10, if the error $[e^* + \sum_{i \in I} \lambda_i e_i]_q$ is designed to be small enough, it is possible to distribute and use the secret key to have a threshold.

[127] Meanwhile, in the related art, the Shamir secret key distribution scheme and the $\{0,1\}$ -LSSS scheme are used for the threshold design described above. However, the Shamir secret key distribution scheme has a problem that the linear combination coefficient λ for recovering the secret key s is very large due to LaGrange Interpolation, so that the prime q must be greater than $(N!)^3$, which is, thus, severely restricted. In addition, the $\{0,1\}$ -LSSS scheme has a disadvantage in that the number of secret keys to be distributed is $O(N^{4.2})$ which is very large.

[128] Accordingly, the disclosure uses a new secret key sharing method that may reduce both the magnitude of the prime and the number of secret keys. Specifically, two costs must be low enough to design a threshold for LWE. The proposed method is to grow a gray area such that the number of partial secret keys collected from t participants is greater than or equal to a predetermined value (i.e., the threshold) required for recovering the secret key.

[129] Accordingly, the disclosure proposes a so-called "subset secret key method" that provides a basic configuration of the LSSS having a small recovery coefficient using

an inhomogeneous small integer solution (ISIS) issue and generalizes the basic configuration.

[130] If it is assumed that a set of secret keys S_i is distributed to each user P_i to satisfy t out of N , n_i is the number of secret sharers collected from a certain i subset of $\{S_1, \dots, S_N\}$ and Δn_i is $n_i - n_{i-1}$ for $i = 1, \dots, N$.

[131] Also, when $\hat{t} = n_{t-1} + 1$ is set, t out of N LSSS is configured in a shared matrix $U \in \mathbb{Z}_q^{n_N \times \hat{t}}$, and $I \subset \{1, \dots, N\}$ with $|I| = t$ is considered, a main purpose is to find $\lambda \in \mathbb{Z}_q^{n_t}$ such as $\|\lambda\|_2 \leq B$, $\lambda \cdot U_I = (1, 0, \dots, 0)$.

[132] Here, U_I is a matrix in $\mathbb{Z}_q^{n_t \times \hat{t}}$ obtained from a shared matrix having columns related to a member $\{p_i\}_{i \in I}$.

[133] When a partial solution λ_0 of $L = \{\lambda \in \mathbb{Z}^{n_t} \mid \lambda \cdot U_I = 0 \pmod{q}\}$ and $\lambda \cdot U_I = (1, 0, \dots, 0)$ is fixed, the above-described equation is also satisfied for $\lambda' \in L$, $\lambda_0 - \lambda'$.

[134] Therefore, if $\dim L = n_t$, $L = q^{\hat{t}}$, λ' is expressed by Equation 11 below.

[135] [Equation 11]

$$[136] \quad \|\lambda := \lambda_0 - \lambda'\|_2 \leq \frac{\sqrt{n_t}}{2} \cdot \sqrt{q^{\hat{t}}} \cdot q^{\hat{t}/n_t} = \frac{n_t}{2} \cdot q^{1 - \frac{\Delta n_t - 1}{2}}$$

[137] Here, it is assumed that the shared matrix U is selected from a uniform distribution to use Gaussian heuristics. For example, an LLL algorithm may be used to find λ . For a sufficiently small t , Minkowski's bound may be used to estimate a bound. Meanwhile, if t is large, an LLL bound should be used. Hereinafter, how to make $(\Delta n_t - 1)/n_t$ large using some methods will be described.

[138] Basically, considering a simple case of $|S_i| = w = O(1)$ when $n_t = wt$ and $\Delta n_t = w$, n_t and Δn_t are $O(t)$ and $O(1)$, respectively.

[139] Meanwhile, because $\|e^* + \sum_{i \in I} \lambda_i e_i\|_q$ is small in Equation 10 and $\|e^* + \sum_{i \in I} \lambda_i e_i\|_q \leq \|e^*\| + \|\lambda\| \|e\|$, the condition of Equation 12 below should be satisfied for accuracy of cryptography when the contents of the disclosure is applied to a $\{-B, B\}$ -LSSS scheme.

