(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 365 595**

(51) Int. Cl.:
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **99969168 .6**
(96) Fecha de presentación : **07.09.1999**
(97) Número de publicación de la solicitud: **1110185**
(97) Fecha de publicación de la solicitud: **27.06.2001**

(54) Título: **Soporte de datos de acceso protegido.**

(30) Prioridad: **11.09.1998 DE 198 41 676**

(45) Fecha de publicación de la mención BOPI:
07.10.2011

(45) Fecha de la publicación del folleto de la patente:
07.10.2011

(73) Titular/es: **Giesecke & Devrient GmbH**
Prinzregentenstrasse 159
81677 München, DE

(72) Inventor/es: **Vater, Harald y**
Drexler, Hermann

(74) Agente: **Arpe Fernández, Manuel**

DESCRIPCIÓN

Soporte de datos de acceso protegido

La invención se refiere a un soporte de datos, que tiene un chip semiconductor, en el que están almacenados datos secretos. En particular, la invención se refiere a una tarjeta chip.

Los soportes de datos que contienen un chip se emplean en un gran número de aplicaciones diferentes, por ejemplo para realizar transacciones financieras, para pagar artículos o prestaciones de servicios o como medio de identificación para el mando de controles de acceso o de entrada. En todas estas aplicaciones se procesan dentro del chip del soporte de datos por regla general datos secretos que deben protegerse contra el acceso por parte de terceras personas no autorizadas. Esta protección está garantizada, entre otras cosas, gracias a que las estructuras internas del chip presentan dimensiones muy pequeñas y, por lo tanto, el acceso a estas estructuras con el fin de espiar datos procesados en las mismas resulta muy difícil. Para hacer aun más difícil el acceso, el chip puede embutirse en una masa con una adherencia muy grande, que si se retira de manera forzada hace que se destruya la plaquita semiconductora o al menos los datos secretos almacenados en la misma. También es posible dotar a la plaquita semiconductora ya en su fabricación de una capa protectora que no pueda eliminarse sin destruir la plaquita semiconductora.

Con un equipo técnico correspondiente, que, si bien es sumamente caro, en principio se encuentra disponible, un atacante podría lograr liberar y examinar la estructura interna del chip. La liberación podría realizarse, por ejemplo, mediante procedimientos especiales de corrosión o mediante un proceso de abrasión adecuado. Las estructuras del chip así liberadas, como por ejemplo circuitos impresos, podrían contactarse con microsondas o examinarse con otros procedimientos para determinar el curso de la señal en estas estructuras. A continuación podrían intentarse averiguar, a partir de las señales detectadas, datos secretos del soporte de datos, como por ejemplo claves secretas, para emplearlos con fines de manipulación. También podría intentarse influir selectivamente mediante las microsondas en el curso de la señal de las estructuras liberadas.

La invención tiene el objetivo de proteger contra un acceso no autorizado los datos secretos existentes en el chip de un soporte de datos.

Este objetivo se logra mediante las combinaciones de características de las reivindicaciones 1 y 9.

Al contrario que el estado actual de la técnica, la solución según la invención no se centra en impedir una liberación de las estructuras internas del chip y una aplicación de microsondas. En lugar de esto, se toman medidas que dificultan a un atacante potencial llegar a conclusiones sobre información secreta a partir del curso de la señal en caso dado interceptados. Estas medidas consisten según la invención en manipular operaciones relevantes para la seguridad de tal manera que los datos secretos utilizados en la realización de estas operaciones relevantes para la seguridad no puedan averiguarse sin añadir otras informaciones confidenciales. Para ello se enmascaran o se adulteran las operaciones relevantes para la seguridad antes de su ejecución con ayuda de funciones adecuadas. Con el fin de dificultar o hacer incluso imposible en particular una evaluación estadística en caso de ejecutarse repetidas veces las operaciones relevantes para la seguridad, se incluye en la función de enmascaramiento un componente aleatorio. Por la solicitud de patente GB 2285562 A se conoce un procedimiento de codificación en el que, por medio de permutaciones y tablas de sustitución, se convierte un texto abierto en un texto codificado. Para la defensa frente a ataques de criptoanálisis se propone incluir en los cálculos durante la codificación números aleatorios generados por un generador de números pseudo-aleatorios, con el fin de impedir que pueda deducirse la clave en caso de efectuarse repetidas veces una codificación de textos claros que se diferencien sólo ligeramente unos de otros.

