(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 February 2006 (02.02.2006)

PCT

(10) International Publication Number
WO 2006/010384 A1

(51) International Patent Classification[7]: H04L 29/00

(21) International Application Number:
PCT/EP2004/008665

(22) International Filing Date: 30 July 2004 (30.07.2004)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: TELEFONAKTIEBOLAGET LM ERICSSON (PUB) [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: BOMAN, Krister [SE/SE]; Nimbusgatan 3, S-431 44 Mölndal (SE). AXELSSON, Stefan [SE/SE]; Ljungkullen 66, S-433 66 Sävedalen (SE). HELLBERG, Jan [SE/SE]; Sveaborgsvägen 16, S-430 33 Fjäras (SE).

(74) Agent: ALBIHNS GÖTEBORG AB; Box 142, S-401 22 Göteborg (SE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

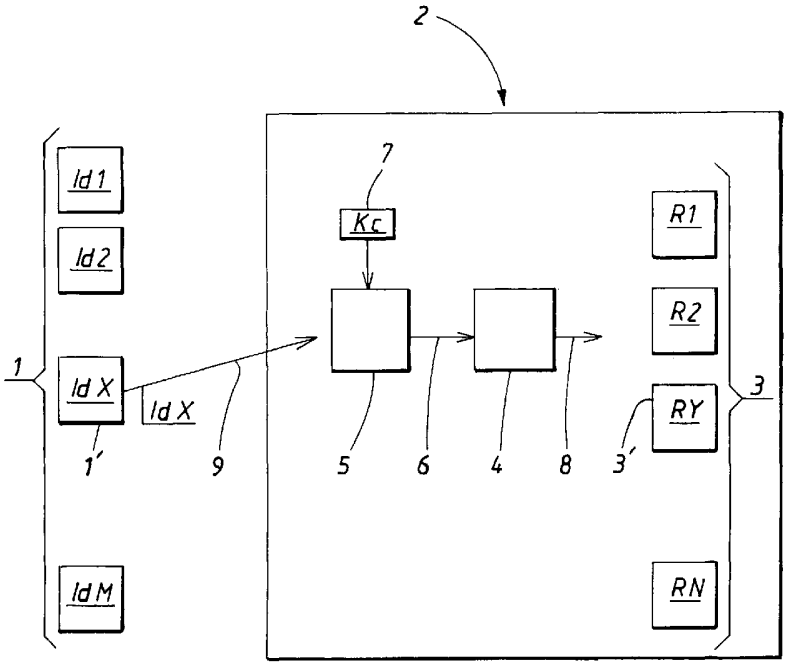
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURE LOAD BALANCING IN A NETWORK



(57) Abstract: The present invention relates to a system comprising at least two resources (3) and a hash function (4), which system is arranged for distributing external users (1) to the resources (3), where the number of users (1) is larger than the number of resources (3). Further, the system comprises means (5) for, at least to a part, creating a uniform distribution. Preferably, the uniformness of the distribution is created by means of an encryption algorithm (5). The present also elates to a method according to the above.

WO 2006/010384 A1

SECURE LOAD BALANCING IN A NETWORK

TECHNICAL FIELD

The present invention relates to a system comprising at least two resources and a hash function, which system is arranged for distributing external users to the resources, where the number of users is larger than the number of resources.

The present invention also relates to a method according to the system above.

BACKGROUND ART

In many application today, a large number of users access a considerable fewer number of resources in a system. The users, on one hand, may be devices handled by humans, the devices may for example be computers and mobile equipment. The resources, on the other hand, may be processes, processors, printers and many other things. A more wide definition of a resource in this context is "something that performs a task for something else". Regarding functionality, the resources are equivalent, thus it is unimportant which resource a certain user is guided to from a functional point of view.

But in order to direct a certain user to the correct resource, it is of great importance that the direction is performed in a balanced way, i.e. that the large number of users is evenly distributed to the relatively few resources, avoiding that some resources are used by very few users and some resources are used by very many users.

Today the above task is generally performed by feeding a user identification code, IdX for user X, to the system comprising the resources. IdX is then fed through a so called hash function.