[140] [Equation 12]

$$[141] \quad B_c + B \cdot B_{sm} < q/4$$

[142] Here, B_c and B_{sm} are upper error limits for valid cipher text and partial decipher text, respectively.

[143] If two upper limits are assumed to be fixed, this condition provides a bound of a modulus magnitude q for a given t .

[144] Because B_c is much smaller than q and the inequality ($B \geq \frac{n_t}{2} \cdot q^{1 - \frac{\Delta n_t - 1}{n_t}}$), an

anymptotic bound of t may be analyzed as follows.

[145] [Equation 13]

$$[146] \quad \frac{n_t}{2} \cdot q^{1 - \frac{\Delta n_{t-1}}{n_t}} \cdot B_{sm} < q/4 \iff 2n_t \cdot B_{sm} < q^{\frac{\Delta n_{t-1}}{n_t}} \\ \iff (2n_t \cdot B_{sm})^{\frac{n_t}{\Delta n_{t-1}}} < q$$

[147] In the disclosure, $(2n_t \cdot B_{sm})^{\frac{n_t}{\Delta n_{t-1}}}$ is $O(t^{(1+\delta)t})$ with small δ . Similarly, the LLL bound is $O(2^t)$.

[148] In consideration of the foregoing, in the disclosure, a plurality of partial secret keys may be distributed to each device.

[149] When a secret key is generated, the processor 450 may generate a plurality of partial secret keys using the generated secret key s and a random matrix. For example, the processor 450 may generate a plurality of random values $(S_2, S_3, \dots, S_{n_{t-1}+1})$, define vector $\vec{S} = (S, S_2, \dots, S_{n_{t-1}+1})^T$ using the secret key s and the random values $s_2, s_3, \dots, S_{n_{t-1}+1}$, and generate a plurality of partial secret keys $\vec{p}$ by reflecting the defined vector on a following random matrix.

[150] [Equation 14]

$$[151] \quad A = \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n_t-1} & a_{1,n_t-1+1} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n_t-1} & a_{2,n_t-1+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \square & \square & \dots & \square & \square \\ a_{n_N,1} & a_{n_N,2} & \dots & a_{n_N,n_t-1} & a_{n_N,n_t-1+1} \end{bmatrix}$$

[152] Here, A is a random matrix and n_i is the number of secret keys gathered when i people gather.

[153] Meanwhile, such a random matrix may have the number of rows corresponding to the number of users and the number of columns corresponding to the threshold, and in particular, the rows may have a value of a product of the number of users and the number of secret keys to be distributed to each user.

[154] Meanwhile, in the disclosure, it is possible to decrypt a secret key in the case of having a threshold, and here, the secret key cannot be recovered when $t-1$ people gather and can be recovered only when t or more people gather. If a matrix when t people gather to obtain the linear combination coefficient is A_t , the matrix A_t may be expressed by Equation 15 below.

[155] [Equation 15]

[156]

$$A_t = \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n_t-1} & a_{1,n_t-1+1} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n_t-1} & a_{2,n_t-1+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \square & \square & \dots & \square & \square \\ a_{n_t,1} & a_{n_t,2} & \dots & a_{n_t,n_t-1} & a_{n_t,n_t-1+1} \end{bmatrix}$$

