



(51) International Patent Classification:

H04L 9/00 (2006.01)

G06F 16/903 (2019.01)

G06F 21/62 (2013.01)

G06F 21/60 (2013.01)

(21) International Application Number:

PCT/EP2021/053240

(22) International Filing Date:

10 February 2021 (10.02.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

20305175.0

25 February 2020 (25.02.2020)

EP

(71) Applicant: THALES DIS FRANCE SA [FR/FR]; 6, rue

de la Verrerie, 92190 Meudon (FR).

(72) Inventor: GOUGET, Aline; C/O THALES DIS FRANCE

SA - Intellectual Property Department 6 rue de la Verrerie,
92190 Meudon (FR).

(74) Agent: BRICKS, Amélie; AXAlto SA, 6, rue de la Ver-

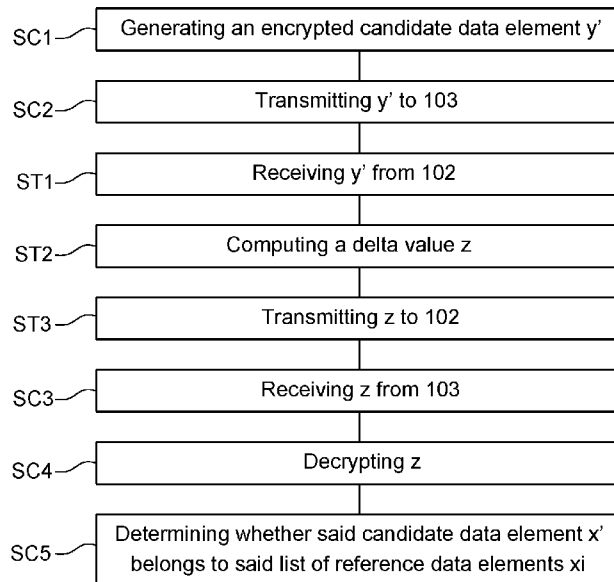
rierie, 92190 Meudon (FR).

(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, IT, JO, JP, KE, KG, KH, KN,
KP, KR, 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.

(54) Title: METHOD FOR TESTING IF A DATA ELEMENT BELONGS TO A LIST OF REFERENCE DATA ELEMENTS

Fig. 3



(57) Abstract: The present invention relates to a method for testing if a data element (x'), called candidate data element, belongs to a list of reference data elements (x_i), performed by a client device (102) and comprising the steps of : - generating (SC1) an encrypted candidate data element (y') by encrypting said candidate data element (x') with a leveled fully homomorphic DGHV (Dijik, Gentry, Halevi, Vaikuntanathan) encryption scheme, - transmitting (SC2) said encrypted candidate data element (y') to a server device (103) storing said reference data elements (x_i) encrypted with said leveled fully homomorphic DGHV encryption scheme, called encrypted reference data elements (y_i), - receiving (SC3), from said server device (103), a delta value depending on a product of differences between said encrypted candidate data element (y') and each of said encrypted reference data

(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))*

elements (y_i) - decrypting (SC4) said delta value with said leveled fully homomorphic DGHV encryption scheme, - based on said decrypted delta value, determining (SC5) whether said candidate data element (x') belongs to said list of reference data elements (x_i), said leveled fully homomorphic DGHV encryption scheme being such that a ciphertext y_i of a data x_i in $[0; n[$, i, n being integers, FHE (Fully homomorphic Encryption) encrypted with a FHE secret key p , is equal to $q_i \cdot p + n \cdot r_i + x_i$ where q_i and r_i are random integers, and such that the ciphertext y_i is decrypted by computing $x_i = (y_i \bmod p) \bmod n$.

METHOD FOR TESTING IF A DATA ELEMENT BELONGS TO A LIST OF REFERENCE DATA ELEMENTS

5 FIELD OF THE INVENTION

The present invention relates to the field of cryptography and data protection in a cloud environment, and of associated cryptographic devices, and more particularly to a method enabling to delegate the checking of the belonging of a confidential data
10 to a list while protecting the confidentiality of the data, the list and the result of the comparison.

BACKGROUND OF THE INVENTION

15 A lot of applications in various domain need to be able to determine at some point if a given element belongs or not to a list of elements, especially in the field of cybersecurity. Such a list may for example be a white list of authorized elements or a black list of forbidden elements. Such applications may for example check if a user has rights to enter a room, access a file or modify some data; check if a certificate belongs
20 to a revocation list; check if a website belongs to a list of authorized or banned web sites...

