(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 356 822**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04763727 .7**
(96) Fecha de presentación : **30.07.2004**
(97) Número de publicación de la solicitud: **1771988**
(97) Fecha de publicación de la solicitud: **11.04.2007**

(54) Título: **Equilibrio de carga segura en una red.**

(45) Fecha de publicación de la mención BOPI:
13.04.2011

(45) Fecha de la publicación del folleto de la patente:
13.04.2011

(73) Titular/es: **Telefonaktiebolaget LM Ericsson (publ)**
Patent Unit
164 83 Stockholm, SE

(72) Inventor/es: **Boman, Krister;**
Axelsson, Stefan y
Hellberg, Jan

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

CAMPO TÉCNICO

La presente invención se refiere a un sistema que comprende al menos dos recursos y una función hash, sistema que está organizado para distribuir usuarios externos por los recursos, en el que el número de usuarios es mayor que el número de recursos.

La presente invención también se refiere a un procedimiento según el sistema anterior.

ESTADO ACTUAL DE LA TÉCNICA

Hoy en día en muchas aplicaciones, un gran número de usuarios acceden a un considerable menor número de recursos en un sistema. Por una parte, los usuarios pueden ser dispositivos manejados por personas, pudiendo ser los dispositivos, por ejemplo, ordenadores y equipo móvil. Por otra parte, los recursos pueden ser procesos, procesadores, impresoras y muchas otras cosas. Una definición más amplia de un recurso en este contexto es "algo que realiza una tarea para algo diferente". Atendiendo a la funcionalidad, los recursos son equivalentes, con lo que carece de importancia hacia qué recurso es guiado determinado usuario desde un punto de vista funcional.

No obstante, para dirigir a un determinado usuario hacia el correcto recurso, es de gran importancia que la dirección se efectúe de una manera equilibrada, es decir, que el gran número de usuarios sea equidistribuido por los relativamente escasos recursos, evitando que algunos recursos sean utilizados por muy pocos usuarios y algunos recursos sean utilizados por muchos más usuarios.

Hoy en día, la anterior tarea se efectúa en general alimentando un código de identificación de usuario, IdX por usuario X, al sistema que comprende los recursos. Entonces se alimenta IdX a través de lo que se denomina una función hash.

En este contexto, una función hash es una transformación que toma datos de un conjunto de definiciones y transforma estos datos en datos de salida de un conjunto de valores, datos de salida que se denominan el valor hash. El conjunto de definiciones generalmente es mayor que el conjunto de valores. Esto implica que la función hash es "varios a uno", es decir, varias combinaciones de datos de entrada dan por resultado los mismos datos de salida o valor hash.

La función hash no preserva la estructura. Idealmente, para cada dato de entrada, la posibilidad de adquirir cualquiera entre los posibles datos de salida debería ser igual. Cualesquiera desigualdades en la frecuencia de distribución de los datos de entrada son transformadas en una distribución uniforme de datos de salida.

Un ejemplo sencillo es cuando 100 000 usuarios, teniendo cada uno de ellos un número de usuario IdX que se halla entre 1 y 100 000 identificando a cada usuario, comparten 16 recursos numerados 1 a 16. La función hash podría ser entonces de tal clase que distribuya regularmente a los usuarios entre los recursos de acuerdo con un algoritmo sencillo. Por ejemplo, cada decimosexto usuario es dirigido hacia el mismo recurso. Entonces los usuarios 1, 17, 33, 49,... son dirigidos hacia el recurso número 1, los usuarios 2, 18, 34, 50,... son dirigidos hacia el recurso número 2 y así sucesivamente.

La característica principal de la función hash es que dirige al usuario en cuestión hacia uno de los recursos 1 a 16.

En general, la función hash da por resultado un idéntico resultado para cierto número de entradas diferentes, es decir, muchas entradas diferentes dan por resultado relativamente pocas salidas diferentes. Esto se denomina "varios a uno".

