

CIPHERTEXT COMPARISON METHOD USING HOMOMORPHIC ENCRYPTION AND APPARATUS FOR PERFORMING THE SAME

CROSS-REFERENCE TO RELATED APPLICATION

5 This application claims priority to and the benefit of Korean Patent Application No. 10-2018-0128929, filed on October 26, 2018, the disclosure of which is incorporated herein by reference in its entirety.

BACKGROUND

10 1. Field

Embodiments of the present disclosure relate to a homomorphic encryption technique.

2. Discussion of Related Art

15 The concept of homomorphic encryption capable of mathematical computation between encrypted data values has emerged and thus it is expected that many changes will be made in cryptographic paradigms. However, homomorphic encryption still has technical limitations and cannot be applied to various fields.

 The fundamental problem with a conventional homomorphic encryption
20 technique is that it is difficult to compare the sizes of two encrypted data values. In detail, the conventional homomorphic encryption technique has integer data and thus, in order to compare sizes of ciphertexts, uses a scheme of comparing ciphertexts bit by bit and analyzing a result of comparing all of the bits. However, when the plaintext data is in a real number form, there is a problem in that such a comparison
25 scheme is inefficient.

SUMMARY

Embodiments of the present disclosure are directed to providing a ciphertext comparison method using homomorphic encryption and an apparatus for performing
5 the same.

According to an aspect of the present disclosure, a ciphertext comparison method using homomorphic encryption is performed in a computing apparatus including one or more processors and a memory for storing one or more programs executable by the one or more processors and includes acquiring a first ciphertext
10 obtained by encrypting first real-number data using a homomorphic encryption algorithm and a second ciphertext obtained by encrypting second real-number data using the homomorphic encryption algorithm, and generating a ciphertext for a result for comparison in size between the first real-number data and the second real-number data using homomorphic evaluation of the first ciphertext, the second ciphertext, and
15 an approximation function for approximating a signum function.

The approximation function may be a function of approximating the signum function to a polynomial composed of addition and multiplication.

The generating of the ciphertext may include performing homomorphic evaluation of subtraction between the first real-number data and the second real-
20 number data using the first ciphertext and the second ciphertext in an encrypted state and performing homomorphic evaluation of the approximation function using a result for the homomorphic evaluation of the subtraction to generate the ciphertext for the result of the size comparison.

The homomorphic encryption algorithm may be an approximate homomorphic encryption algorithm that supports homomorphic evaluation of addition, subtraction, and multiplication.

According to another aspect of the present disclosure, a ciphertext
5 comparison apparatus using homomorphic encryption includes one or more processors, a memory, and one or more programs, wherein the one or more programs are stored in the memory and executed by the one or more processors, and the programs include instructions for acquiring a first ciphertext obtained by encrypting first real-number data using a homomorphic encryption algorithm and a second
10 ciphertext obtained by encrypting second real-number data using the homomorphic encryption algorithm, and generating a ciphertext for a result for comparison in size between the first real-number data and the second real-number data using homomorphic evaluation of the first ciphertext, the second ciphertext, and an approximation function for approximating a signum function.

15 The approximation function may be a function approximating the signum function to a polynomial composed of addition and multiplication.

The generating of the ciphertext may include performing homomorphic evaluation of subtraction between the first real-number data and the second real-number data using the first ciphertext and the second ciphertext in an encrypted state
20 and performing homomorphic evaluation of the approximation function using a result for the homomorphic evaluation of the subtraction to generate the ciphertext for the result of the size comparison.

The homomorphic encryption algorithm may be an approximate homomorphic encryption algorithm that supports homomorphic evaluation of
25 addition, subtraction, and multiplication.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other objects, features and advantages of the present disclosure will become more apparent to those of ordinary skill in the art by
5 describing exemplary embodiments thereof in detail with reference to the accompanying drawings, in which:

FIG. 1 is a block diagram illustrating a computing environment including a computing apparatus suitable for use in example embodiments; and

FIG. 2 is a flowchart showing a ciphertext comparison method using
10 homomorphic encryption according to an embodiment of the present disclosure.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

Hereinafter, embodiments of the present disclosure will be described in detail with reference to the accompanying drawings. The following detailed
15 description is provided to assist the reader in gaining a comprehensive understanding of the methods, apparatuses, and/or systems described herein. However, the description is only an example, and the present disclosure is not limited thereto.