When such a list is long, the computational power and/or time needed to check if an element belongs to such a list may become important. Devices with low
25 computational power such as smartcards, smartphones or laptops may then benefit from delegating such a verification to a distant device with bigger resources, such as a server in the cloud.

Such a delegation may be a threat to the confidentiality of both the candidate
30 element and the list versus which it is checked, when the distant device performing the verification may be compromised and cannot be trusted.

Consequently, there is a need for a method enabling to delegate to a distant device the checking of the belonging of a confidential data to a list while protecting the confidentiality of the data, of the list and of the result of the comparison.

SUMMARY OF THE INVENTION

For this purpose and according to a first aspect, this invention therefore relates to a method for testing if a data element, called candidate data element, belongs to a list of reference data elements, performed by a client device and comprising the steps of :

- generating an encrypted candidate data element by encrypting said candidate data element with a leveled fully homomorphic DGHV (Dijik, Gentry, Halevi, Vaikuntanathan) encryption scheme,
- transmitting said encrypted candidate data element to a server device storing said reference data elements encrypted with said leveled fully homomorphic DGHV encryption scheme, called encrypted reference data elements,
- receiving, from said server device, a delta value depending on a product of differences between said encrypted candidate data element and each of said encrypted reference data elements,
- decrypting said delta value with said leveled fully homomorphic DGHV encryption scheme,
- based on said decrypted delta value, determining whether said candidate data element belongs to said list of reference data elements,

said leveled fully homomorphic DGHV encryption scheme being such that a ciphertext y_i of a data x_i in $[0; n[$, i, n being integers, FHE (Fully homomorphic Encryption) encrypted with a FHE secret key p , is equal to $q_i.p + n.r_i + x_i$ where q_i and r_i are random integers, and such that the ciphertext y_i is decrypted by computing $x_i = (y_i \bmod p) \bmod n$.

It enables the client device to delegate the checking operation without disclosing to the server device the value of the candidate data element and without enabling the server device to gain knowledge of the result of the comparison.

According to a second aspect, this invention therefore relates also to a method for testing if a data element, called candidate data element, belongs to a list of reference data elements, said method being performed by a server device storing said reference data elements encrypted with a leveled fully homomorphic DGHV (Dijik, Gentry, Halevi, Vaikuntanathan) encryption scheme, called encrypted reference data elements, and comprising the steps of:

- receiving, from a client device, an encrypted candidate data element obtained by encryption of said candidate data element with said leveled fully homomorphic DGHV encryption scheme,
- computing a delta value depending on a product of differences between said encrypted candidate data element and each of said encrypted reference data elements,
- transmitting said computed delta value to said client device,

such that, after decrypting of said delta value with said leveled fully homomorphic DGHV encryption scheme, the client device is able to determine whether said candidate data element belongs to said list of reference data elements, based on said decrypted delta value,

said leveled fully homomorphic DGHV encryption scheme being such that a ciphertext y_i of a data x_i in $[0; n[$, i, n being integers, FHE (Fully homomorphic Encryption) encrypted with a FHE secret key p , is equal to $q_i.p + n.r_i + x_i$ where q_i and r_i are random integers, and such that the ciphertext y_i is decrypted by computing $x_i = (y_i \bmod p) \bmod n$.

It enables the server device to test the belonging of the candidate data element to the list without having itself access to the values of the reference data elements against which the candidate data element is tested, nor to the result of the test.

In an embodiment, said delta value z may be equal to $(y_1 - y') * (y_2 - y') \dots (y_T - y')$ or may be equal to $(y_1 - y') * (y_2 - y') \dots (y_T - y')$ modulo y_0 where $y_0 = p * q_0 + r_0 * n$ with $|q_0| > |q_i|$, with $y_1, \dots, y_T$ said encrypted reference data elements and y' said encrypted candidate data element, with T an integer and $1 \leq i \leq T$, and

the step of determining whether said candidate data element belongs to said list of reference data elements may comprise comparing said decrypted delta value with 0 and, when said decrypted delta value is different from 0, then said candidate data

element does not belong to the list of reference data elements, and when said decrypted delta value is equal to 0, said candidate data element belongs to the list of reference data elements.