- [157] As described above, because the disclosure uses the random matrix, Gaussian heuristics $\lambda_1 \approx \lambda_2 \approx \dots \approx \lambda_{n_t}$ in which sizes of the successive minima of the lattice are all similar may be established in an orthogonal matrix A_t^+ for A_t described above.
- [158] Therefore, an upper bound of the magnitude of $\{\lambda_i\}$ may be given through the Lattice reduction algorithm or Minkowski's Bound, and the upper bound of the magnitude of the linear combination coefficient $\{v_i\}$ may be calculated by applying the upper bound to Babai's algorithm.
- [159] Meanwhile, in case of making a difference by distributing w secret keys per person when implemented, the random matrix may have Nw rows and $(t-1)w+1$ columns. Alternatively, in case of making a difference by distributing a secret key to each set including k people among N people, the random matrix may have $\begin{pmatrix} N \\ k \end{pmatrix}$ rows and $\begin{pmatrix} t-1 \\ k \end{pmatrix} + 1$ columns.
- [160] In case of distributing the partial secret keys in this manner, because the values of n_t and $n_{t-1}+1$ are different, the linear combination coefficient $\{v_i\}$ is not uniquely determined. Therefore, Babai's nearest plane algorithm may be used to find the upper bound of the magnitude of the linear combination coefficient $\{v_i\}$.
- [161] Meanwhile, the existing threshold design is defined such that a secret key cannot be recovered when $t-1$ or less gather and recovered when t or more gather. According to the disclosure, a weaker definition may also be applied for efficiency. That is, in case that a secret key is distributed such that the secret key cannot be recovered if $t-c$ or less, other than t , gather for a certain constant c and can be recovered if t or more gather, then the matrix A_t becomes a $n_t \times \{n_{t-c}+1\}$ matrix and a difference between rows and columns is larger, making the linear combination coefficient $\{v_i\}$ smaller.
- [162] In addition, the processor 450 may control the communication device 410 to transmit the generated partial secret key to other devices. Here, the processor 450 may control the communication device 410 to transmit a plurality of partial secret keys to each device.
- [163] When the public key is generated, the processor 450 may control the communication device 410 to transmit the public key to other devices.
- [164] The processor 450 may generate a homomorphic cipher text for a message. For example, the processor 450 may generate the homomorphic cipher text by applying the

previously generated public key to the message. Here, the processor 450 may generate the cipher text to have a length corresponding to a size of a scaling factor.

[165] When the homomorphic cipher text is generated, the processor 450 may control the communication device 410 to store the generated cipher text in the memory 420 or transmit the cipher text to another device according to a user request or a predetermined default command.

[166] Meanwhile, according to an embodiment of the disclosure, packing may be performed. The use of packing in homomorphic encryption makes it possible to encrypt multiple messages in a single cipher text. In this case, when an arithmetic operation is performed between the cipher texts in the arithmetic operation device 400, an arithmetic operation burden is significantly reduced because the arithmetic operation is performed on a plurality of messages in parallel.

[167] Specifically, when a message includes a plurality of message vectors, the processor 450 may convert the plurality of message vectors into a polynomial that may be encrypted in parallel, and then multiply the polynomial by a scaling factor, and perform homomorphic encryption thereon using a public key. Accordingly, a cipher text packing a plurality of message vectors may be generated.

[168] When the homomorphic cipher text is required to be decrypted, the processor 450 may generate a polynomial decipher text by applying a secret key to the homomorphic cipher text and generate a message by decoding the polynomial decipher text. Here, the generated message may include an error as mentioned in Equation 1 described above.

[169] Meanwhile, in case of having the partial secret key, the processor 450 may control the communication device 410 to generate a partial decipher text using the partial secret key for the homomorphic cipher text and transmit the generated partial decipher text to another device, or may decrypt the message for the cipher text by collecting a predetermined number (i.e., threshold) of partial decipher texts or more provided from other devices.

[170] In addition, when the processor 450 has the partial secret key, the processor 450 may collect the partial secret keys equal to or greater than the threshold from other devices and generate a secret key using the collected partial secret keys. In addition, the processor 450 may decrypt the message using the generated secret key.

[171] The processor 450 may perform an arithmetic operation on the cipher text. Specifically, the processor 450 may perform an arithmetic operation such as addition, subtraction, or multiplication, while maintaining the encrypted state regarding the homomorphic cipher text.