In this context, a hash function is a transformation that takes data from a definition set and transforms these data to output data in a value set, which output data is called the hash value. The definition set is generally larger than the value set. This means that the hash function is "many to one", i.e. several combinations of input data result in the same output data or hash value. The hash function does not preserve structure. Ideally, for each input data, the possibility for acquiring any of the possible output data should be equal. Any inequalities in the frequency distribution of the input data is transformed into a uniform distribution of output data.

A simple example is where 100 000 users, each one having a user number IdX which is between 1-100 000 identifying each user, share 16 resources numbered 1-16. The hash function may then be of such a sort that it evenly distributes the users among the resources according to a simple algorithm. For example, each sixteenth user is directed to the same resource. Then the users 1, 17, 33, 49 ... are directed to resource number 1, the users 2, 18, 34, 50 ... are directed to resource number 2, and so on.

The main feature of the hash function is that it directs the user in question to one of the resources 1-16. Generally, the hash function results in an identical result for a number of different inputs, i.e. many different inputs result in relatively few different outputs. This is called "many to one".

If the resources, to which the users are guided, each one is adapted to handle an equivalent amount of users, it is important that the hash function produces a uniformly distributed output. Then the users are uniformly distributed among the resources, causing a load balance.

There may, however, be problems due to accident as well as on purpose. Accidentally, the users may consist of different groups, requesting access to the resources to different degrees. If these groups are unfortunately balanced, the users that are guided to a certain resource by the hash function may request access to the resources to a larger extent than the other users. This certain resource is then subject to a larger load than the other resources, resulting in a biased load balance among the resources.

On purpose, so-called "hash attacks" occur, which are intended to cause a biased load balance among the resources. The hash attacks are generally made possible by the attackers having sufficient knowledge about the system and/or the attackers making use of information that is output from the system comprising the resources. The attackers then see to that each request for resources, when passing the hash function, is guided to one and the same resource. This resource is then subject to an unusually high load, and then functions more or less inefficiently, which may result in a so called "denial of service", where the resource does not accept any more users. This may affect the service efficiency of the whole system.

The reason for unleashing a hash attack is to achieve a "denial of service", i.e. making one or more resources unavailable for other users. The other users that are guided to the attacked resource or resources, which other users are unaware of that a hash attack is in progress, only perceive that the service they are requesting is unavailable. This reveals a poor service availability for the other users, which in turn impairs the good will and thus the trademark of the service provider.

Today, there are server systems which are arranged to adapt the hash function due to the current load balance, and prevent that a biased load balance occur. This adaptive arrangement requires a lot of system resources and maintenance, and may have difficulties keeping up with occurring load imbalances that occur during a hash attack. Even if the adaptive system is able to achieve a proper load balance during a hash attack, the adaptive

procedure generally requires such an amount of system of resources that a "denial of service" situation more or less occurs anyway, since the system is busy defending itself. The attacker thus achieves its goal anyway.

DISCLOSURE OF THE INVENTION

It is an object of the present invention to provide a system and a method for preventing hash attacks by assuring that a proper load balance is maintained, only requiring a small amount of system resources.

This object is solved by means of a system according to the preamble of claim 1, which system further comprises means for, at least to a part, creating a uniform distribution.

This object is further solved by means of a method according to the preamble of claim 10, which method further comprises the steps: inputting a unique user identification code or number and creating a uniform distribution of the users to the resources, where the distribution is accomplished by using a hash function.

Preferably, the uniformness of the distribution according to the system and method above is created by means of an encryption algorithm.

Preferred embodiments are disclosed in the dependent claims.

Several advantages are obtained by means of the present invention. For example:

- An inexpensive means, requiring very little maintenance, for preventing a hash attack is obtained.
- A hash attack may be prevented using very little system resources.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will now be described more in detail with reference to the enclosed drawings, where:

Figure 1 shows a general overview of a system according to a first embodiment of the invention;

Figure 2 shows a general overview of a system according to a second embodiment of the invention; and

Figure 3 shows a general overview of a system according to a third embodiment of the invention.

EMBODIMENTS OF THE INVENTION

As shown in Figure 1, a number M of users 1, each one having an identification code or number Id1 to IdM, is able to connect to a system 2 having a number N of resources 3, each one having an identification code or number R1 to RN, where the number M of users 1 is much larger than the number N of resources 3, i.e. M>>N. The users 1 may for example be mobile equipment, such as mobile telephones or mobile computers, handled by mobile equipment owners, and the system 2 may be a mobile equipment node, and where the resources 3 are services provided at the mobile equipment system node.

