

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) Publication number:

0 551 678 A1

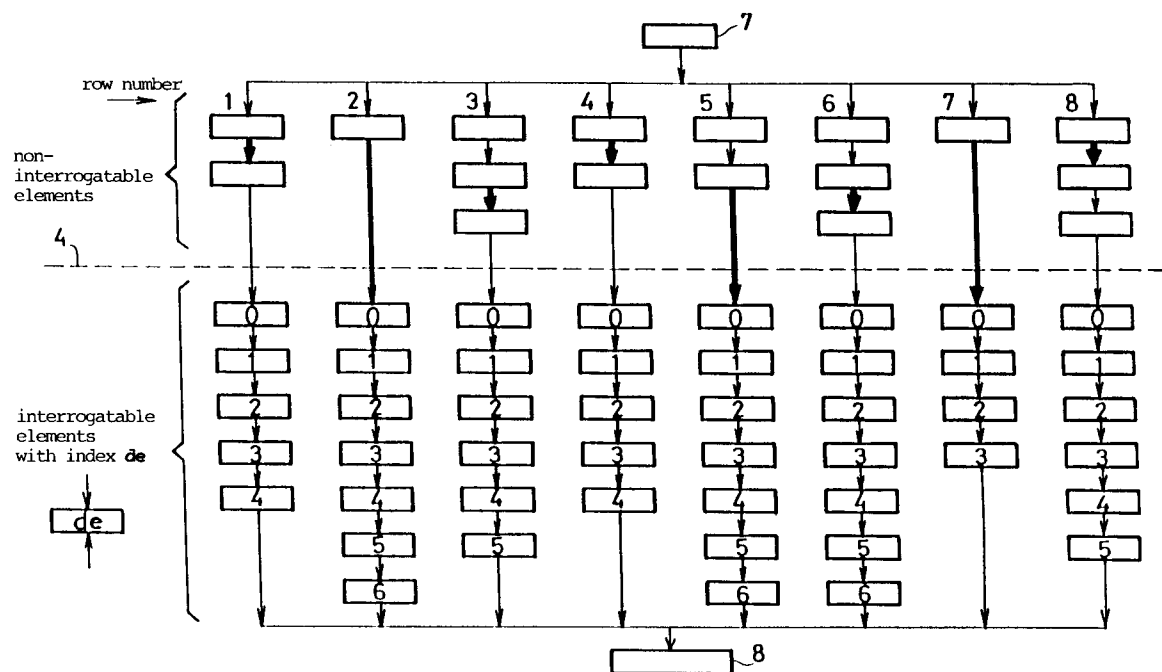
(12)

EUROPEAN PATENT APPLICATION(21) Application number: **92204021.7**(51) Int. Cl.⁵: **G06F 12/14, G06F 1/00,
H04L 9/32, G07F 7/10**(22) Date of filing: **18.12.92**(30) Priority: **20.12.91 NL 9102146**(43) Date of publication of application:
21.07.93 Bulletin 93/29(84) Designated Contracting States:
AT BE DE DK ES FR GB IT NL SE(71) Applicant: **STAAT DER NEDERLANDEN te
dezen vertegenwoordigd door de
Directeur-Generaal van de Rijkswaterstaat
4 Koningskade
NL-2596 AA The Hague(NL)**(72) Inventor: **Stoelhorst, Henk Jakob
26, Hermelijnstraat
NL-2623 EB Delft(NL)
Inventor: Chaum, David
411, Kruislaan
NL-1098 SJ Amsterdam(NL)
Inventor: Gerritse, Jacobus Johannes
69, Pleineslaan
NL-3734 EM Den Dolder(NL)
Inventor: van Wijk, Dirk Peter
26, Westeindseweg
2381 EC Zoeterwoude(NL)**(74) Representative: **van der Arend, Adrianus G.A.,
Ir. et al
EXTERPATENT B.V. P.O. Box 3241
NL-2280 GE Rijswijk (NL)**(54) **Method and system for changing, from a component of a system and subject to checking, the contents of a register or another component.**

(57) Method and system for processing a change value within a system having a number of components operating as participants, a first component having an arithmetic section, which from outside is at least partially unreachable and which has a register which is unreachable directly from outside, and a second component supplying a message, which comprises a change value, to the first component for the purpose of changing the contents of the register. The first component contains a set of elements, which represent numbers which are divided into rows, each second and subsequent element of each row being determined, by application of one or more one-way functions, from the directly preceding element of the row. The second component receives a

first datum which is a function of numbers underlying the set or of the last elements thereof. In response to receiving the message originating from the second component, the first component has to send elements from a number of rows to the second component. The second component evaluates the last-mentioned received elements on the basis of the indices sent and by application of the one-way functions to the last elements of the rows in question, and therefrom obtains a second datum. If the first and second data, which may first have been elaborated further, are identical, the second component judges the register contents to have been changed correctly.