[172] When the arithmetic operation is completed, the arithmetic operation device 400 may detect data of a valid area from arithmetic operation result data. Specifically, the arithmetic operation device 400 may perform a rounding process on the arithmetic

operation result data to detect data of a valid area. The rounding process refers to round-off of a message in an encrypted state. Alternatively, the rounding process may also be referred to as rescaling.

- [173] In addition, when a portion of an approximation message in the arithmetic operation result cipher text exceeds a threshold, the arithmetic operation device 400 may perform a rebooting operation on the cipher text.
- [174] As described above, the arithmetic operation device 400 according to the present embodiment generates the partial secret keys that satisfy the threshold using the random matrix, thereby further reducing the size of the linear combination coefficient required for recovering the secret key. Further, because the arithmetic operation device 400 distributes a plurality of partial secret keys to each user, which is advantageous when N is very large compared to t .
- [175] Hereinafter, a trade-off method according to threshold design will be described.
- [176] First, it is assumed that there is a (t, N) -threshold design that distributes c partial secret keys to each person. According to this, $2N$ people may be divided into two groups P_0 and Q_0 to create a $(2t, 2N)$ -threshold design.
- [177] Also, $P_N = Q_C$, $Q_N = P_C$ may be easily checked when $P_i = \{b_1, \dots, b_i, a_{i+1}, \dots, a_N\}$, $Q_i = \{a_1, \dots, a_i, b_{i+1}, \dots, b_N\}$ is defined.
- [178] Here, the secret key s may be divided by $s = x_i - y_i$ and (t, N) - threshold design having secret keys as x_i, y_i to $\{P_i, Q_i\}$.
- [179] If $2t-1$ people or less gather, any $\{P_i, Q_i\}$ pair cannot recover all the secret keys x_i, y_i , so the secret key s cannot be recovered. If $2t$ people or more gather, at least one of N people $N \setminus \{P_i, Q_i\}$ may recover the secret key x_i, y_i , so the secret key s may be recovered.
- [180] Thus, if a (t, N) - threshold design for distributing c secret keys to each person exists, a $(2t, 2N)$ threshold design for distributing cN secret keys to each person may also be created.
- [181] FIG. 3 is a flowchart illustrating an example of a method of generating a cipher text of the disclosure.
- [182] Referring to FIG. 3, a secret key and a public key may be generated (S310). Specifically, a ring may be set, a secret key may be generated through the set ring, and a public key may be generated using the generated secret key. Here, for threshold design, a plurality of partial secret keys may be generated using the secret key. A specific operation of generating the partial secret keys will be described later with reference to FIG. 4.
- [183] Thereafter, the cipher text may be generated using the generated public key (S320). For example, a homomorphic cipher text may be generated by applying a public key to

a message.

- [184] The generated cipher text may be transmitted (S330). The generated homomorphic cipher text may be stored or transmitted to another device.
- [185] FIG. 4 is a flowchart illustrating an example of a method of generating a partial secret key of the disclosure.
- [186] Referring to FIG. 4, a secret key may be calculated (S410). Specifically, addition and multiplication are defined between elements, and a secret key may be calculated from a ring which is a set closed for addition and multiplication.
- [187] A plurality of partial secret keys may be generated using the calculated secret key and a random matrix (S420). Specifically, a plurality of random values may be generated and a plurality of partial secret keys may be generated by applying vector matrix including the plurality of random values and the secret key to a random matrix. Here, the random matrix may have the number of rows corresponding to the number of users and the number of columns corresponding to the threshold. The random matrix may have the number of users and the number of rows corresponding to the number of secret keys to be distributed to each user so that a plurality of secret keys may be distributed to each user.
- [188] The plurality of generated partial secret keys may be distributed (S430). Specifically, in case of distributing the plurality of secret keys to each user, the plurality of generated partial secret keys may be distributed to each user.
- [189] FIG. 5 is a flowchart illustrating a method of decrypting a cipher text using a plurality of partial secret keys.
- [190] Referring to FIG. 5, first, partial decipher texts equal to or greater than a threshold for the cipher text using a partial secret key is collected (S510). Specifically, as described above, message may be decrypted when the secret keys equal to or greater than the threshold are collected, and thus, an arithmetic operation device may collect the partial secret keys equal to or greater than the threshold or the partial decipher texts equal to or greater than the threshold.
- [191] If the partial decipher texts equal to or greater than the threshold are not collected (S520-N), the collecting operation described above may be repeated, and if the partial decipher texts equal to or greater than the threshold are not collected within a predetermined time, the decrypting operation may be terminated or an error may be notified.
- [192] If the partial decipher texts equal to or greater than the threshold are collected (S520-Y), the collected partial decipher texts may be linearly combined to decrypt the message (S530).
- [193] Meanwhile, although decrypting the message using the partial decipher texts equal to or greater than the threshold is described, in case of implementation, after the partial secret keys equal to or greater than the threshold are collected, a secret key may be