5 It enables the client device to determine easily if the candidate data element belongs to the list based on the delta value computed by the server device. It enables also to set the parameters of the DVHG scheme such that the scheme only copes with one multiplication while still preserving the capacity of the client device to determine if the candidate data element belongs to the list based on the transmitted delta value.

10 Said reference data elements may be plaintext data or hashes of plaintext data.

Said reference data element are IBANs (International Bank Account Number) or hashes of IBANs.

15 According to a third aspect, this invention therefore relates also to a computer program product directly loadable into the memory of at least one computer, comprising software code instructions for performing the steps of the methods according to the first or second aspect when said product is run on the computer.

20 According to a fourth aspect, this invention therefore relates also to a client device comprising a processor and an interface configured to perform the steps of the method according to the first aspect.

25 According to a fifth aspect, this invention therefore relates also to a server device comprising a memory storing reference data elements encrypted with a leveled fully homomorphic DGHV (Dijik, Gentry, Halevi, Vaikuntanathan) encryption scheme, a processor and an interface configured to perform the steps of the method according to the second aspect.

30 According to a sixth aspect, the invention relates also to a system comprising a client device according to the fourth aspect and a server device according to the fifth aspect.

To the accomplishment of the foregoing and related ends, one or more embodiments comprise the features hereinafter fully described and particularly pointed out in the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The following description and the annexed drawings set forth in detail certain illustrative aspects and are indicative of but a few of the various ways in which the principles of the embodiments may be employed. Other advantages and novel features will become apparent from the following detailed description when considered in conjunction with the drawings and the disclosed embodiments are intended to include all such aspects and their equivalents.

- Figure 1 is a schematic illustration of a system comprising a client device and one or more remote servers according to an embodiment of the present invention;
- Figure 2 is a schematic illustration of a client device according to an embodiment of the present invention;
- Figure 3 illustrates schematically a method for testing if a candidate data element belongs to a list of reference data elements, according to an embodiment of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

The invention aims at solving the issue of enabling a client device to delegate to a distant server device the testing of the belonging of a confidential data element, called candidate data element, to a list of reference data elements while protecting the confidentiality of the candidate data element, of the list and of the result of the comparison, at a cost low enough to make practical implementation possible on currently existing common computation devices.

The candidate data element and the reference data elements may be plaintext data. For example, they may be IBAN (International Bank Account Number) numbers and the method according to the invention may be used to determine if a bank account belongs to a white list or black list of bank accounts to/from which money transfers are

authorized/forbidden. Alternatively, they may be user identifiers and the method according to the invention may be used to determine if a user is authorized to access a facility or digital resource. Alternatively, they may be digital certificate identifiers and the method according to the invention may be used to determine if a candidate
5 certificate is still valid or if it has been revoked by a certificate authority. Alternatively, they may be passwords and the method according to the invention may be used to determine if a password is already used or has been used recently.

Instead of being plaintext data, the candidate data element and the reference
10 data elements may be hashes of such plaintext data.

In order to protect the confidentiality of any element provided to the server device, either the candidate data element or reference data elements, a first core idea of the invention is to encrypt it with a levelled fully homomorphic encryption scheme.
15 Such a scheme, thanks to its homomorphic properties, enables to perform an operation on encrypted data without prior decryption of these and to get as a result an encrypted value of the output of this operation as if it had been applied to decrypted data. Consequently, the server in charge of performing the computations needed to determine if the candidate data element belongs to the list, may perform the required
20 operations directly on encrypted data, without ever decrypting it and therefore without having access to the value of the candidate data element and of the reference data elements of the list.

In the following paragraphs, the expressions “HE” or “homomorphic” used as
25 adjectives are used to qualify data encrypted by an encryption operation of said Homomorphic Encryption scheme or to qualify operations performed on such encrypted data.

A problem of homomorphic encryption schemes is the cost of the operations to
30 be performed on homomorphically encrypted data. Fully homomorphic encryption schemes imply complex calculations which come with a heavy cost. Levelled encryption schemes may be simpler but the size of the parameters of such schemes, such as the key length, must be raised as the depth of the circuit to be assessed grows,

in order to keep the results accurate. If such a levelled scheme is used to encrypt the reference data elements of the list, when new reference data elements are added to the list, the depth of the circuit grows by one for each new data element and all the reference data elements of the list have to be re-encrypted using updated scheme parameters.