Si cada uno de los recursos, hacia los que son guiados los usuarios, está adaptado para manejar una cantidad equivalente de usuarios, es importante que la función hash produzca una salida distribuida uniformemente. Entonces los usuarios son distribuidos uniformemente entre los recursos, provocando un equilibrio de carga.

La divulgación WO03/069474 propone una distribución de los usuarios por los recursos en función de la naturaleza de la tarea, es decir, ronda (round robin) si la tarea es una tarea de procesamiento y hash si la tarea es de almacenamiento.

Sin embargo, puede haber problemas a consecuencia de accidente o a propósito.

Por accidente, los usuarios pueden consistir en diferentes grupos, que solicitan acceso a los recursos en diferentes grados. Si estos grupos son distribuidos desacertadamente, los usuarios que son guiados hacia un determinado recurso por la función hash pueden solicitar acceso a los recursos en mayor medida que los demás usuarios. Este determinado recurso se ve sometido entonces a una mayor carga que los demás recursos, dando por resultado un equilibrio de carga sesgado entre los recursos.

A propósito tienen lugar los denominados "ataques hash", cuya intención es provocar un equilibrio de carga sesgado entre los recursos. Los ataques hash generalmente los hacen posibles atacantes que tienen suficiente conocimiento del sistema y/o los atacantes que se valen de información que proporciona a su salida el sistema que

comprende los recursos. Los atacantes procuran entonces que cada petición de recursos, al pasar por la función hash, sea guiada hacia un mismo recurso. Este recurso se ve sometido entonces a una carga excepcionalmente alta y funciona entonces de manera más o menos ineficiente, lo que puede dar por resultado lo que se denomina una "denegación de servicio", en la que el recurso deja de aceptar usuarios. Esto puede repercutir en la eficacia de servicio del sistema completo.

El motivo de desencadenar un ataque hash es el de lograr una "denegación de servicio", es decir, hacer que uno o más recursos no estén disponibles para otros usuarios. Los otros usuarios que son guiados hacia el recurso o recursos atacados, cuyos otros usuarios no se dan cuenta de que se está desarrollando un ataque hash, sólo perciben que el servicio que están solicitando no está disponible. Esto revela una mediocre disponibilidad de servicio para los otros usuarios, lo que a su vez perjudica el fondo de comercio y, así, la marca comercial del proveedor de servicios.

Hoy en día, existen varios sistemas servidores que están organizados para adaptar la función hash debido al equilibrio de carga en curso e impedir que tenga lugar un equilibrio de carga sesgado. Esta organización adaptativa requiere muchos recursos del sistema y mantenimiento y puede tener dificultades para mantenerse al producirse desequilibrios de carga que tienen lugar durante un ataque hash. Incluso si el sistema adaptativo es capaz de lograr un adecuado equilibrio de carga durante un ataque hash, el procedimiento adaptativo requiere generalmente tal cantidad de recursos del sistema que, de todos modos, en mayor o menor medida se produce una situación de "denegación de servicio", puesto que el sistema está ocupado defendiéndose a sí mismo. En cualquier caso, el atacante logra así su objetivo.

EXPLICACIÓN DE LA INVENCIÓN

La presente invención tiene por objeto proporcionar un sistema y un procedimiento para impedir ataques hash asegurando que se mantiene un adecuado equilibrio de carga, que únicamente requieren una pequeña cantidad de recursos del sistema.

Un aspecto de la presente invención es un aparato según se define en la reivindicación independiente 1. Otro aspecto de la invención es un procedimiento según se define en la reivindicación independiente 9. Formas de realización adicionales de la invención están especificadas en las respectivas reivindicaciones dependientes que se adjuntan.

Con preferencia, la uniformidad de la distribución según el sistema y procedimiento anteriores se crea por medio de un algoritmo de cifrado.

Formas de realización preferidas se desvelan en las reivindicaciones dependientes.