generated using the collected partial secret keys, and a homomorphic cipher text may be decrypted using the generated secret key.

[194] Meanwhile, the method of processing a cipher text according to various embodiments described above may be implemented in the form of a program code for performing each step and may be stored in a recording medium and distributed. In this case, a device in which the recording medium is mounted may perform the operations such as encryption, cipher text processing, or the like described above.

[195] The recording medium may be various types of computer-readable mediums such as ROM, RAM, memory chip, memory card, external hard disk, hard disk, CD, DVD, magnetic disk, or magnetic tape.

[196] While the disclosure has been described with reference to the accompanying drawings, it is to be understood that the scope of the disclosure is defined by the claims described hereinafter and should not be construed as being limited to the above-described embodiments and/or drawings. It is to be clearly understood that improvements, changes, and modifications that are obvious to those skilled in the art are also within the scope of the disclosure as defined in the claims.

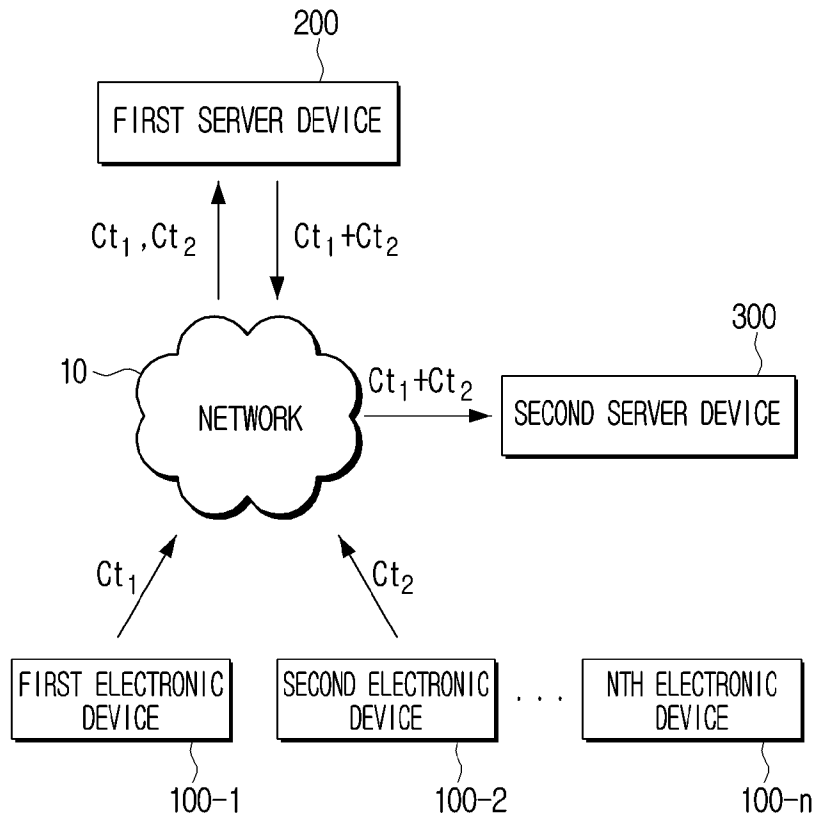
Claims

- [Claim 1] An encryption method comprising:
calculating a secret key from a ring as a set closed for addition and multiplication defined between elements;
generating a plurality of partial secret keys using the calculated secret key and a random matrix; and
distributing the plurality of generated partial secret keys.
- [Claim 2] The encryption method as claimed in claim 1, wherein
the random matrix has a number of rows corresponding to a number of users and a number of columns corresponding to a threshold.
- [Claim 3] The encryption method as claimed in claim 1, wherein
the random matrix has a number of rows corresponding to a number of users and a number of secret keys to be distributed to each user and a number of columns corresponding to a threshold.
- [Claim 4] The encryption method as claimed in claim 3, wherein
in the distributing, the plurality of distribution secret keys is distributed to each user.
- [Claim 5] The encryption method as claimed in claim 1, wherein
in the generating, a plurality of random values is generated and the plurality of partial secret keys are generated by applying a vector matrix including the plurality of random values and the secret key to the random matrix.