In order to keep the size of the parameters of the scheme low, the second main idea of the invention is to check the belonging of a candidate data element to a list of reference data elements by computing the product of the differences between the candidate data element and each of the reference data elements of the list. Indeed, such a product becomes null when the candidate element belongs to the list. In addition, when such a computation is performed on FHE-encrypted values, decrypting the result will always return null when the candidate element belongs to the list, whatever the size of the parameters of the scheme as long as the parameter set has been selected to support at least one homomorphic multiplication. As a result, the parameters may be chosen such that the scheme is accurate for evaluating the result of just a single multiplication. In such a case, when the candidate element does not belong to the list, the result of the computation of the homomorphic product of the differences between the candidate data element and each of the reference data elements of the list cannot be guaranteed as accurate but this not an issue since in that case the value of the product has no interest, except that it is not null. For a better comprehension, examples will be given in the following paragraphs.

In the rest of the description, the method according to the invention is described as using the leveled fully homomorphic encryption scheme known as DGHV (Dijk, Gentry, Halevi, Vaikuntanathan) scheme ((*"Fully Homomorphic Encryption over the Integer"*, Dijk and al. [DGHV]). Based on this description, the invention could be implemented using other levelled fully homomorphic encryption schemes such as BGV ((*"(Leveled) Fully Homomorphic Encryption without Bootstrapping"*, Brakerski and al.).

Figure 1 is a schematic illustration of system 100 comprising a network 101 connecting a client device 102 such as a smartcard, a mobile telephone, a tablet, or a personal computer, to a server device 103. The client device 102 is operated by a user

104 and interacts with the server device to delegate to the server device the checking of the belonging of a candidate data element to a list of reference data elements.

Figure 2 is a schematic illustration of a client device 102. The client device 102 may include a processor 201 connected via a bus 202 to a random access memory (RAM) 203, a read-only memory (ROM) 204, and/or a non-volatile memory (NVM) 205. The client device 102 may further include a communication interface 206 by which the client device 102 may be connected to the network 101. Such an interface may be a wireless interface connected to an antenna and may be used to connect the client device 102 to various forms of wireless networks, e.g., wide-area networks, WiFi networks, or mobile telephony networks. Alternatively, such an interface may be a wired interface such as an Ethernet internet. The client device may also include input/output means 207 providing interfaces to the user of the client device, such as one or more screens, loudspeakers, a mouse, tactile surfaces, a keyboard etc...

The server device 103 has the same kind of architecture and may include the same elements as the client device (301, ...).

The following paragraphs describe the steps SC of a **method** for testing if a candidate data element x' belongs to a list of reference data elements, performed by the client device 102, according to a first aspect of the invention as depicted on **figure 3**; and the steps ST of a **method** for testing if the candidate data element x' belongs to the list of reference data elements, performed by the server device 103. In the following description, the list of reference data elements is supposed to include T elements with T an integer, and the reference data elements are noted x_i with $1 \leq i \leq T$.

In a first client step SC1, the processor of the client device generates an encrypted candidate data element y' by encrypting said candidate data element x' with the leveled fully homomorphic DGHV encryption scheme.

$y' = p * q + r * n + x'$ with p the secret key of the DGHV scheme

q and r random integers according to DGHV specs

n an integer such that x_i in $[0; n[$ for $1 \leq i \leq T$.

In a second client step SC2, the client device transmits said encrypted candidate data element y' to the server device storing said reference data elements x_i encrypted with the leveled fully homomorphic DGHV encryption scheme, called encrypted reference data elements y_i .

5

$y_i = p * q_i + r_i * n + x_i$ with p the secret key of the DGHV scheme

q_i and r_i random integers according to DGHV specs

$1 \leq i \leq T$.

10

The coefficients q_i and q may be large numbers randomly chosen for each new encryption and the coefficient r_i and r may be small numbers randomly chosen for each new encryption.

15

In a first server step ST1, the server device receives, from the client device 102, the encrypted candidate data element y' obtained by encryption of said candidate data element x' with said leveled fully homomorphic DGHV encryption scheme.

20

In a second server step ST2, the server device computes a delta value z depending on the product of the differences between the encrypted candidate data element y' and each of the encrypted reference data elements y_i he has stored. For example, when the delta value z is equal to this product, it may read $z = \prod_{i=1}^T (y_i - y')$.