Por medio de la presente invención se obtienen diversas ventajas. Por ejemplo:

- Se obtiene un medio económico, que requiere muy poco mantenimiento, para impedir un ataque hash.
- Se puede impedir un ataque hash utilizando muy pocos recursos del sistema.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

A continuación se describirá la invención con más detalle, con referencia a los dibujos que se acompañan, en los que:

La figura 1 muestra una vista general de conjunto de un sistema según una primera forma de realización de la invención;

la figura 2 muestra una vista general de conjunto de un sistema según una segunda forma de realización de la invención; y

la figura 3 muestra una vista general de conjunto de un sistema según una tercera forma de realización de la invención.

FORMAS DE REALIZACIÓN DE LA INVENCIÓN

Según se muestra en la figura 1, cierto número M de usuarios 1, teniendo cada uno de ellos un código o número de identificación Id1 a IdM, es capaz de conectarse a un sistema 2 que tiene cierto número N de recursos 3, teniendo cada uno de ellos un código o número de identificación R1 a RN, donde el número M de usuarios 1 es mucho mayor que el número N de recursos 3, es decir, M>>N. Los usuarios 1 pueden ser, por ejemplo, equipo móvil, tal como teléfonos móviles u ordenadores móviles, manejados por propietarios del equipo móvil, y el sistema 2 puede ser un nodo de equipo móvil, y en el que los recursos 3 son servicios proporcionados en el nodo del sistema de equipo móvil.

Si un determinado usuario 1', que tiene un determinado código o número de identificación IdX, quiere acceder a un recurso en el sistema, carece de importancia, desde un punto de vista funcional, hacia cuál de los

recursos 3 debería ser guiado el usuario. Para poder lograr un equilibrio de carga regular de usuarios 1 para los recursos 3, se hace pasar el código o número de identificación IdX por una función hash 4, función hash 4 que crea una difusión regular de los usuarios 1, distribuyéndolos entre los recursos disponibles 3.

De acuerdo con la presente invención, para poder aleatorizar hacia qué recurso 3 es guiado un determinado usuario 1, en primer lugar se aleatoriza la entrada a la función hash 4. Esto se obtiene cifrando los datos de entrada a la función hash 4, utilizando un algoritmo de cifrado 5, donde el cifrado produce una cifra 6 utilizando al menos una clave de cifrado Kc 7. Esta cifra 6 se utiliza como entrada a la función hash 4, que produce un valor hash 8, que guía al usuario hacia un determinado recurso 3', con un determinado código o numero de identificación RY, de entre los recursos disponibles 3.

El algoritmo de cifrado 5 produce una cifra de salida única 6 para una determinada entrada 9 en un determinado momento; esto se denomina "uno a uno". Un buen algoritmo de cifrado 5 proporciona una salida uniforme, salida que en el mejor de los casos está completamente aleatorizada. Como el cifrado se utiliza como aleatorizador, "blanqueando" la entrada 6 a la función hash 4, no tiene lugar ningún descifrado en forma alguna. Es importante que el cifrado sea de tal clase que se adquiera una aleatorización sin repetición. Entonces una determinada entrada 9 debería dar por resultado cualquier salida 6 dentro del intervalo de salidas de cifrado, teniendo cada vez la misma probabilidad de adquirir cualquier valor dentro del intervalo de salidas de cifrado. Así, se obtiene una distribución uniforme de los usuarios 1 entre los recursos 3.

Un ejemplo sencillo, todavía con referencia a la figura 1, es donde 100 000 usuarios 1, teniendo cada uno de ellos un número de usuario IdX que se halla entre 1 y 100 000, identificador de cada usuario, comparten 16 recursos 3, teniendo cada recurso un número de identificación RY que se halla entre 1 y 16. En otras palabras, M = 100 000 y N = 16. La función hash 4 distribuye regularmente a los usuarios entre los recursos 3. La salida de la función hash 4 dirige al usuario hacia uno de los recursos 3. Antes de alimentar el número de usuario IdX en la función hash 4, éste es cifrado mediante un algoritmo de cifrado 5, que aleatoriza el número de usuario IdX. El intervalo de la salida de cifrado 6, la cifra, puede ser mucho mayor que el número M de usuarios 1, aunque no es necesario.