EP 0 551 678 A1

FIG. 2.

The invention relates to a method for processing a change value within a system having a number of components operating as participants, a first component having an arithmetic section, which from outside is at least partially unreachable and which has a register which is unreachable directly from outside, and a second component supplying a message, which comprises a change value, to the first component for the purpose of changing the contents of the register.

The first component is, for example, a card with a microcomputer, also called "smart card". There may be a third component in a communication path between the first component and the second component, and which could be arranged by the user of the first component for the purpose of changing, and passing on in the changed state, with fraudulent intent, the change value received from the first component. Changing the contents of the register is known per se in practice. With the exception of the solutions offered by the invention, the applicant does not know of any method in which the correctness of the changing of the register contents can be checked by the second component. The ability to check the changing of the register contents is important, in particular, if the register contents represent a monetary value, which is to be decreased by the second component in the case of payment for goods or services, or which is to be increased by the second component after payment of "real" money. Countering the fraudulent increase of the register contents is important, for example, if the contents represent a number of goods or services which the user of the first component is owed by the user of the second component.

The object of the invention is therefore to check the correctness of the changing of the register contents.

This objective is achieved according to the invention by means of the method as described in claim 1. As a result, every alteration of the change value by the third component will result in the first component sending back, to the second component, elements of the first group of rows whose indices are higher than the second component was expecting on the basis of the change value sent. The third component, namely, is not able to calculate elements with lower indices of the rows in question on the basis of the elements received from the first component, because the elements of a row can only be calculated starting from an element having a lower index.

In order to prevent the third component, after sufficiently frequent use, from learning all the elements of the first group of rows, it is preferred that, after each message received by the first component, the at least one origin number is changed, as

a result of which the elements determined therefrom are also changed.

Other properties and advantages of the invention will become apparent from the following explanation by reference to the drawings, in which:

Figure 1 shows a diagram of a system which is suitable for application of the invention;

Figure 2 shows a diagram of a set of elements which represent numbers, for use in the method according to the invention; and

Figure 3 shows a representation of a one-way function for determining the elements of the set of Figure 2.

Figure 1 shows a system which is suitable for application of the invention and which comprises a first component 1, a second component 2 and a third component 3. The first and second components 1, 2 are generally computers. The first component is formed, for example, by a card with a microcomputer, also called "smart card", in which case the third component 3 can be used for communication between the first and second components 1, 2. The first component has an at least partially unreachable arithmetic section with a register which is unreachable from outside. Unreachable means that the operation of the arithmetic section, at least in part, cannot be changed, and the contents of the register can only be changed via the arithmetic section and not from outside the first component 1 bypassing the arithmetic section.

The register of the first component 1 is intended to store a value which can be changed from outside via the arithmetic section of the first component 1 with a change value. The register contents, for example, represent a monetary value or a number of goods or services which the owner of the first component 1 is owed by another participant in the system. The third component 3, which may be owned by the user of the first component 1, can be changed with fraudulent intent in such a way that it is capable of changing the change value which it receives from the second component 2, prior to passing on the changed value to the first component 1. The invention intends to check this. To this end, the second component 2, after sending a message which contains a change value, expects a response from the third component 3, which response must be defined by the first component 1 in such a way that it is impossible for the third component 3 to alter the change value without also altering the response sent to the second component 2. As a result of the second component 2 comparing an expected response or a result derived therefrom with the actually received response or a result derived therefrom, the second component 2 is then able to check the correctness of the changing of the register contents.

In order to achieve said objective, the first component 1 contains a set of elements which represent numbers and which are divided into a number of rows.

Figure 2 shows a set of this kind having eight rows $r = 1$ to $r = 8$ inclusive. Each element of each row is represented by a small rectangle. Each row comprises a number of elements which are non-interrogatable from outside the first component 1 and which are shown above the dashed line 4. Each row also comprises a number of interrogatable elements which, in contrast, are interrogatable from outside the first component 1. Within the rectangles representing the interrogatable elements, the indices **de** of the elements are shown. Each second element of each row, in Figure 2 each second element in the row counted downwards, is calculated from the preceding element by applying a one-way function. Preferably, the set of elements should be used only a small number of times for interrogating elements. Subsequently, the first component has to use another set.