La consecuencia de ello es que un atacante no puede averiguar los datos secretos a partir de los trenes de datos en caso dado interceptadas.

En lo que sigue, la operación relevante para la seguridad está representada por la función h, que representa datos de entrada x en función de datos de salida y, es decir $y = h(x)$. Para impedir que los datos de entrada secretos x puedan ser espiados, según la invención se determina una función enmascarada h_{R1R2}, de modo que se aplica

$$y \otimes R_2 = h_{R1R2}\,(x \otimes R_1).$$

Ahora, la operación relevante para la seguridad se ejecuta por medio de la función enmascarada h_{R1R2}, cuyos datos de entrada no son los datos secretos reales x, sino datos secretos enmascarados $x \otimes R_1$, que han sido generados combinando los datos secretos reales x con un número aleatorio R_1. Sin conocer el número aleatorio R_1 no es posible averiguar los datos secretos reales x a partir de los datos secretos enmascarados $x \otimes R_1$. Como resultado de aplicar la función enmascarada h_{R1R2} a los datos secretos enmascarados $x \otimes R_1$ se obtienen datos de salida enmascarados $y \otimes R_2$. A partir de los datos de salida enmascarados $y \otimes R_2$ pueden averiguarse mediante una combinación adecuada los datos de salida y. Cada vez que se ejecute de nuevo la función relevante para la seguridad pueden preestablecerse antes nuevos números aleatorios R_1 y R_2, a partir de los cuales se determine

respectivamente una nueva función enmascarada h_{R1R2}. Como alternativa pueden estar almacenadas de manera permanente varias funciones enmascaradas h_{R1R2}, de las cuales se seleccione una aleatoriamente de manera respectiva antes de ejecutar la operación relevante para la seguridad. Al mismo tiempo resulta particularmente ventajoso utilizar dos funciones h_{R1R2} y $h_{R1'R2'}$, en las que los números aleatorios R'_1 y R'_2 sean los valores inversos de los números aleatorios R_1 y R_2 en relación con el tipo de combinación elegido para el enmascaramiento. En otra variante, los números aleatorios R_1 y R_2 pueden también ser iguales. Los números aleatorios R_1 y R_2 pueden seleccionarse en particular de forma estadísticamente independiente, de modo que no exista ninguna correlación entre los datos de entrada y salida que pueda utilizarse para un ataque.

Si se procesan adicionalmente otras operaciones antes o después de la operación relevante para la seguridad *h* aquí contemplada, los números aleatorios R_1 y R_2 pueden utilizarse también para el enmascaramiento de los datos procesados con las restantes operaciones.

La solución según la invención puede emplearse de forma particularmente ventajosa en operaciones relevantes para la seguridad que contengan funciones no lineales. En el caso de funciones no lineales no es posible aplicar medidas de protección ya conocidas basadas en un enmascaramiento de los datos secretos antes de ejecutar las funciones. Las medidas de protección ya conocidas presuponen que las funciones son lineales en lo relativo a las operaciones de enmascaramiento, para que el enmascaramiento pueda anularse de nuevo tras la ejecución de las funciones. Sin embargo, en la solución según la invención no se adulteran o se enmascaran sólo los datos secretos, sino también las operaciones relevantes para la seguridad que procesan los datos secretos. El enmascaramiento de los datos secretos y el enmascaramiento de las operaciones relevantes para la seguridad están mutuamente adaptados de modo que a partir de los datos secretos enmascarados puedan deducirse los datos secretos reales después de ejecutar las operaciones relevantes para la seguridad. La adaptación entre el enmascaramiento de los datos secretos y el enmascaramiento de las operaciones relevantes para la seguridad puede realizarse de un modo particularmente sencillo si las operaciones relevantes para la seguridad están realizadas en forma de tablas, así llamadas *Tablas de consulta* (Look-up tables). En las mencionadas tablas, cada valor de entrada *x* tiene asignado un valor de salida *y*. La ejecución de las funciones realizadas a través de las tablas se efectúa buscando los valores de salida *y* correspondientes a los valores de entrada *x* en cuestión.

A continuación se explica la invención por medio de las formas de realización representadas en las figuras, que muestran:

- figura 1, una vista en planta de una tarjeta chip,

- figura 2, una vista en planta de un detalle muy ampliado del chip de la tarjeta chip representada en la figura 1,

- figuras 3a, 3b, 3c y 3d representaciones de *Tablas de consulta*.