If a certain user 1', having a certain identification code or number IdX, wants to access a resource in the system, it is unimportant which one of the resources 3 the user should be guided to from a functional point of view. In order to achieve an even load balance of users 1 for the resources 3, the IdX identification code or number is passed through a hash function 4, which hash function 4 creates an even spread of the users 1, distributing them among the available resources 3.

According to the present invention, in order to randomize which resource 3 a certain user 1 is guided to, the input to the hash function 4 is first

randomized. This is obtained by encrypting the input data to the hash function 4, using an encryption algorithm 5, where the encryption produces a cipher 6 by using at least a cipher key Kc 7. This cipher 6 is used as an input to the hash function 4, which produces a hash value 8, guiding the user to a certain resource 3', having a certain identification code or number RY, among the available resources 3.

The encryption algorithm 5 produces a unique output cipher 6 for a certain input 9 at a certain time, this is called "one to one". A good encryption algorithm 5 provides a uniform output, which output ideally is completely randomized. As the encryption is used as a randomizer, "whitening" the input 6 to the hash function 4, no decryption takes place at all. It is important that the encryption is of a such kind that a non-repeating randomizing is acquired. A certain input 9 should then result in any output 6 within the encryption output range, having the same probability for acquiring any value within the encryption output range every time. Thus a uniform distribution of the users 1 among the resources 3 is obtained.

A simple example, still with reference to Figure 1, is where 100 000 users 1, each one having a user number IdX which is between 1-100 000, identifying each user, share 16 resources 3, each resource having a user number RY which is between 1 and 16. In other words, M = 100 000 and N = 16. The hash function 4 evenly distributes the users among the resources 3. The output of the hash function 4 directs the user to one of the resources 3. Before feeding the user number IdX into the hash function 4, it is encrypted by an encryption algorithm 5, randomizing the user number IdX. The range of the encryption output 6, the cipher, may be much larger than the number M of users 1, although it is not necessary.

If user number 50 000 wants to use a resource 3, the number 50 000 is encrypted and the encryption then produces a number within the encryption output range. Each time the number 50 000 is encrypted, any output within

the output range is produced, having the same probability for acquiring any value within the output range every time the number 50 000 is encrypted. This is the case for any user number being fed into the encryption algorithm 5.

According to the example, the hash function 4 evenly produces a number in the range 1-16 as an output 8. The hash function 4 according to this example always produces the same output for a given input. As the encryption algorithm 5 produces any number within the encryption output range every time an input is fed into the encryption algorithm 5, the hash function 4 is fed with any number within the encryption output range every time an input 9 is fed into the encryption algorithm 5. As the input 6 to the hash function 4 is randomized, the output 8 from the hash function 4 is also randomized, making hash attacks unfeasible, since the distribution is uniformed.

As shown in Figure 2, according to a second embodiment, the user's input 9 into the system 2 is fed into a hash function 4 first, and then the output 8 of the hash function 4 is randomized by means of an encryption algorithm 5. The encryption algorithm 5 then preferably has an output which is easy to translate to a certain identification code or number RY of the resources 3.

Further, as shown in Figure 3, according to a third embodiment, the user's input 9 into the system is fed into a so-called keyed hash function 10, which provides a randomized output 11. In order to achieve this, a hash key Kh 12 is used for the keyed hash function 10. As before, encryption has to be of such a kind that each time when one certain input 9 into the system 2 is fed into the keyed hash function 10, any output 11 within the output range is produced, having the same probability for acquiring any value within the output range every time. In this case, no separate encryption algorithm is used, but the encryption and the load distribution is all taken care of by the keyed hash function 10. The keyed hash function 10 preferably has an output

11 which is easy to translate to a certain identification code or number RY of the resources 3.

The efficiency of any randomizing procedure is purely dependent on the efficiency of the encryption algorithm. The more randomized encryption that is produced, the more randomized output from the hash function in question is produced and then a more even load balance is acquired for the resources. A wide variety of encryption algorithms exists, having different kinds of cipher keys, and will not be discussed in more detail here. The main feature of the present invention is to use a function that have randomizing properties, and a suitable encryption function should not be difficult to find for the skilled person. Any other randomizing means is also conceivable within the scope of the present invention.