One-way functions are known per se, and Figure 3 gives an example. In Figure 3, a variable x forms an input variable for a DES algorithm or a DES-based algorithm, which is represented by a box 5 and which uses a key k which is allowed to be known. The result of the algorithm of box 5 is supplied to an exclusive OR function which is indicated by box 6 and which is sometimes called XOR function. The exclusive OR function also receives the variable x and as a result supplies the output variable y . If for a DES-based algorithm the variables x and y and the key k are sufficiently large, it is virtually impossible to obtain the input variable x from the output variable y by inverse calculation. The greater the variables x , y and/or the key k , the more difficult it is to calculate backwards from y to x , and the stronger the one-way function is called.

The one-way functions used for determining the elements of the set shown in Figure 2 can be different. For a simple implementation of the system, however, they are identical.

In Figure 2, in each row at least one one-way function is used which is stronger than the other one-way function(s) of the row and which is indicated as a thicker transition line than the other transition lines between the elements. As a result it becomes even more difficult to obtain a non-interrogatable element by inverse calculation from the interrogatable elements. This is important if the first elements of the rows are defined from an origin element 7 which represents a number and which is fixed or which is changed in a predetermined manner which can be generally known, for example after processing of each received message. If a swindler should once have obtained the knowledge

of element 7 or the first elements of the rows by inverse calculation, he would always be able to calculate all the elements of each set. Therefore, after processing of a number of messages the origin element 7 is preferably also changed with the aid of a generated random number. Application of the invention does not, however, require that the set contains non-interrogatable elements.

The number of interrogatable elements of each row can be arbitrarily large, and can be different for different rows. For the purpose of a simple implementation, each row could contain the same number of interrogatable elements.

The check intended according to the invention can take place in various ways with the aid of the set shown in Figure 2. Because the description and the understanding of the invention would not thereby be simplified, it was decided to do without an explanation by reference to flow diagrams for the operation of each component 1, 2 and 3 for each of the different ways.

Prior to the second component 2 carrying out a comparison, as mentioned hereinafter, for the purpose of checking the correct processing of the change value, the second component 2 receives from another component of the system a first datum which is a function of one or more origin numbers, for example the origin element 7, which underlie the set of elements, or which is a function of the last elements of the set, which in Figure 2 are jointly represented by the rectangle 8. Said other component may be a component, which is considered to be very reliable and which assigns different, unique origin elements 7 to one or more first components 1, and which, prior to the first components 1 being able to use the received origin elements 7, supplies a list of the assigned origin elements 7 to the second component 2. Instead of the list of origin elements 7, said very reliable component can supply a list containing end elements 8, which correspond to the origin elements 7, to the second component 2. Each element of such a list forms an abovementioned first datum. Alternatively, the first datum can be obtained from an enciphered or authenticated version of the last element 8 of the set, which version is supplied by the first component 1 to the second component 2, which then deciphers said version to give the element 8 and checks it for genuineness, and if found genuine, uses it as the first datum, prior to the second component 2, as explained hereinafter, asking the first component 1 for interrogatable elements from the set. Which enciphering algorithm is used is of no importance to the invention. An example for enciphering of the element 8 and for checking the genuineness of the enciphered version thereof has been described in the Dutch patent application NL-A-9102145 which was filed by

applicant together with the present application.

In each of the embodiments according to the invention mentioned hereinafter the second component 2 expects specific numbers from the first component 1, which are represented by interrogatable elements having indices which (also) have been calculated by the second component 2 on the basis of the change value. Starting from the received numbers, and by application of the one-way functions in question, the second component 2 calculates the elements which should be the last elements of the rows in question. Said calculated last elements together can be regarded as the second datum.

When the second component 2 has received a list of unique origin elements 7, the second component 2 first calculates therefrom a corresponding list of end elements 8 as first data. After the second component 2 has calculated a second datum, the second component 2 checks whether this second datum occurs in the list of first data. Only if this is the case is the processing of the change value adjudged to be correct and the first datum in question is deleted from the list.