En la figura 1 está representada una tarjeta chip 1 a modo de un ejemplo del soporte de datos. La tarjeta chip 1 se compone de un cuerpo de tarjeta 2 y un módulo de chip 3, que está encajado en una escotadura del cuerpo de tarjeta 2 prevista para este fin. Los componentes esenciales del módulo de chip 3 son unas superficies de contacto 4, que permiten establecer una conexión eléctrica con un aparato externo, y un chip 5, que está conectado eléctricamente a las superficies de contacto 4. Como alternativa o adicionalmente a las superficies de contacto 4 puede estar prevista también una bobina, no representada en la figura 1, u otro medio de transmisión para el establecimiento de un enlace de comunicación entre el chip 5 y un aparato externo.

En la figura 2 está representada una vista en planta de un detalle muy ampliado del chip 5 de la figura 1. Lo especial de la figura 2 consiste en que se representa la superficie activa del chip 5, es decir que en la figura 2 no está representada ninguna de las capas que por lo general protegen la capa activa del chip 5. Para obtener información sobre el curso de la señal dentro del chip pueden por ejemplo contactarse con microsondas las estructuras liberadas 6. En el caso de las microsondas se trata de unas agujas muy finas que, mediante un posicionador de precisión, se ponen en contacto eléctrico con las estructuras liberadas 6, por ejemplo circuitos impresos. El curso de la señal registrado con las microsondas se procesan posteriormente con dispositivos de medición y evaluación adecuados con el fin de poder sacar conclusiones sobre datos secretos del chip.

Con la invención se consigue que, aunque un atacante logre eliminar la capa protectora del chip 5 sin destruir el circuito y contactar con microsondas las estructuras liberadas 6 del chip 5 o intervenirlas de otro modo, le resulte muy difícil o incluso imposible acceder a, especialmente, datos secretos del chip. Por supuesto, la invención interviene también si un atacante consigue acceder de otro modo al curso de la señal del chip 5.

Las figuras 3a, 3b, 3c y 3d muestran ejemplos sencillos de *Tablas de consulta*, en las que tanto los datos de entrada como los de salida tienen en cada caso una longitud de 2 bits. Todos los valores de la tabla están representados como datos binarios. En la primera fila están representados en cada caso los datos de entrada *x* y en la segunda fila los datos de salida *y* respectivamente asignados por columnas.

En la figura 3a está representada una *Tabla de consulta* para la función *h* sin enmascarar. De la figura 3a se desprende que el valor de entrada $x = 00$ tiene asignado el valor de salida $h(x) = 01$, el valor de entrada 01 tiene asignado el valor de salida 11, el valor de entrada 10 tiene asignado el valor de salida 10 y el valor de entrada 11

tiene asignado el valor de salida 00. La *Tabla de consulta* según la figura 3a representa una función *h* no lineal que ha de ejecutarse en el marco de una operación relevante para la seguridad. Sin embargo, en el marco de la invención no se utiliza para la ejecución de la operación relevante para la seguridad la *Tabla de consulta* representada en la figura 3a, sino que a partir de esta *Tabla de consulta* se deriva una *Tabla de consulta* enmascarada según las figuras 3b, 3c y 3d.

En la figura 3b está representado un paso intermedio de la determinación de la *Tabla de consulta* enmascarada. La *Tabla de consulta* según la figura 3b se generó a partir de la *Tabla de consulta* según la figura 3a, combinando cada valor de la primera fila de la tabla de la figura 3a de forma O exclusiva con el número aleatorio R_1 = 11. Así, la combinación O exclusiva del valor 00 de la primera fila y primera columna de la tabla de la figura 3a con el número 11 da como resultado el valor 11, que ahora constituye el elemento de la primera fila y primera columna de la tabla de la figura 3b. Los demás valores de la primera fila de la tabla representada en la figura 3b se determinan análogamente a partir de los valores de la primera fila de la tabla representada en la figura 3a y el número aleatorio R_1 = 11. La tabla representada en la figura 3b podría emplearse ya como *Tabla de consulta* enmascarada para el procesamiento de datos secretos también enmascarados con el número aleatorio R_1 = 11. El resultado serían entonces respectivamente los valores de texto abierto que pueden leerse en la fila 2 de la tabla de la figura 3b.