Si el usuario número 50 000 quiere utilizar un recurso 3, se cifra el número 50 000 y el cifrado produce entonces un número dentro del intervalo de salidas de cifrado. Cada vez que se cifra el número 50 000, se produce cualquier salida dentro del intervalo de salidas, teniendo la misma probabilidad de adquirir cualquier valor dentro del intervalo de salidas cada vez que se cifra el número 50 000. Tal es el caso para cualquier número de usuario que se alimenta en el algoritmo de cifrado 5.

De acuerdo con el ejemplo, la función hash 4 produce regularmente como salida 8 un número en el intervalo 1 a 16. La función hash 4 según este ejemplo siempre produce la misma salida para una entrada dada. Como el algoritmo de cifrado 5 produce cualquier número dentro del intervalo de salidas de cifrado cada vez que se alimenta una entrada en el algoritmo de cifrado 5, la función hash 4 se alimenta con cualquier número dentro del intervalo de salidas de cifrado cada vez que se alimenta una entrada 9 en el algoritmo de cifrado 5. Como la entrada 6 a la función hash 4 es aleatorizada, la salida 8 de la función hash 4 también es aleatorizada, haciendo impracticables los ataques hash, puesto que la distribución está uniformizada.

Según se muestra en la figura 2, de acuerdo con una segunda forma de realización, la entrada de usuario 9 en el sistema 2 se alimenta en primer lugar en una función hash 4 y luego se aleatoriza la salida 8 de la función hash 4 por medio de un algoritmo de cifrado 5. El algoritmo de cifrado 5 tiene entonces preferentemente una salida que es fácil de traducir en un determinado código o número de identificación RY de los recursos 3.

Además, según se muestra en la figura 3, de acuerdo con una tercera forma de realización, la entrada de usuario 9 en el sistema se alimenta en lo que se denomina una función hash por clave 10, que proporciona una salida aleatorizada 11. Con el fin de lograr esto, se utiliza una clave de hash Kh 12 para la función hash por clave 10.

Al igual que anteriormente, el cifrado tiene que ser de tal clase que siempre que se alimenta una determinada entrada 9 en el sistema 2 en la función hash por clave 10, se produce cualquier salida 11 dentro del intervalo de salidas, teniendo cada vez la misma probabilidad de adquirir cualquier valor dentro del intervalo de salidas. En este caso, no se utiliza ningún algoritmo de cifrado distinto, sino que la función hash por clave 10 se encargará tanto del cifrado como de la distribución de carga. La función hash por clave 10 tiene preferentemente una salida 11 que es fácil de traducir en un determinado código o número de identificación RY de los recursos 3.

La eficacia del procedimiento de aleatorización depende íntegramente de la eficacia del algoritmo de cifrado. Cuanto más aleatorizado sea el cifrado que se produce, más aleatorizada estará la salida de la función hash en cuestión que se produce y, entonces, se adquirirá para los recursos un equilibrio de carga más regular. Existe una amplia variedad de algoritmos de cifrado, que tienen diferentes clases de claves de cifrado, y no serán examinados con más detalle en este documento. La principal característica de la presente invención es la de utilizar una función que tiene propiedades de aleatorización y, para el experto en la materia, no debería de ser difícil hallar una función de cifrado apropiada. Cualquier otro medio de aleatorización también es concebible en el campo de aplicación de la presente invención.

La invención no queda limitada a las formas de realización anteriormente descritas, sino que puede variar

libremente dentro del campo de aplicación de las reivindicaciones que se adjuntan. Los usuarios pueden ser, por ejemplo, ordenadores, donde el sistema es una red de ordenadores que comprende recursos de sistema informático, tales como servidores e impresoras, hacia los que son dirigidos los usuarios.