In the case that the second component 2 has received none of said lists, but has received, prior to interrogating elements from the set, the enciphered end element 8 from the first component 1, the second component 2 calculates therefrom the first datum and compares it with the calculated second datum. Only if these two data are identical is the processing of the change value adjudged to be correct.

It is to be noted that hereinbefore and hereinafter the first and second data are also meant to refer to results derived therefrom which are suitable for carrying out said comparison in the second component 2.

According to a first embodiment, a group of rows, for example the rows 1, 2 and 3, is assigned to the change value. If the first component 1 receives a change value from the third component 3, and the change value is meant to decrease the contents of the register, the first component 1 determines the (radix - 1) complement, which is equal to the radix complement minus 1, separately for each digit of the change value, or of groups of digits of the change value. The chosen radices are a function of the radices of rows of the set, which are assigned to the separate or batches of digits of the change value. The complements established are assumed to be the indices of interrogatable elements of the assigned rows in question. Assume for example that the first component receives as a change value the number 352, in the notation according to the radices of the rows in question of the set. If the (radix - 1) complement is determined for each digit of this number, this results, for the

set shown in Figure 2 whose rows are different in length and each contain fewer than 10 elements, in the number $(4 - 3) (6 - 5) (5 - 2) = 113$. The first component 1 then sends the element with index 1 of the first row, the element with index 1 of the second row and the element with index 3 of the third row to the second component 2 via the third component. If on the other hand only a single row with, for example, 1000 (in decimal notation) elements had been assigned to the change value, the (radix - 1) complement would be $(999 - 352) = 647$ (in decimal notation), and the first component 1 would send the element with index 647 of that row to the second component 2 via the third component 3.

As the second component 2 transmits a higher change value, it expects in return indices of interrogatable elements of the rows assigned to the change value, which indices together represent a lower number. If in the example given above the second component 2, for example, had sent the change value 415, it expects in return the number $(4 - 4) (6 - 1) (5 - 5) = 050$, and in the case that only one row of 1000 elements had been assigned to the change value, $(999 - 415) = 584$. It follows from the above that, if the third component 3 has decreased the change value, irrespective of the number of rows assigned to the change value, of the number of elements of said rows, and of the numbers of elements of said rows being equal or unequal, the second component 2 will receive numbers which are represented by elements of which at least one will have a higher index than is expected by the second component 2. Because the third component 3 is virtually unable to apply a one-way function inversely, the third component 3 is unable to calculate the number which is represented by elements with lower indices expected by the second component 2.

If the change value is meant to increase the contents of the register of the first component 1, the first component 1 need not to calculate complements, and the sought-for indices of the rows assigned to the change value can be set equal to the corresponding digits of the change value. Each increase of the change value by the third component will then result in a higher index of at least one element than the second component 2 had expected.

According to a second embodiment for the purpose of effecting the check according to the invention, a group of rows, for example rows 4 and 5, is used to represent a checksum. If the change value is meant to decrease the contents of the register of the first component 1, the checksum consists of the sum of the component 1, the checksum consists of the sum of the (radix - 1) complements of the digits of the change value which

are assigned to rows 1, 2 and 3. The digits of the checksum then represent indices of interrogatable elements of the rows 4 and 5 assigned to the checksum. Said elements are sent via the third component 3 to the second component 2, together with an interrogatable element from each of the rows 1, 2 and 3 which have been assigned to the change value, with the indices which are represented by the digits in question of the change value. If the second component 2, for example, transmits the change value 415, the checksum for the set shown in Figure 2 is $(4 - 4) + (6 - 1) + (5 - 5) = 0 + 5 + 0 = 05$. The first component 1 will then send, of the fifth row, the number which is represented by the element with the index 5 and, of the fourth row, the number which is represented by the element with the index 0. If the third component 3 had decreased the change value, for example to 351, the checksum thereof would be $(4 - 3) + (6 - 5) + (5 - 1) = 1 + 1 + 4 = 06$, which points to the element with index 6 of row 5 and the element with index 0 of row 4. The third component 3 is unable to calculate backwards from the number, which is represented by the element with index 6 of row 5, to the number which is expected by the second component 2 and which is represented by the element with index 5 of row 5.