In describing embodiments of the present disclosure, when it is determined that a detailed description of a known technique associated with the present
20 disclosure would unnecessarily obscure the subject matter of the present disclosure, the detailed description will be omitted. Also, terms used herein are defined in consideration of the functions of the present disclosure and may be changed depending on a user, the intent of an operator, or a custom. Accordingly, the terms must be defined based on the following overall description of this specification.
25 The terminology used herein is only for the purpose of describing embodiments of

the present disclosure and is not restrictive. The singular forms “a,” “an,” and “the” are intended to include the plural forms as well, unless the context clearly indicates otherwise. It should be understood that the terms “comprises,” “comprising,” “includes,” and/or “including” specify the presence of stated features, integers, steps, operations, elements, components, and/or groups thereof when used herein, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

FIG. 1 is a block diagram illustrating a computing environment including a computing apparatus suitable for use in example embodiments. In the illustrated embodiment, each component may have a function and capability that differs from those described below, and an additional component may be included in addition to those in the following description.

As shown, a computing environment 10 includes a computing apparatus 12. According to an embodiment, the computing apparatus 12 may be an apparatus for performing a ciphertext comparison method to be described below.

The computing apparatus 12 includes at least one processor 14, a computer-readable storage medium 16, and a communication bus 18. The processor 14 may enable the computing apparatus 12 to operate according to the aforementioned example embodiment. 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 which may be configured to enable the computing apparatus 12 to perform operations according to an example embodiment when they are executed by the processor 14.

The computer-readable storage medium 16 is configured to store computer-executable instructions, program codes, program data, and/or other suitable forms of

information. The program 20 stored in the computer-readable storage medium 16 includes a set of instructions executable by the processor 14. In an embodiment, the computer-readable storage medium 16 may be a memory (a volatile memory such as a 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 forms of storage media accessible by the computing apparatus 12 and configured to store desired information, or a suitable combination thereof.

The communication bus 18 connects the processor 14, the computer-readable storage medium 16, and other various components of the computing apparatus 12 to one another.

The computing apparatus 12 may also include one or more input/output interfaces 22 that provide an interface for one or more input/output devices 24 and one or more network communication interfaces 26. The input/output interfaces 22 and the network communication interfaces 26 are connected to the communication bus 18. The input/output devices 24 may be connected to other components of the computing apparatus 12 through the input/output interfaces 22. For example, the input/output devices 24 may include input devices such as a pointing device (a mouse or a track pad), a keyboard, a touch input device (a touch pad or a touch screen), a voice or sound input device, and various kinds of sensor devices and/or photographing devices and output devices such as a display device, a printer, a speaker, and/or a network card. For example, the input/output devices 24 may be included in the computing apparatus 12 as components that form the computing apparatus 12 and may be connected to the computing apparatus 12 as separate devices distinct from the computing apparatus 12.

FIG. 2 is a flowchart showing a ciphertext comparison method using homomorphic encryption according to an embodiment of the present disclosure.

The steps shown in FIG. 2 may be performed by the computing apparatus 12.

Referring to FIG. 2, first, the computing apparatus 12 acquires a first
5 ciphertext obtained by encrypting first real-number data and a second ciphertext
obtained by encrypting second real-number data (210). In this case, the first
ciphertext and the second ciphertext are generated through encryption using a
homomorphic encryption algorithm.

Meanwhile, the first ciphertext and the second ciphertext may be generated
10 by the same device or different devices. Also, the computing apparatus 12 may
receive ciphertexts directly from devices that have generated the ciphertexts or may
acquire ciphertexts from a separate data base where the ciphertexts have been stored.

Meanwhile, the homomorphic encryption algorithm refers to an encryption
algorithm capable of computing a ciphertext in an encrypted state to generate a
15 ciphertext for a result of computing plaintext data. In detail, the homomorphic
encryption algorithm is an encryption algorithm capable of performing homomorphic
evaluation $\text{Eval}(f, \text{Enc}(a))$ on a function f using a ciphertext $\text{Enc}(a)$ in an encrypted
state as shown in the following Equation 1 and thus generating a ciphertext $\text{Enc}(f(a))$
for a result $f(a)$ of performing evaluation of the function f using a plaintext a .