The invention is not limited to the above described embodiments, but may vary freely within the scope of the appended claims. The users may for example be computers, where the system is a computer network comprising computer system resources, such as servers and printers, to which the users are directed.

Encryption algorithms that may form basis for the encryption algorithm according to the invention may for example be AES (Advanced Encryption Standard).

Encryption algorithms may not only use a cipher key Kc for generating a cipher, but other kinds of initializing data are also conceivable.

CLAIMS

1. A system comprising at least two resources (3) and a hash function (4), which system is arranged for distributing external users (1) to the resources (3), where the number of users (1) is larger than the number of resources (3), characterized in that the system further comprises means (5) for, at least to a part, creating a uniform distribution.

2. A system according to claim 1, characterized in that the uniformness of the distribution is created by means of an encryption algorithm (5).

3. A system according to claim 2, characterized in that the encryption algorithm (5) encrypts a unique user identification code or number (IdX) and sends the cipher output (6) to the hash function (4).

4. A system according to claim 3, characterized in that the hash function output (8) is arranged to be linked to a certain resource (3').

5. A system according to claim 2, characterized in that the hash function (4) is arranged to be fed at its input with a unique user identification code or number (IdX), and sends the hash function (4) output (8) to the encryption algorithm (5).

6. A system according to claim 5, characterized in that the cipher output (6) is arranged to be linked to a certain resource (3').

7. A system according to claim 2, characterized in that the encryption algorithm is a part of the hash function, which hash function thus constitutes a so-called keyed hash function (10).

8. A system according to any one of the previous claims, characterized in that the users (1) are pieces of mobile equipment handled by mobile equipment owners, and that the system (2) is a mobile

equipment system node, and where the resources (3) are services provided at the mobile equipment system node.

9. A system according to any one of the claims 1-7, characterized in that the users (1) are computers, where the system (2) is a computer network, and where the resources (3) are computer system resources to which the computers are directed.

10. A method for distributing external users (1) to at least two resources (3) in a system, where the number of users (1) is larger than the number of resources (3), which method comprises the steps:
inputting a unique user identification code or number (IdX) into the system; and
creating a uniform distribution of the users (1) to the resources (3), where the distribution is accomplished by using a hash function (4).

11. A method according to claim 10, characterized in that the uniformness of the distribution is created by means of an encryption algorithm (5).

12. A method according to claim 11, characterized in that the encryption algorithm (5) encrypts a unique user identification code or number (IdX) and sends the cipher output (6) to the hash function (4).

13. A method according to claim 12, characterized in that the hash function output (8) is linked to a certain resource (3').

14. A method according to claim 11, characterized in that the hash function (4) is fed at its input with the unique user identification code or number (IdX), and sends the hash function output (8) to the encryption algorithm (5).

15. A method according to claim 14, characterized in that the cipher output (6) is linked to a certain resource (3').

16. A method according to claim 11, characterized in that the encryption algorithm is a part of the hash function, which hash function thus constitutes a so-called keyed hash function (10).

17. A method according to any one of the claims 10-16, characterized in that the users (1) are pieces of mobile equipment handled by mobile equipment owners, and that the system (2) is a mobile equipment system node, and where the resources (3) are services provided at the mobile equipment system node.

18. A method according to any one of the claims 10-16, characterized in that the users (1) are computers, where the system (2) is a computer network, and where the resources (3) are computer system resources to which the computers are directed.