Alternatively, $z = \prod_{i=1}^T (y_i - y') \bmod y_0$ with $y_0 = p * q_0 + r_0 * n$ where q_0 and r_0 are random integers and q_0 is such that $|q_0| > |q_i|$, $1 \leq i \leq T$.

25

Since the candidate data element and the reference data elements are all FHE-encrypted, the delta value z depends on the random numbers q , r , q_i and r_i used when the data elements were encrypted. As a result, the server device cannot draw any information from the delta value z and cannot determine if the candidate data element belongs or not to the list of reference data elements.

30

In a third server step ST3, the server device transmits the computed delta value z to said client device 102.

In a third client step SC3, the client device receives from the server device 103 the delta value z depending on the product of the differences between the encrypted candidate data element y' and each of the encrypted reference data elements y_i .

5 In a fourth client step SC4, the client device decrypts the delta value with said leveled fully homomorphic DGHV encryption scheme. In DGHV scheme, a ciphertext y_i is decrypted by computing $x_i = (y_i \bmod p) \bmod n$.

10 When the delta value $z = \prod_{i=1}^T (y_i - y')$, such a decryption may be performed by computing $(z \bmod p) \bmod n$.

In a fifth client step SC5, the client device determines based on the decrypted delta value whether the candidate data element x' belongs to said list of reference data elements x_i .

15

In order to do so, when the delta value $z = \prod_{i=1}^T (y_i - y')$, the client device may compare the decrypted delta value with 0 and, when the decrypted delta value is different from 0, then the candidate data element x' does not belong to the list of reference data elements x_i , and when the decrypted delta value is equal to 0, said candidate data element x' belongs to the list of reference data elements x_i .

20

Indeed, when the candidate data element x' is equal to a reference data element x_j of the list, we have $y_j - y' = p \cdot (q_j - q) + (r_j - r) \cdot n$. Therefore the value $\prod_{i=1}^T (y_i - y')$ may be re-written as $A \cdot p + B \cdot n$ with $A = (q_j - q) \cdot \prod_{i \neq j, i=1}^T (y_i - y')$ and $B = (r_j - r) \cdot \prod_{i \neq j, i=1}^T (y_i - y')$. When the delta value $z = \prod_{i=1}^T (y_i - y')$, decrypting it by computing $(z \bmod p) \bmod n$ gives a null value (high probability means $(1-1/n)$).

25

Such a way of determining if the candidate data element belongs to the list of reference data elements is effective even when the length of the parameters of the DGHV scheme is only big enough to cope with a depth of one multiplication. In such a case, when $z = \prod_{i=1}^T (y_i - y')$, the decryption of z will output a wrong value: $(z \bmod p) \bmod n$ will often not be equal to $\prod_{i=1}^T (x_i - x')$. But it doesn't matter. What matters is that when the candidate data element x' is equal to a reference data element x_j of the

30

list, $z = \prod_{i \neq j, i=1}^T (y_i - y'_i) * [p * (q_j - q) + (r_j - r) * n]$ and $(z \bmod p) \bmod n = 0$. Therefore, the size of the parameters of the DGHV scheme and the computation time required to perform encryptions, decryptions and operations on FHE encrypted values is minimized.

5

In order to prevent the server device from having access to the value of the reference data elements x_i of the list, only the encrypted reference data elements y_i are provided to the server device. As an example, prior to the steps described above, the client device may select, among a set of data elements it stores, the data elements that should form the list of reference data elements. It may then FHE-encrypt said selected data elements and transfer the generated encrypted reference data elements to the server device.

10

If the client device wishes to update the list of the server device by adding into it a new data element, the client device may generate the corresponding encrypted reference data element and transmit it to the server device so that the server device includes it in its list of encrypted reference data elements against which the encrypted candidate data elements should be checked.

15

As a result, the method described above enables the client device to delegate the checking of the belonging of the candidate data element to the list of reference data elements stored under a FHE-encrypted form by the server device. The confidentiality of both the data elements and the checking result is ensured since the server device only has access to FHE-encrypted values and cannot deduce from the calculations it performs (computing the delta value) if the candidate data element being tested is indeed included in the list he owns.