Los algoritmos de cifrado que pueden constituir la base para el algoritmo de cifrado según la invención pueden ser, por ejemplo, AES (estándar avanzado de cifrado).

Los algoritmos de cifrado no sólo pueden utilizar una clave de cifrado Kc para generar una cifra, sino que también son concebibles otras clases de datos de inicialización.

REIVINDICACIONES

1. Un sistema que comprende al menos dos recursos (3) y una función hash (4), en el que la función hash (4) está organizada para distribuir usuarios externos (1) por los recursos (3), cuyos usuarios externos (1) cobran la forma de

dispositivos manipulados por personas, donde el número de usuarios (1) es mayor que el número de recursos (3),

caracterizado porque el sistema comprende además un medio de aleatorización (5) que, junto con la función hash (4), está organizado para crear, al menos en parte, una distribución uniforme de los usuarios externos (1) entre los recursos (3), en el que el medio de aleatorización (5) se materializa en un algoritmo de cifrado en el que una entrada da por resultado cualquier salida dentro de un intervalo de salidas de cifrado, teniendo la misma probabilidad de adquirir cualquier valor dentro del intervalo de salidas de cifrado cada vez que se cifra la entrada.

2. Un sistema según la reivindicación 1, **caracterizado porque** el algoritmo de cifrado (5) cifra un código o número de identificación de usuario único (IdX) y envía la salida de cifrado (6) a la función hash (4).

3. Un sistema según la reivindicación 2, **caracterizado porque** la salida de la función hash (8) está organizada para ser vinculada a un determinado recurso (3').

4. Un sistema según la reivindicación 1, **caracterizado porque** la función hash (4) está organizada para ser alimentada por su entrada con un código o número de identificación de usuario único (IdX) y envía la salida (8) de la función hash (4) al algoritmo de cifrado (5).

5. Un sistema según la reivindicación 4, **caracterizado porque** la salida de cifrado (6) está organizada para ser vinculada a un determinado recurso (3').

6. Un sistema según la reivindicación 1, **caracterizado porque** el algoritmo de cifrado forma parte de la función hash, función hash que constituye así lo que se denomina una función hash por clave (10).

7. Un sistema según una cualquiera de las reivindicaciones precedentes, **caracterizado porque** los usuarios (1) son piezas de equipo móvil manejadas por propietarios de equipo móvil y porque el sistema (2) es un nodo del sistema de equipo móvil, y en el que los recursos (3) son servicios proporcionados en el nodo del sistema de equipo móvil.

8. Un sistema según una cualquiera de las reivindicaciones 1 a 6, **caracterizado porque** los usuarios (1) son ordenadores, en el que el sistema (2) es una red de ordenadores y en el que los recursos (3) son recursos de sistema informático hacia los que son dirigidos los ordenadores.

9. Un procedimiento de distribución de usuarios externos (1) por al menos dos recursos (3) en un sistema, cuyos usuarios externos (1) cobran la forma de dispositivos manejados por personas, en el que el número de usuarios (1) es mayor que el número de recursos (3), procedimiento que comprende la etapa de introducir un código o número de identificación de usuario único (IdX) en el sistema,

caracterizándose el procedimiento **por** la etapa de:

crear una distribución uniforme de los usuarios (1) entre los recursos (3), en el que la distribución se consigue utilizando una función hash (4), en el que la uniformidad de la distribución se crea utilizando un medio de aleatorización, en el que el medio de aleatorización (5) se materializa en un algoritmo de cifrado en el que una entrada da por resultado cualquier salida dentro de un intervalo de salidas de cifrado, teniendo la misma probabilidad de adquirir cualquier valor dentro del intervalo de salidas de cifrado cada vez que se cifra la entrada.

10. Un procedimiento según la reivindicación 9, **caracterizado porque** el algoritmo de cifrado (5) cifra un código o número de identificación de usuario único (IdX) y envía la salida de cifrado (6) a la función hash (4).

11. Un procedimiento según la reivindicación 10, **caracterizado porque** la salida de la función hash (8) está vinculada a un determinado recurso (3').