- [Claim 6] The encryption method as claimed in claim 1, further comprising:
generating a public key using the secret key; and
generating a cipher text using the generated public key.
- [Claim 7] The encryption method as claimed in claim 6, further comprising:
collecting partial decipher texts each generated by applying the cipher text to a partial secret key equal to or greater than a threshold; and
decrypting a plain text for the cipher text using the partial decipher texts equal to or greater than the threshold.
- [Claim 8] The encryption method as claimed in claim 1, further comprising:
collecting partial secret keys equal to or greater than a threshold, among the plurality of partial secret keys; and
recovering the secret key using the collected partial secret keys.
- [Claim 9] An arithmetic operation device comprising:
a memory configured to store at least one instruction; and
a processor configured to execute the at least one instruction,

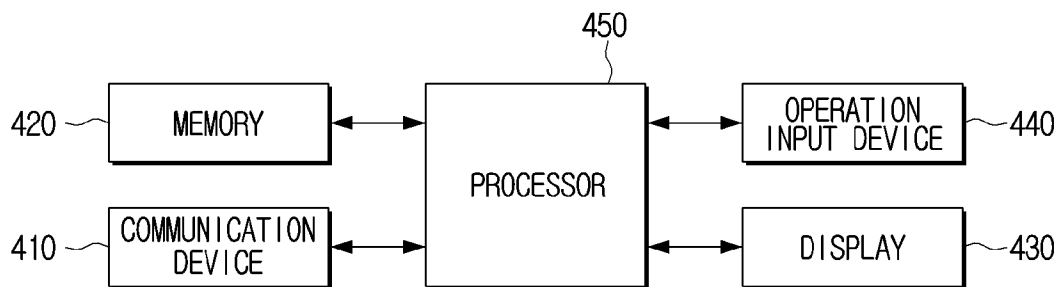
wherein the processor, by executing the at least one instruction, calculates a secret key from a ring as a set closed for addition and multiplication defined between elements, generates a plurality of partial secret keys using the calculated secret key and a random matrix, and distributes the plurality of generated partial secret keys.

- [Claim 10] The arithmetic operation device as claimed in claim 9, wherein the processor generates a plurality of random values and generate the plurality of partial secret keys by applying a vector matrix including the plurality of random values and the secret key $*$ to the random matrix.
- [Claim 11] The arithmetic operation device as claimed in claim 9, wherein the random matrix has a number of rows corresponding to a number of users and a number of secret keys to be distributed for each user and a number of columns corresponding to a threshold, and the processor is configured to distribute the plurality of partial secret keys to each user.
- [Claim 12] The arithmetic operation device as claimed in claim 9, wherein the processor generates a public key using the secret key and generate a cipher text using the generated public key.
- [Claim 13] The arithmetic operation device as claimed in claim 12, wherein the processor collects partial decipher texts each generated by applying the cipher text to a partial secret key equal to or greater than a threshold and decrypts a plain text for the cipher text using the partial decipher text equal to or greater than the threshold.