20 [Equation 1]

$$\text{Eval}(f, \text{Enc}(a)) \rightarrow \text{Enc}(f(a)).$$

Meanwhile, according to an embodiment of the present disclosure, the
homomorphic encryption algorithm may be, for example, a homomorphic encryption
algorithm that supports homomorphic evaluation of addition, subtraction, and

multiplication, such as an approximate homomorphic encryption algorithm disclosed in “J. H. Cheon, A. Kim, M. Kim, and Y. Song. Homomorphic encryption for arithmetic of approximate numbers. In Advances in Cryptology-ASIACRYPT 2017: 23rd International Conference on the Theory and Application of Cryptology and Information Security, pages 409-437.”, “J. H. Cheon, K. Han, A. Kim, M. Kim, and Y. Song. Bootstrapping for approximate homomorphic encryption. Cryptology ePrint Archive, Report 2018/153, 2018,” or the like.

In detail, the above-described approximate homomorphic encryption algorithm is composed of the following four algorithms, and the first ciphertext and the second ciphertext may be ciphertexts generated using the following algorithm $\text{Enc}(\text{pk}, m)$.

(1) $\text{KeyGen}(1^\lambda) \rightarrow (\text{pk}, \text{sk}, \text{evk})$: a public key pk , a secret key sk , and an evaluation key evk are generated to have a stability parameter λ .

(2) $\text{Enc}(\text{pk}, m) \rightarrow c$: a ciphertext c for plaintext data m is generated using pk .

(3) $\text{Eval}(\text{evk}, f, c) \rightarrow c^*$: a ciphertext c^* for an approximate value $f(m)+e$ of $f(m)$ is generated from a ciphertext c^* using an evaluation key evk (here, e is a very small calculation error).

(4) $\text{Dec}(\text{sk}, c^*) \rightarrow m$: a ciphertext c^* is decrypted using the secret key sk , and $f(m)+e$ is output.

Meanwhile, an available homomorphic encryption algorithm according to an embodiment of the present disclosure is not limited to the above-described approximate homomorphic encryption algorithm, and any type of homomorphic

encryption algorithm can be used as long as it is a homomorphic encryption algorithm that supports homomorphic evaluation of addition, subtraction, and multiplication.

When the first ciphertext and the second ciphertext are acquired, the
5 computing apparatus 12 generates a ciphertext for a result of comparison in size between the first real-number data and the second real-number data using homomorphic evaluation of the first ciphertext, the second ciphertext, and an approximation function for approximating a signum function (220).

In detail, the computing apparatus 12 may perform homomorphic evaluation
10 of subtraction between the first real-number data and the second real-number data using the first ciphertext and the second ciphertext in an encrypted state. Also, the computing apparatus 12 may perform homomorphic evaluation of an approximation function using the homomorphic evaluation result for the difference between the first real-number data and the second real-number data to generate the ciphertext for the
15 result of comparison in size between the first real-number data and the second real-number data.

Meanwhile, the signum function may be defined as Equation 2 below:

[Equation 2]

$$sgn(x) = \begin{cases} 1 & \text{if } x > 0 \\ 0 & \text{if } x = 0 \\ -1 & \text{if } x < 0 \end{cases}$$

20 Also, according to an embodiment of the present disclosure, the approximation function for the signum function defined as Equation 2 may be a function for approximating the signum function to a polynomial form represented by addition and multiplication with respect to x.

For example, an approximation function $\text{sgn}_{\text{approx}}(x)$ obtained by approximating a signum function $\text{sgn}(x)$ to a polynomial is shown in Equation 3 below:

[Equation 3]

$$5 \quad \text{sgn}(x) \approx \text{sgn}_{\text{approx}}(x)$$

The computing apparatus 12 according to an embodiment of the present disclosure may generate the ciphertext for the result of the comparison in size between the first real-number data and the second real-number data using the homomorphic evaluation algorithm of the above-described approximate homomorphic encryption algorithm (i.e., $\text{Eval}(\text{evk}, f, c)$) as shown in Equation 4 below:

[Equation 4]

$$\text{Eval}(\text{evk}, \text{sgn}_{\text{approx}}(x-y), \text{Enc}(\text{pk}, a), \text{Enc}(\text{pk}, b)) \rightarrow \text{Enc}(\text{pk}, \text{sgn}_{\text{approx}}(a-b))$$

where a is the first real-number data, b is the second real-number data, $\text{Enc}(\text{pk}, a)$ is the first ciphertext, $\text{Enc}(\text{pk}, b)$ is the second ciphertext, and $\text{Enc}(\text{pk}, \text{sgn}_{\text{approx}}(a-b))$ is a ciphertext for a result value obtained by applying $a-b$ to $\text{sgn}_{\text{approx}}(x)$.