The third component 3 could decrease the change value in such a way that the checksum remains equal. In the example the third component 3 could, for example, set the change value equal to 145. Because the checksum does not change, the third component 3, and therefore also the second component 2, will receive the correct numbers from the rows 4 and 5. However, the first component 1 must also supply the numbers assigned to the change value which are represented by the element with index 4 of row 1, the element with index 1 of row 2 and the element with index 5 of row 3. If the third component 3 has decreased the change value in the abovementioned manner, the third component 3 is then unable to obtain by inverse component 1 and associated with the element with index 4 of row 2, the number expected by the second component 2 and associated with the element with index 1 of row 2. The second component 2 will then, therefore, receive an incorrect number from at least one row, in this example the second row.

If a set of elements is to be used only once, there is no point for the third component 3 to ask the first component 1, prior to a request from the second component 2, for all the elements having the lowest indices of the rows, if use is made of the checksum and the second component at the same time asks for elements of rows assigned to the checksum. If the third component 3, namely, were to ask for all the elements having the lowest in-

dices of the rows, in order to be able, upon receiving them, to calculate the other elements, the first component 1 can be arranged so as to give no response, because the request put virtually cannot or must not arise, or the first component 1 will supply elements from rows of elements assigned to the checksum, having the highest indices from which the third component 3 cannot calculate elements with lower indices.

The condition of being able to use the set only once can be managed safely by the at least partially inaccessible section of the first component, which can, for example, be a "smart card".

If the second component 2 sends the checksum along with the message, and the first component 1 also calculates the checksum, it is possible to detect a fault in the communication between the components and to report this to the second component 2, without the first component 1 immediately incurring the suspicion of making fraudulent actions.

The set of elements, as shown in Figure 2, can comprise more rows of elements than is necessary for checking the correctness of the changing of the contents of the register of the first component 1. An example for the use of the other rows is described in NL-A-9102145 mentioned herein before according to which the second component 2, by application of the additional rows, can check an authenticated digital datum supplied by the first component 1 for its genuineness. The authenticated digital datum represents, for example, a cheque, in which case the change value may represent a monetary value whereby a balance stored in the register can be changed.

It is to be noted that within the context of the invention various modifications are possible. For example, the numbering of the elements of each row of the set, starting from the origin element, can be in decreasing order instead of increasing order, as shown in Figure 2. Further, the cases in which (radix - 1) complements are or are not calculated may be interchanged. The choice of these options depends on what alteration of the change value, for the purpose of changing said register contents of the first component, is to be adjudged to be a fraud. In this context, four cases can be distinguished:

- 1) If the register contents are to be decreased:
 - 1a) the inadmissibly smaller decrease of the register contents;
 - 1b) the inadmissibly larger decrease of the register contents;
 - 1c) the increase of the register contents;
- 2) If the register contents are to be increased:
 - 2a) the inadmissibly lower increase of the register contents;

- 2b) the inadmissibly larger increase of the register contents; and
 2c) the decrease of the register contents.

Claims

1. Method for processing a change value within a system having a number of components operating as participants, a first component having an arithmetic section, which from outside is at least partially unreachable and which has a register which is unreachable directly from outside, and a second component supplying a message, which comprises a change value, to the first component for the purpose of changing the contents of the register, **characterised in that** within the first component a set of elements, which represent numbers, is stored or can be determined from at least one origin element, the set of elements being divided into rows of elements, each second and subsequent element of each row being determined, by applying one or more one-way functions, from the directly preceding element of the row, the successive elements of each row up to, i.e. excluding, an element with a predetermined index, hereinafter called first interrogatable element, being kept secret from the second component, the second component knowing the one-way functions which are used for determining the elements following the first interrogatable element, which elements are interrogatable elements, a component supplying to the second component a first datum which is a function of the origin numbers or of the last elements of the set, the first component, upon receiving the message, sending to the second component interrogatable elements of a first group of rows, of which the indices are determined on the basis of the change value in such a way that at least one of the indices increases if a third component, present in a communication path between the first component and the second component, prior to onward transmission to the first component, increases or decreases the change value received from the second component if the change value is intended to increase or decrease, respectively, the contents of the register, the second component, based on the change value, determining the indices of interrogatable elements of the first group of rows in the same manner, the second component, by applying the one-way functions in question and on the basis of the indices determined by the second component and of the radices of the rows in question, evaluating the received elements up to elements which should be the last elements of said rows, the second component comparing a second datum, obtained from the evaluation and possibly elaborated further, with the previously received first datum and adjudging the changing of the contents of the register to be correct if the comparison results in an identity.
2. Method according to claim 1, **characterised in that** the first group of rows is assigned to the change value, that, if the change value is intended to decrease the contents of the register, the first component determines the (radix - 1) complements of the digits of the change value, which are assigned to the rows in question, and uses said complements as the indices to be determined of interrogatable elements of the first group of rows, and that, if the change value is not intended to decrease the register contents, the last-mentioned indices are determined by the digits of the change value, which are assigned to the rows in question.
3. Method according to claim 1, **characterised in that** the first group of rows is assigned to a checksum which, if the change value is intended to decrease the contents of the register, is represented by the sum of the (radix - 1) complements of digits of the change value, which are assigned to rows in question, and otherwise the checksum is represented by the sum of the digits of the change value, which are assigned to the rows in question, the digits of the checksum representing the indices to be determined of interrogatable elements of the first group of rows, a second group of rows of the set being assigned to the change value, the first component, prior to receiving the message, sending the last elements of the rows of the second group to the second component and, upon receiving the message, sending interrogatable elements to the second component, of which the indices agree with the digits of the change value, which are assigned to the rows in question, and the second component involving the elements, which have been received from the second group on the basis of the last-mentioned indices, in the evaluation and comparison.
4. Method according to claim 3, **characterised in that** both the first component and the second component determine the checksum for their own use.
5. Method according to claim 3 or 4, **characterised in that** the message contains the