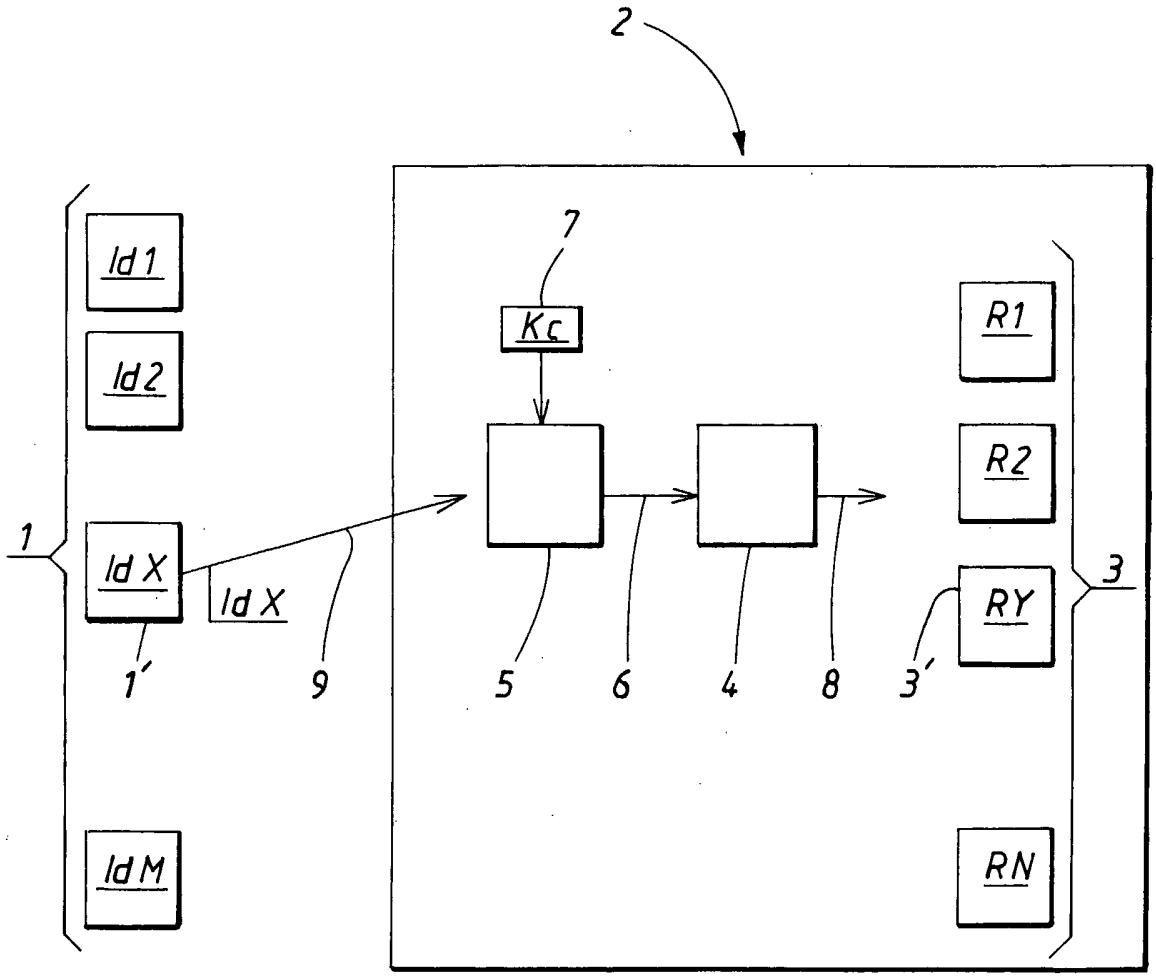


FIG.1

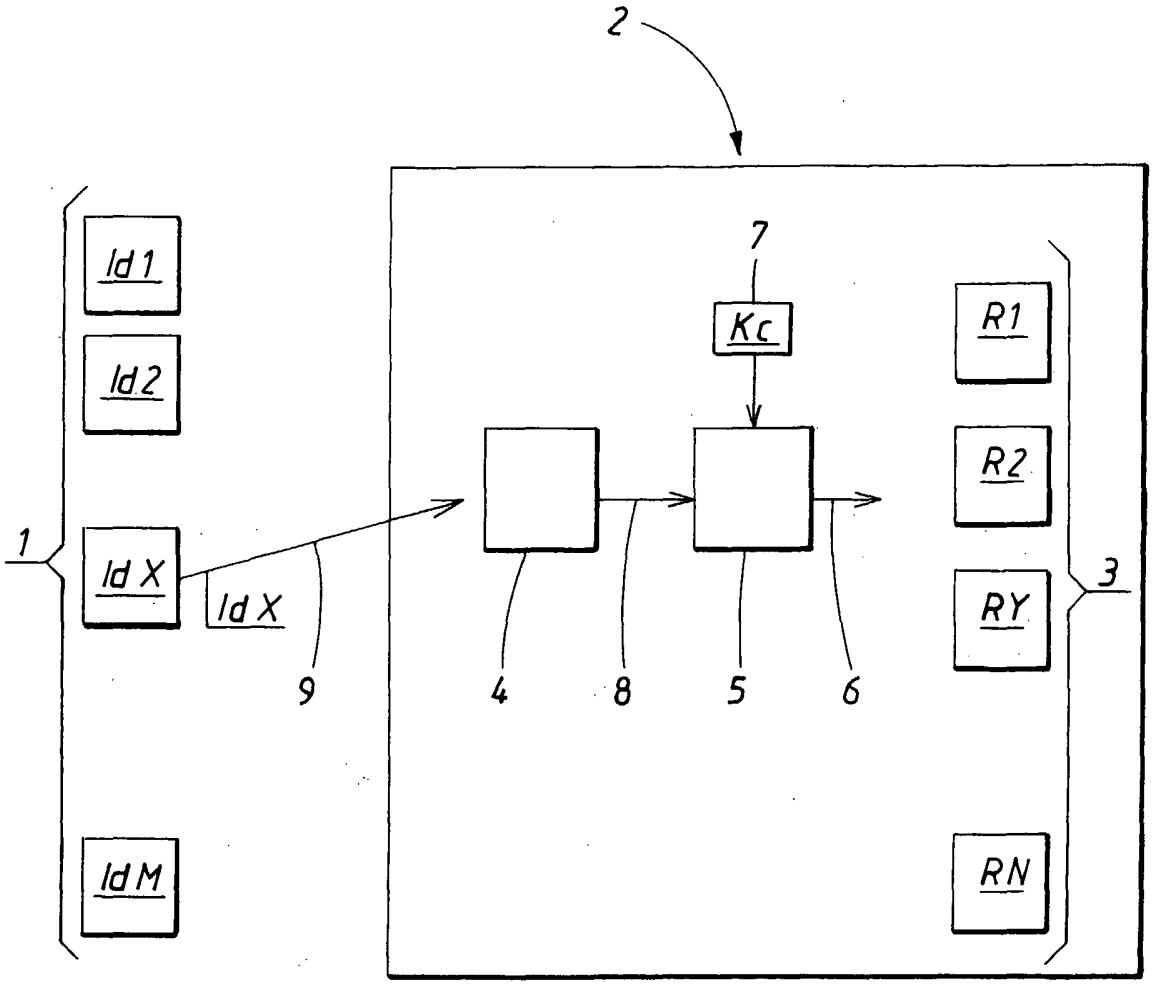


FIG. 2

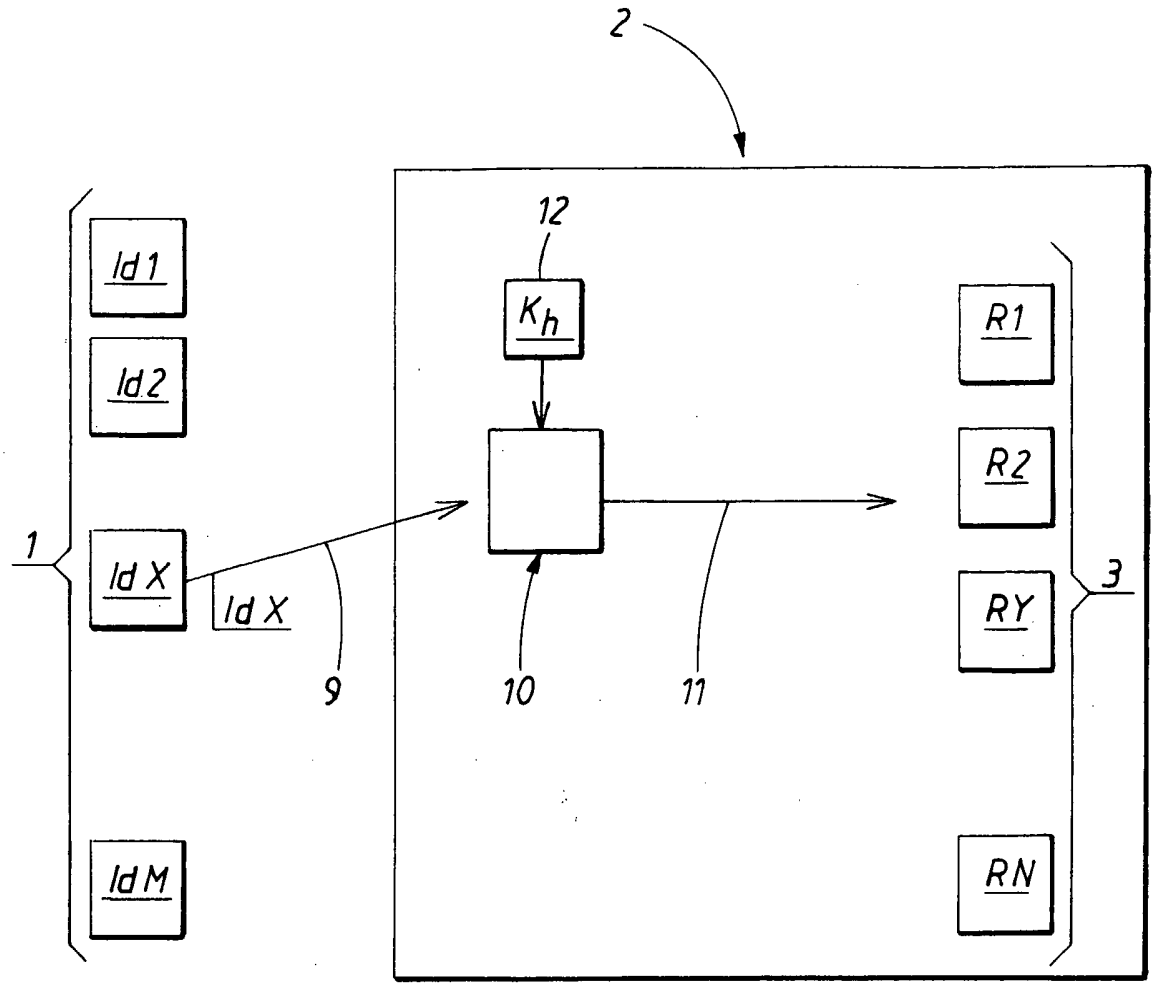


FIG. 3

INTERNATIONAL SEARCH REPORT

International Application No
[redacted]/EP2004/008665

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/00

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)
IPC 7 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 practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 03/069474 A (TELEFONAKTIEBOLAGET L M ERICSSON ; WILLEHADSON, STEFAN; DANNE, ANDERS;) 21 August 2003 (2003-08-21) abstract page 4, line 18 - line 32 page 5, line 23 - page 8, line 9 page 8, line 25 - page 9, line 27 figures 1,2	1,2, 8-11,17, 18