12. Un procedimiento según la reivindicación 9, **caracterizado porque** la función hash (4) es alimentada en su entrada con el código o número de identificación de usuario único (IdX) y envía la salida de la función hash (8) al algoritmo de cifrado (5).

13. Un procedimiento según la reivindicación 12, **caracterizado porque** la salida de cifrado (6) está vinculada a un determinado recurso (3').

14. Un procedimiento según la reivindicación 9, **caracterizado porque** el algoritmo de cifrado forma parte de la función hash, función hash que constituye así lo que se denomina una función hash por clave (10).

15. Un procedimiento según una cualquiera de las reivindicaciones precedentes 9 a 14, **caracterizado porque** los usuarios (1) son piezas de equipo móvil manejadas por propietarios de equipo móvil y porque el sistema (2) es un nodo del sistema de equipo móvil, y en el que los recursos (3) son servicios proporcionados en el nodo del

sistema de equipo móvil.

16. Un procedimiento según una cualquiera de las reivindicaciones 9 a 14, **caracterizado porque** los usuarios (1) son ordenadores, en el que el sistema (2) es una red de ordenadores y en el que los recursos (3) son recursos de sistema informático hacia los que son dirigidos los ordenadores.

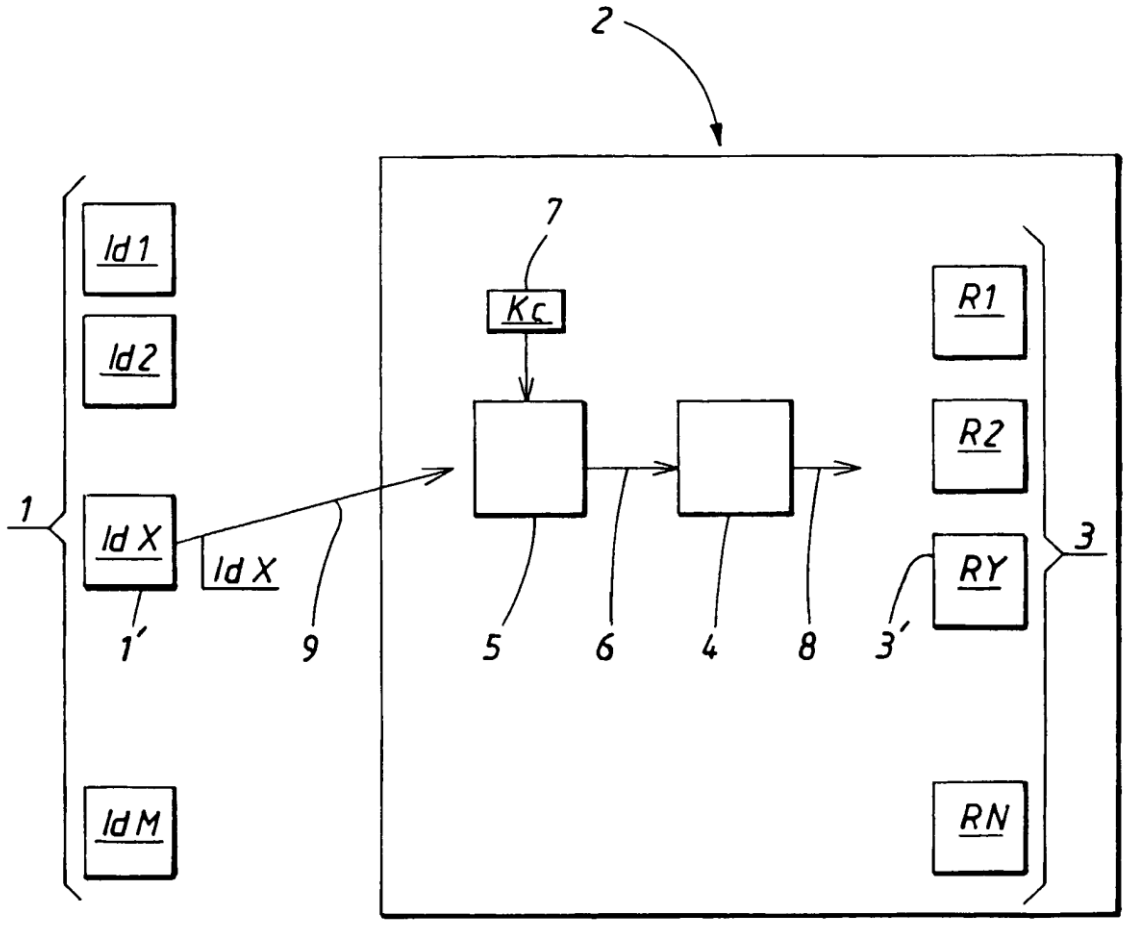

FIG.1

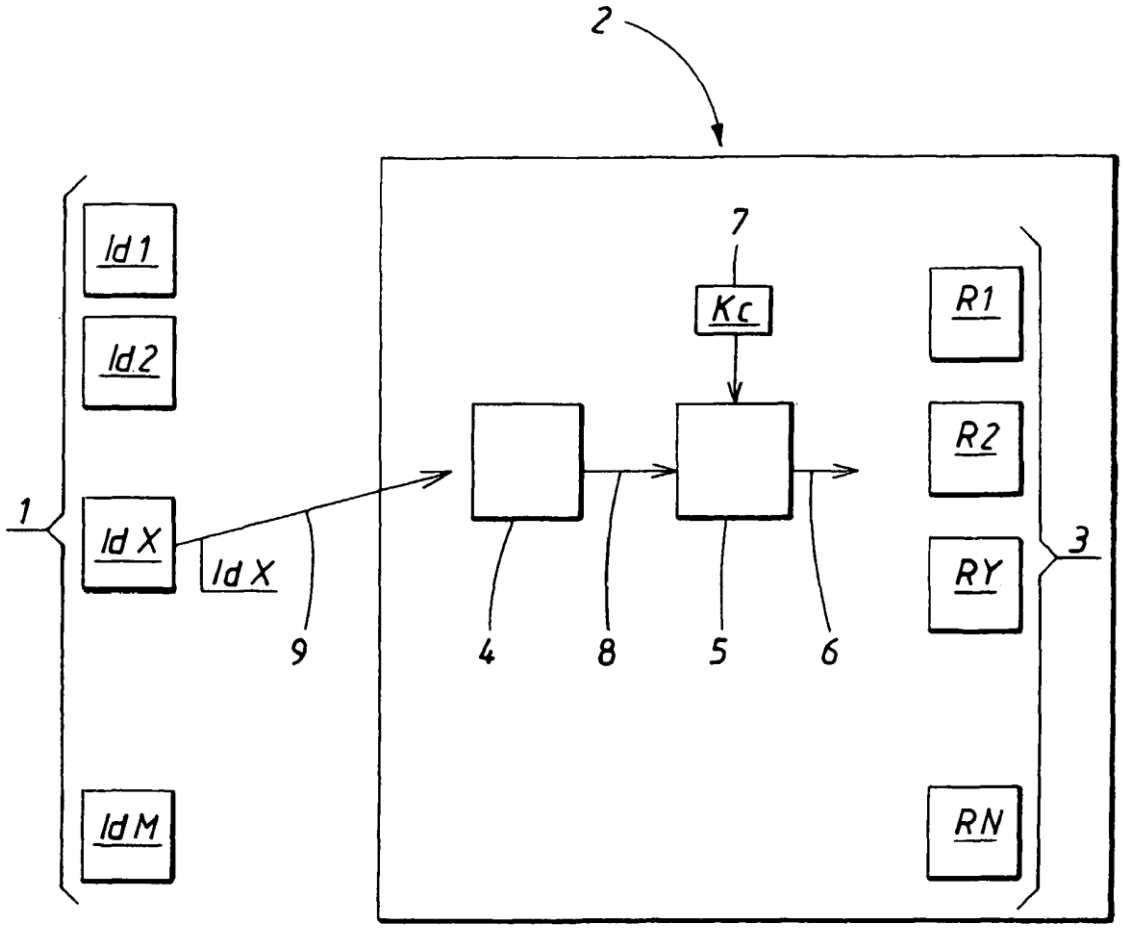

FIG. 2

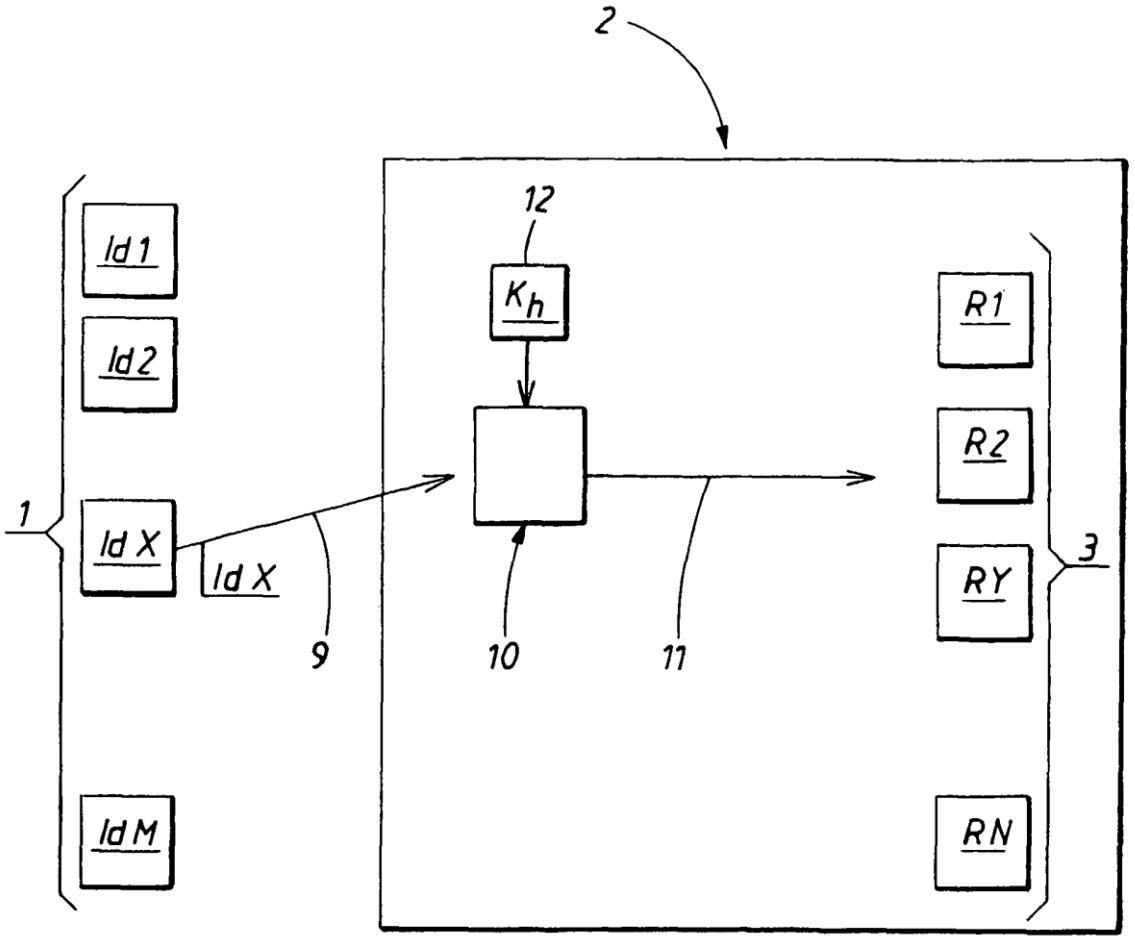

FIG. 3