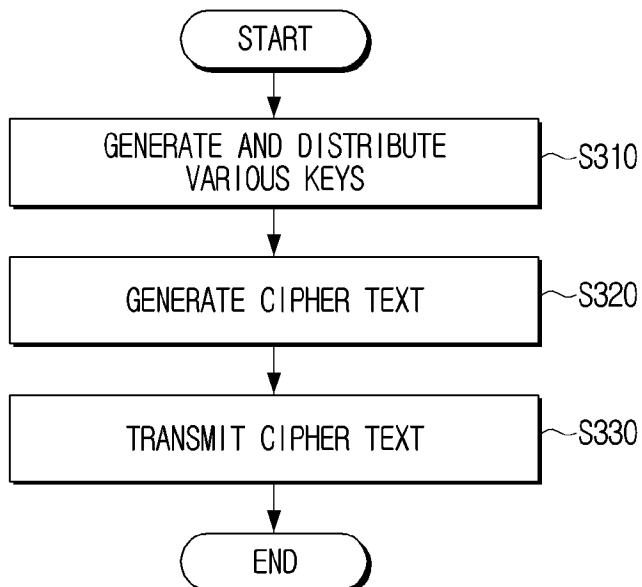
[Fig. 1]



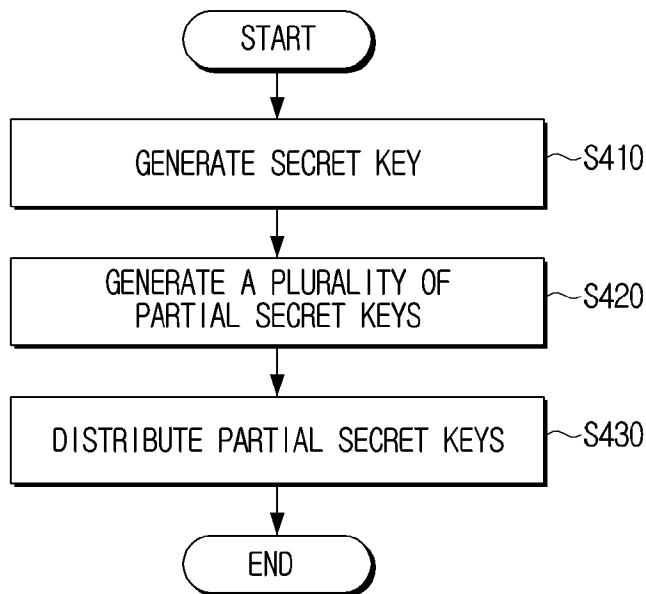
[Fig. 2]

400

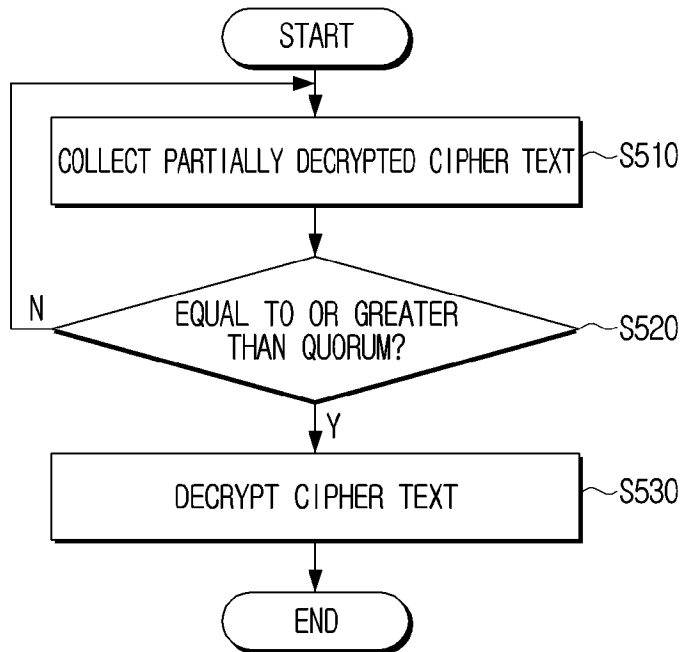
[Fig. 3]