20

25

CLAIMS

1. A method for testing if a data element (x'), called candidate data element, belongs to a list of reference data elements (x_i), performed by a client device (102) and comprising the steps of :

- generating (SC1) an encrypted candidate data element (y') by encrypting said candidate data element (x') with a leveled fully homomorphic DGHV (Dijik, Gentry, Halevi, Vaikuntanathan) encryption scheme,
- transmitting (SC2) said encrypted candidate data element (y') to a server device (103) storing said reference data elements (x_i) encrypted with said leveled fully homomorphic DGHV encryption scheme, called encrypted reference data elements (y_i),
- receiving (SC3), from said server device (103), a delta value depending on a product of differences between said encrypted candidate data element (y') and each of said encrypted reference data elements (y_i),
- decrypting (SC4) said delta value with said leveled fully homomorphic DGHV encryption scheme,
- based on said decrypted delta value, determining (SC5) whether said candidate data element (x') belongs to said list of reference data elements (x_i),

said leveled fully homomorphic DGHV encryption scheme being such that a ciphertext y_i of a data x_i in $[0; n[$, i, n being integers, FHE (Fully homomorphic Encryption) encrypted with a FHE secret key p , is equal to $q_i.p + n.r_i + x_i$ where q_i and r_i are random integers, and such that the ciphertext y_i is decrypted by computing $x_i = (y_i \bmod p) \bmod n$.

2. A method for testing if a data element (x'), called candidate data element, belongs to a list of reference data elements (x_i), said method being performed by a server device (103) storing said reference data elements (x_i) encrypted with a leveled fully homomorphic DGHV (Dijik, Gentry, Halevi, Vaikuntanathan) encryption scheme, called encrypted reference data elements (y_i), and comprising the steps of:

- receiving (ST1), from a client device (102), an encrypted candidate data element (y') obtained by encryption of said candidate data element (x') with said leveled fully homomorphic DGHV encryption scheme,
- computing (ST2) a delta value (z) depending on a product of differences between said encrypted candidate data element (y') and each of said encrypted reference data elements (y_i),
- transmitting (ST3) said computed delta value (z) to said client device (102),

such that, after decrypting of said delta value with said leveled fully homomorphic DGHV encryption scheme, the client device (102) is able to determine whether said candidate data element (x') belongs to said list of reference data elements (x_i), based on said decrypted delta value,

said leveled fully homomorphic DGHV encryption scheme being such that a ciphertext y_i of a data x_i in $[0; n[$, i, n being integers, FHE (Fully homomorphic Encryption) encrypted with a FHE secret key p , is equal to $q_i.p + n.r_i + x_i$ where q_i and r_i are random integers, and such that the ciphertext y_i is decrypted by computing $x_i = (y_i \bmod p) \bmod n$.

3. The method of claim 1 or 2 wherein :

- said delta value z equals to $(y_1 - y') \cdot (y_2 - y') \dots (y_T - y')$ or equals to $(y_1 - y') \cdot (y_2 - y') \dots (y_T - y')$ modulo y_0 where $y_0 = p \cdot q_0 + r_0 \cdot n$ with $|q_0| > |q_i|$, with $y_1, \dots, y_T$ said encrypted reference data elements and y' said encrypted candidate data element, with T an integer and $1 \leq i \leq T$,
- determining whether said candidate data element (x') belongs to said list of reference data elements (x_i) comprises comparing said decrypted delta value with 0 and, when said decrypted delta value is different from 0, then said candidate data element (x') does not belong to the list of reference data elements (x_i), and when said decrypted delta value is equal to 0, said candidate data element (x') belongs to the list of reference data elements (x_i).

4. The method of any one of claims 1 to 3, wherein said reference data elements (x_i) are plaintext data or hashes of plaintext data.

5. The method of any one of claims 1 to 4, wherein said reference data element (x_i) are IBANs (International Bank Account Number) or hashes of IBANs.
- 5 6. A computer program product directly loadable into the memory of at least one computer, comprising software code instructions for performing the steps of any one of claims 1 to 5, when said product is run on the computer.
7. A client device (102) comprising a processor (201) and an interface (207) configured to perform the steps of any one of claims 1 and 3 to 5.
- 10 8. A server device (103) comprising a memory (303, 304, 305) storing reference data elements (x_i) encrypted with a leveled fully homomorphic DGHV (Dijik, Gentry, Halevi, Vaikuntanathan) encryption scheme, a processor (301) and an interface (307) configured to perform the steps of any one of claims 2 to 5.
- 15 9. A system (100) comprising a client device (102) according to claim 7 and a server device (103) according to claim 8.