Also, $\text{Enc}(\text{pk}, \text{sgn}_{\text{approx}}(a-b))$ may satisfy Equation 5 below:

[Equation 5]

$$20 \quad \text{Enc}(\text{pk}, \text{sgn}_{\text{approx}}(a-b)) = \begin{cases} \text{Enc}(\text{pk}, 1+e) & \text{if } x > 0 \\ \text{Enc}(\text{pk}, 0+e) & \text{if } x = 0 \\ \text{Enc}(\text{pk}, -1+e) & \text{if } x < 0 \end{cases}$$

where e is a very small error value.

Meanwhile, in the above-described example, the homomorphic evaluation of the approximation function is illustrated as being performed using the homomorphic

evaluation algorithm of the approximate homomorphic encryption algorithm. In addition to the above example, however, the homomorphic evaluation of the approximation function may be performed using various types of homomorphic evaluation algorithms of the homomorphic encryption algorithm that can support
5 homomorphic evaluation of addition, subtraction, and multiplication.

In FIG. 2, the ciphertext comparison method has been described as having a plurality of steps. However, at least some of the steps may be performed in a changed order, performed in combination with another step, omitted, divided into sub-steps and then performed, or performed in addition to one or more steps that are
10 not shown.

According to the embodiments of the present disclosure, a ciphertext for a result of comparison in size of plaintext data values through homomorphic evaluation of an approximation function for approximating a signum function may be generated, and thus efficient size comparison is possible.

15 Although the disclosure has been described with reference to exemplary embodiments, it will be understood by those skilled in the art that various changes may be made without departing from the spirit or scope of the disclosure. Accordingly, the scope of the present disclosure is not construed as being limited to the described embodiments but is defined by the appended claims as well as
20 equivalents thereto.

WHAT IS CLAIMED IS:

1. A ciphertext comparison method using homomorphic encryption, the method being performed in a computing apparatus including one or more processors
5 and a memory for storing one or more programs executable by the one or more processors; the ciphertext comparison method comprising:

acquiring a first ciphertext obtained by encrypting first real-number data using a homomorphic encryption algorithm and a second ciphertext obtained by encrypting second real-number data using the homomorphic encryption algorithm;
10 and

generating a ciphertext for a result for comparison in size between the first real-number data and the second real-number data using homomorphic evaluation of the first ciphertext, the second ciphertext, and an approximation function for approximating a signum function.

15

2. The ciphertext comparison method of claim 1, wherein the approximation function is a function of approximating the signum function to a polynomial composed of addition and multiplication.

20 3. The ciphertext comparison method of claim 1, wherein the generating of the ciphertext comprises:

performing homomorphic evaluation of subtraction between the first real-number data and the second real-number data using the first ciphertext and the second ciphertext in an encrypted state; and

performing homomorphic evaluation of the approximation function using a result for the homomorphic evaluation of the subtraction to generate the ciphertext for the result of the size comparison.

5 4. The ciphertext comparison method of claim 1, wherein the homomorphic encryption algorithm is an approximate homomorphic encryption algorithm that supports homomorphic evaluation of addition, subtraction, and multiplication.

10 5. A ciphertext comparison apparatus using homomorphic encryption, the apparatus comprising:

one or more processors;

a memory; and

one or more programs,

15 wherein,

the one or more programs are stored in the memory and executed by the one or more processors, and

the programs comprise instructions for:

acquiring a first ciphertext obtained by encrypting first real-number data

20 using a homomorphic encryption algorithm and a second ciphertext obtained by encrypting second real-number data using the homomorphic encryption algorithm; and

generating a ciphertext for a result for comparison in size between the first real-number data and the second real-number data using homomorphic

evaluation of the first ciphertext, the second ciphertext, and an approximation function for approximating a signum function.

6. The ciphertext comparison apparatus of claim 5, wherein the
5 approximation function is a function of approximating the signum function to a polynomial composed of addition and multiplication.

7. The ciphertext comparison apparatus of claim 5, wherein the generating
of the ciphertext comprises:
10 performing homomorphic evaluation of subtraction between the first real-number data and the second real-number data using the first ciphertext and the second ciphertext in an encrypted state; and
performing homomorphic evaluation of the approximation function using a
result for the homomorphic evaluation of the subtraction to generate the ciphertext
15 for the result of the size comparison.

8. The ciphertext comparison apparatus of claim 5, wherein the
homomorphic encryption algorithm is an approximate homomorphic encryption
algorithm that supports homomorphic evaluation of addition, subtraction, and
20 multiplication.