Normalmente, las distintas columnas de una *Tabla de consulta* se ordenan por datos de entrada *x* ascendentes. En la figura 3c está representada una tabla determinada mediante un cambio de orden correspondiente de la tabla de la figura 3b.

Si se desea enmascarar aun más la tabla según la figura 3c o ésta no debe proporcionar valores de texto abierto como valores de salida sino valores también enmascarados, se aplica una operación O exclusiva adicional con un número aleatorio R_2 adicional.

En la figura 3d está representado el resultado de la aplicación de esta operación O exclusiva adicional. En esta operación se combinan respectivamente los elementos de la segunda fila de la tabla según la figura 3c de forma O exclusiva con el número aleatorio R_2 = 10. El elemento de la segunda fila y primera columna de la tabla según la figura 3d se produce por lo tanto mediante una combinación O exclusiva del elemento de la segunda fila y primera columna de la tabla según la figura 3c con el número aleatorio R_2 = 10. Los demás elementos de la segunda fila de la tabla según la figura 3d se forman análogamente. La primera fila de la tabla según la figura 3d se toma sin cambios de la figura 3c.

Con la tabla representada en la figura 3d pueden determinarse, a partir de datos de entrada enmascarados, datos de salida también enmascarados. Los datos de salida enmascarados así determinados pueden utilizarse en otras operaciones con las que hayan de procesarse datos enmascarados o a partir de los mismos pueden determinarse datos de texto abierto mediante una combinación O exclusiva con el número aleatorio R_2 = 10.

Utilizando la tabla representada en la figura 3d es posible ejecutar también operaciones no lineales con datos secretos enmascarados y proteger estos datos secretos contra un acceso no autorizado. Además, también se protegen las operaciones relevantes para la seguridad mismas contra un acceso no autorizado, ya que en cada ejecución de las operaciones pueden emplearse funciones enmascaradas de distinta forma, e incluso si fuera posible determinar las funciones enmascaradas no podrían deducirse las operaciones relevantes para la seguridad mismas. Sin embargo, tras una conversión a texto abierto, tanto las operaciones relevantes para la seguridad original como las operaciones ejecutadas por medio de funciones enmascaradas dan resultados idénticos. Así, por ejemplo, un valor de entrada 00 según la tabla de la figura 3a da como resultado un valor de salida 01. Para comprobar si la tabla enmascarada representada en la figura 3d da el mismo valor de salida debe combinarse en primer lugar el valor de entrada 00 de forma O exclusiva con el número aleatorio R_1 = 11. Como resultado de esta combinación se obtiene el valor 11. Según la tabla de la figura 3d, un valor de entrada 11 da como resultado un valor de salida de también 11. Para determinar el texto abierto a partir de este valor de salida debe combinarse el valor de salida de forma O exclusiva con el número aleatorio R_2 = 10. Como resultado de esta combinación se obtiene el valor 01, que coincide exactamente con el valor determinado por medio de la tabla representada en la figura 3a.

El enmascaramiento de las operaciones relevantes para la seguridad o de los valores de entrada puede producirse no sólo mediante una combinación O exclusiva, sino también por medio de otros tipos de combinación adecuados, por ejemplo mediante una adición modular. Además, la invención no está limitada a la aplicación de funciones no lineales representadas mediante las *Tablas de consulta*. Más bien pueden emplearse cualesquiera funciones no lineales y también lineales para las que sea posible determinar una función enmascarada adecuada.

REIVINDICACIONES

1. Soporte de datos con un chip semiconductor (5) que tiene al menos una memoria en la que está almacenado un programa operativo que es capaz de ejecutar al menos una operación (*h*), requiriéndose para ejecutar dicha operación (*h*) datos de entrada (*x*) y generándose al ejecutar la operación (*h*) datos de salida (*y*), **caracterizado porque**

- la operación (*h*) se enmascara antes de su ejecución,

- la operación enmascarada (h_{R1}) se ejecuta con datos de entrada enmascarados ($x \otimes R_1$) y

- el enmascaramiento de la operación (*h*) y el enmascaramiento de los datos de entrada (*x*) están mutuamente adaptados de modo que la ejecución de la operación enmascarada (h_{R1}) con datos de entrada enmascarados ($x \otimes R_1$) da como resultado datos de salida (*y*) idénticos a los datos de salida (*y*) determinados en la ejecución de la operación sin enmascarar (*h*) con datos de entrada sin enmascarar (*x*).