1/2

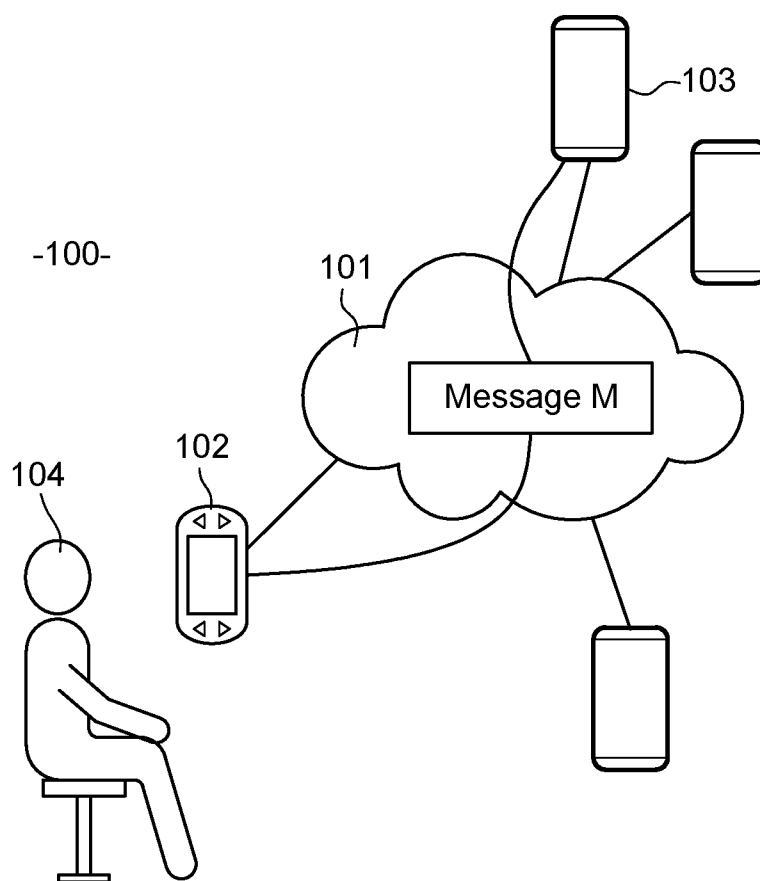
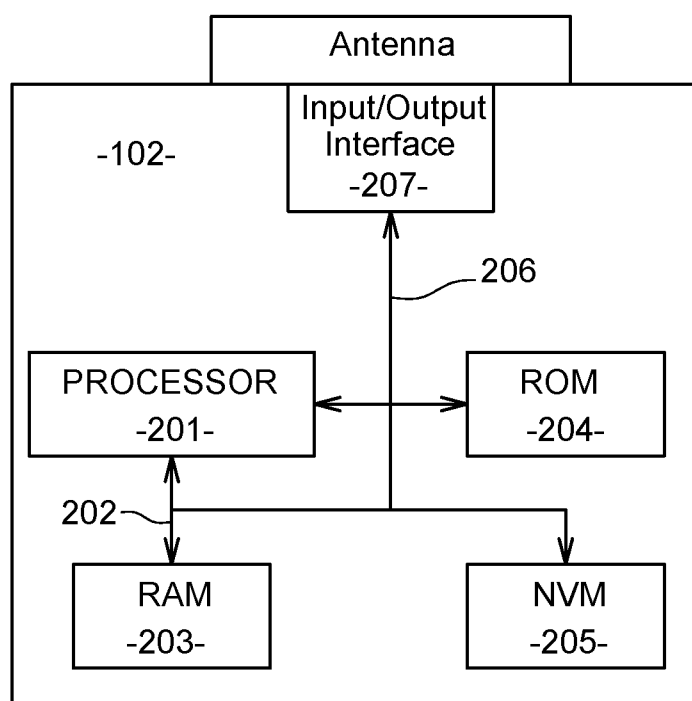
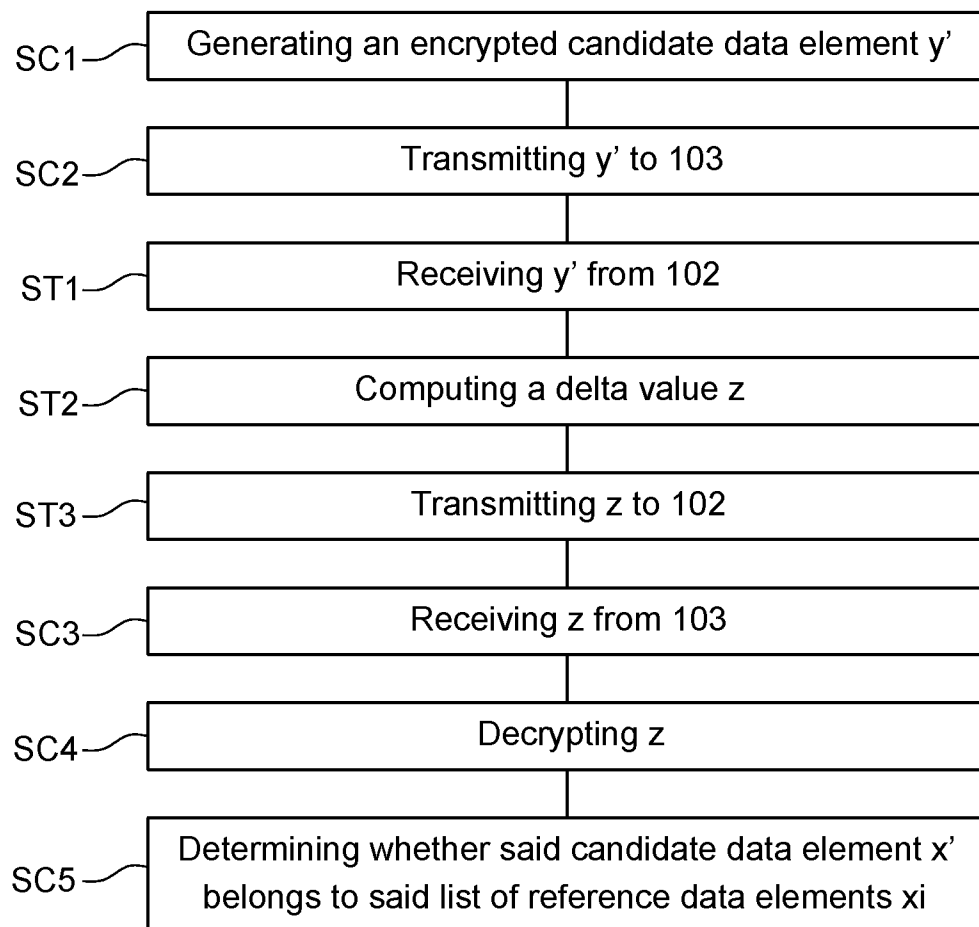
Fig. 1**Fig. 2**