checksum which has been determined by the second component.

6. Method according to one of the preceding claims, **characterised in that** the first component does not meet a request, received by means of a message, to supply interrogatable elements having the lowest indices of the rows. 5

7. Method according to one of the preceding claims, **characterised in that** after each message received by the first component, the at least one origin element and the elements which are determined therefrom are changed. 10
15

8. Method according to one of the preceding claims, **characterised in that** for the purpose of determining at least one element which has a lower index than that of the second interrogatable element of a row, a stronger one-way function is applied than a one-way function which is applied for determining an element with a higher index than that of the first interrogatable element. 20
25

9. Method according to claim 8, **characterised in that** with the exception of the stronger one-way function the one-way functions are identical. 30

10. Method according to one of the preceding claims, **characterised in that** the numbers of elements of all the rows are equal. 35

11. Method according to one of the preceding claims, **characterised in that** the first interrogatable element of each row is the second element of the row. 40

12. System suitable for applying the method according to one of the preceding claims. 45

13. System according to claim 12, **characterised in that** the first component is a card having a microcomputer ("smart card"). 50
55

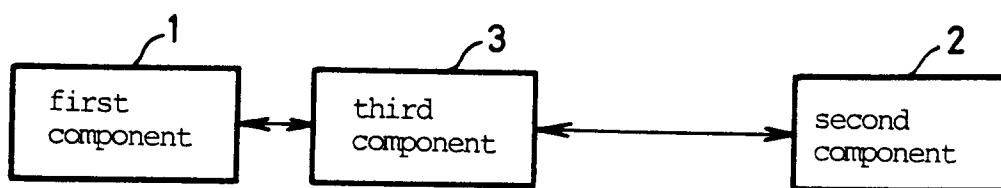


FIG. 1.

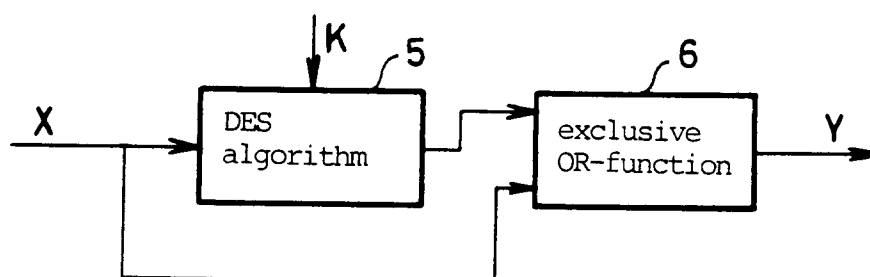


FIG. 3.