[Fig. 4]



[Fig. 5]



A. CLASSIFICATION OF SUBJECT MATTER**H04L 9/08(2006.01)i, H04L 9/06(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 9/08; G06F 21/60; G06F 21/62; H04L 9/00; H04L 9/06; H04L 9/30; H04L 9/32

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: calculate, secret key, partial, random matrix, share, distribute

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	STANISLAW SPIEZ et al. Secret Sharing Matrixes, INSTITUTE OF MATHEMATICS OF THE POLISH ACADEMY OF SCIENCES, 09 September 2009 Pages 1-3 and 15.	1-13
Y	KR 10-2007-0011293 A (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) 24 January 2007 Paragraph [0112]; claims 1, 18; and figure 6	1-13
Y	JP 2009-033608 A (NTT DOCOMO INC et al.) 12 February 2009 Paragraphs [0014], [0036]; and figure 1	7, 13
A	US 2017-0053132 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 23 February 2017 Paragraphs [0047], [0093], [0126]-[0127], [0133]-[0139]; claims 1, 5; and figure 1	1-13
A	US 2016-0119119 A1 (XEROR CORPORATION) 28 April 2016 Paragraphs [0009], [0062], [0091]; and figure 1	1-13



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

18 May 2020 (18.05.2020)

Date of mailing of the international search report

19 May 2020 (19.05.2020)

Name and mailing address of the ISA/KR

International Application Division

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/KR2020/001687

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 10-2007-0011293 A	24/01/2007	CN 1922643 A EP 1746561 A1 JP 4786531 B2 US 2007-0274518 A1 US 7773746 B2 WO 2005-109379 A1	28/02/2007 24/01/2007 05/10/2011 29/11/2007 10/08/2010 17/11/2005
JP 2009-033608 A	12/02/2009	JP 5142361 B2	13/02/2013
US 2017-0053132 A1	23/02/2017	EP 2718826 A1 US 10127402 B2 US 10255135 B2 US 10395054 B2 US 10558819 B2 US 2011-0126295 A1 US 2012-0311345 A1 US 2012-0311346 A1 US 2012-0311395 A1 US 2012-0311557 A1 US 2013-0232378 A1 US 2013-0238565 A1 US 2013-0238932 A1 US 2014-0164877 A1 US 2014-0331065 A1 US 2014-0331100 A1 US 2014-0337684 A1 US 2018-0018232 A1 US 2018-0089029 A1 US 2019-0278936 A1 US 8656253 B2 US 8782439 B2 US 8918897 B2 US 8965939 B2 US 9110593 B2 US 9152514 B2 US 9270298 B2 US 9465824 B2 US 9501349 B2 US 9703812 B2 US 9842222 B2 US 9940195 B2 WO 2012-170255 A1	16/04/2014 13/11/2018 09/04/2019 27/08/2019 11/02/2020 26/05/2011 06/12/2012 06/12/2012 06/12/2012 06/12/2012 05/09/2013 12/09/2013 12/09/2013 12/06/2014 06/11/2014 06/11/2014 13/11/2014 18/01/2018 29/03/2018 12/09/2019 18/02/2014 15/07/2014 23/12/2014 24/02/2015 18/08/2015 06/10/2015 23/02/2016 11/10/2016 22/11/2016 11/07/2017 12/12/2017 10/04/2018 13/12/2012
US 2016-0119119 A1	28/04/2016	JP 2016-035554 A US 9749128 B2	17/03/2016 29/08/2017