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2021/053240

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L9/00 G06F21/62 G06F16/903 G06F21/60
ADD.

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 G06F

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2018/198601 A1 (LAINE KIM HENRY MARTIN [US] ET AL) 12 July 2018 (2018-07-12) paragraphs [0018], [0022], [0025], [0029], [0036]; figures 1-2 -----	1,2,4-9
Y	EP 3 334 083 A1 (GEMALTO SA [FR]) 13 June 2018 (2018-06-13) paragraph [0069] -----	1,2,4-9
A	US 2017/293913 A1 (GULAK GLENN [CA] ET AL) 12 October 2017 (2017-10-12) paragraphs [0088] - [0090] -----	1-9



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

"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

20 April 2021

Date of mailing of the international search report

29/04/2021

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Horbach, Christian

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2021/053240

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2018198601	A1	12-07-2018	NONE

EP 3334083	A1	13-06-2018	CN 110235409 A 13-09-2019
		EP 3334083 A1	13-06-2018
		EP 3552338 A1	16-10-2019
		US 2020076614 A1	05-03-2020
		WO 2018104412 A1	14-06-2018

US 2017293913	A1	12-10-2017	CA 3002582 A1 19-10-2017
		CN 109314641 A	05-02-2019
		EP 3443706 A1	20-02-2019
		JP 2019514301 A	30-05-2019
		KR 20180127506 A	28-11-2018
		PH 12018502196 A1	16-09-2019
		SG 11201809010T A	29-11-2018
		US 2017293913 A1	12-10-2017
		US 2019182216 A1	13-06-2019
		US 2019205875 A1	04-07-2019
		WO 2017177313 A1	19-10-2017