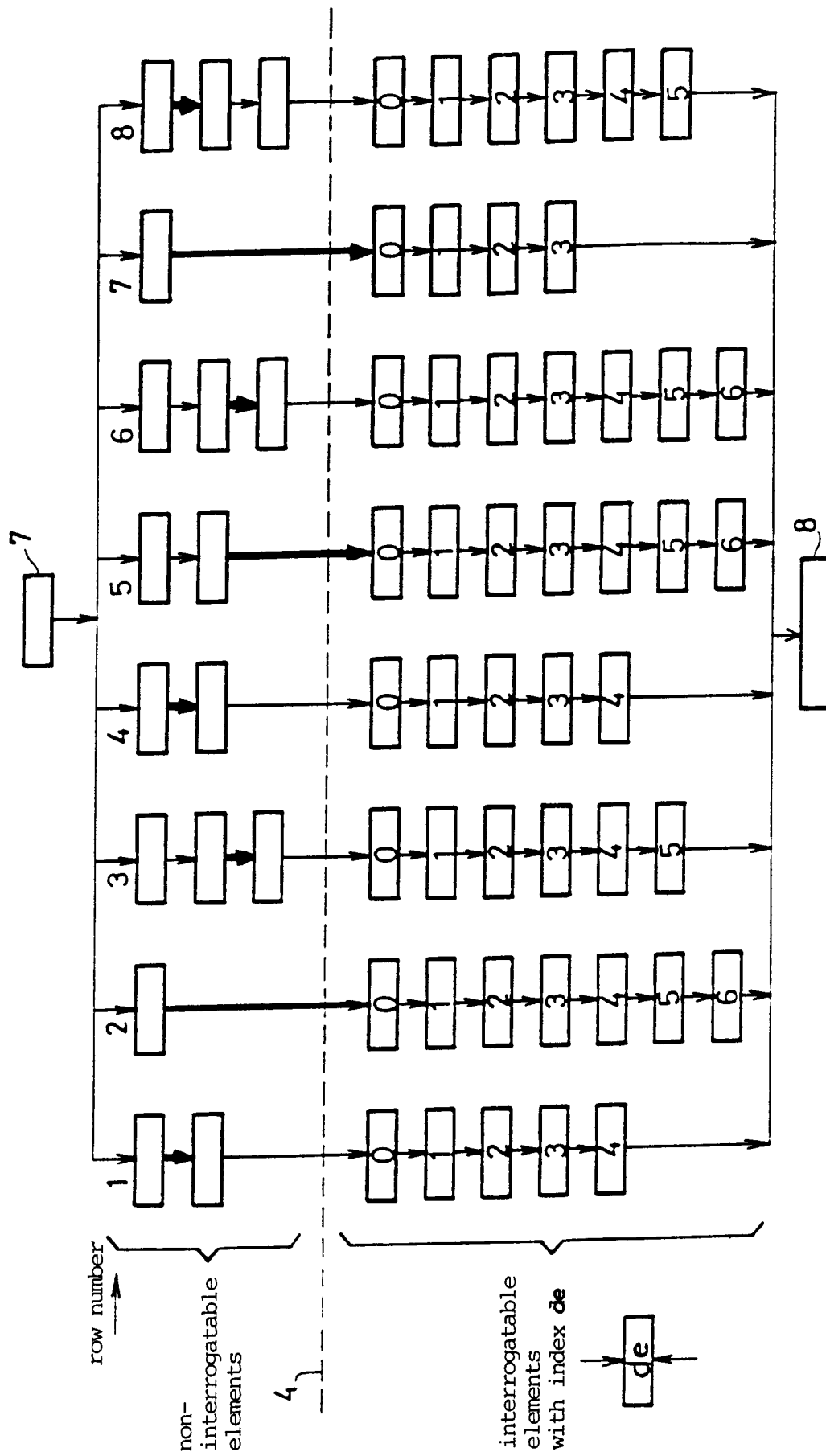


Fig. 2.



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number

EP 92 20 4021

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
X	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 28, no. 2, July 1985, NEW YORK, US; pages 603 - 604 'Matrix Digital Signature for Use with the Data Encryption Algorithm' * the whole document *	1,10	G06F12/14 G06F1/00 H04L9/32 G07F7/10
Y	---	7,12,13	
Y	GB-A-2 050 021 (ATALLA TECHNOVATIONS) * page 3, line 7 - line 96 *	7	
Y	GB-A-2 100 190 (THE GREY LAB ESTABLISHMENT) * abstract; figure 2 * * page 2, line 11 - line 46 * * page 2, line 88 - line 98 * * page 3, line 13 - line 65 *	12,13	
A	EP-A-0 135 888 (SIEMENS) * abstract; figure 2 * * page 2, line 1 - page 3, line 32 *	3-5	
			TECHNICAL FIELDS SEARCHED (Int. Cl.5)
			G06F G07F
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 24 FEBRUARY 1993	Examiner POWELL D.
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			