X	US 6 601 084 B1 (BHASKARAN SAJIT ET AL) 29 July 2003 (2003-07-29) abstract column 2, line 60 - column 4, line 15 figures 1-3,5A-6D,11	1,2, 8-11,17, 18

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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 document 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	Date of mailing of the international search report
14 April 2005	27/04/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bichler, M

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/008665

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 078 957 A (ADELMAN ET AL) 20 June 2000 (2000-06-20) abstract column 2, line 56 - column 4, line 48 column 9, line 22 - column 10, line 44 figures 1,4	1,2, 8-11,17, 18

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/008665

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 03069474 A	21-08-2003	AU 2002314685 A1	04-09-2003
		DE 10297645 T5	24-02-2005
		GB 2402780 A	15-12-2004
		WO 03069474 A1	21-08-2003
US 6601084 B1	29-07-2003	AU 764546 B2	21-08-2003
		AU 1903999 A	12-07-1999
		CA 2319449 A1	01-07-1999
		EP 1116082 A2	18-07-2001
		WO 9932956 A2	01-07-1999
US 6078957 A	20-06-2000	AU 1211500 A	13-06-2000
		CA 2351413 A1	02-06-2000
		DE 69915871 D1	29-04-2004
		DE 69915871 T2	03-02-2005
		EP 1135726 A2	26-09-2001
		JP 2003518338 T	03-06-2003
		WO 0031942 A2	02-06-2000