2. Soporte de datos según la reivindicación 1, **caracterizado porque** en la determinación de la operación enmascarada (h_{R1}) y de los datos de entrada enmascarados ($x \otimes R_1$) entra en juego al menos un número aleatorio (R_1).

3. Soporte de datos según una de las reivindicaciones anteriores, **caracterizado porque** la determinación de la operación enmascarada (h_{R1}) y de los datos de entrada enmascarados ($x \otimes R_1$) se realiza por medio de combinaciones O exclusiva.

4. Soporte de datos según una de las reivindicaciones anteriores, **caracterizado porque** la operación enmascarada (h_{R1}) se almacena previamente de manera permanente en el soporte de datos.

5. Soporte de datos según la reivindicación 4, **caracterizado porque** en el soporte de datos se almacenan previamente de manera permanente al menos dos operaciones enmascaradas (h_{R1}, h_{R1}') y entonces, cuando debe ejecutarse una operación enmascarada, se selecciona aleatoriamente una de las operaciones enmascaradas (h_{R1}, h_{R1}') almacenadas.

6. Soporte de datos según una de las reivindicaciones 1 a 3, **caracterizado porque** la operación enmascarada (h_{R1}) es respectivamente calculada de nuevo antes de su ejecución y para este cálculo se determina de nuevo el, al menos, un número aleatorio (R_1).

7. Soporte de datos según una de las reivindicaciones anteriores, **caracterizado porque** la operación (*h*) se realiza mediante una tabla que está almacenada en el soporte de datos y que establece una correspondencia entre los datos de entrada (*x*) y los datos de salida (*y*).

8. Soporte de datos según la reivindicación 7, **caracterizado porque** el enmascaramiento de los datos de entrada (*x*) contenidos en la tabla se realiza mediante una combinación con el al menos un número aleatorio (R_1).

9. Soporte de datos con un chip semiconductor (5) que tiene al menos una memoria en la que está almacenado un programa operativo que es capaz de ejecutar al menos una operación (*h*), requiriéndose para ejecutar dicha operación (*h*) datos de entrada (*x*) y generándose al ejecutar la operación (*h*) datos de salida (*y*), **caracterizado porque**

- la operación (*h*) se enmascara antes de su ejecución,

- la operación enmascarada (h_{R1}) se ejecuta con datos de entrada enmascarados ($x \otimes R_1$),

- el enmascaramiento de la operación (*h*) y el enmascaramiento de los datos de entrada (*x*) están mutuamente adaptados de modo que la ejecución de la operación enmascarada (h_{R1R2}) con datos de entrada enmascarados ($x \otimes R_1$) da como resultado datos de salida ($y \otimes R_2$) que están enmascarados respecto de los datos de salida (*y*) determinados en la ejecución de la operación sin enmascarar (*h*) con datos de entrada sin enmascarar (*x*) y

- a partir de los datos de salida enmascarados ($y \otimes R_2$), por medio de datos (R_2) utilizados para el enmascaramiento de la operación (*h*), pueden determinarse los datos de salida sin enmascarar (*y*).

10. Soporte de datos según la reivindicación 9, **caracterizado porque** en la determinación de los datos de entrada enmascarados ($x \otimes R_1$) entran en juego al menos un número aleatorio (R_1) y porque en la determinación de las operaciones enmascaradas (h_{R1R2}) entran al menos dos números aleatorios (R_1, R_2).

11. Soporte de datos según una de las reivindicaciones 9 ó 10, **caracterizado porque** la determinación de la operación enmascarada (h_{R1R2}) y de los datos de entrada enmascarados ($x \otimes R_1$) se realiza por medio de combinaciones O exclusiva.

12. Soporte de datos según una de las reivindicaciones 9 a 11, **caracterizado porque** la operación enmascarada (h_{R1R2}) se almacena previamente de manera permanente en el soporte de datos.

13. Soporte de datos según la reivindicación 12, **caracterizado porque** en el soporte de datos se almacenan previamente de manera permanente al menos dos operaciones enmascaradas (h_{R1R2}, $h_{R1'R2'}$) y entonces, cuando debe ejecutarse una operación enmascarada, se selecciona aleatoriamente una de las operaciones enmascaradas (h_{R1R2}, $h_{R1'R2'}$) almacenadas.

14. Soporte de datos según la reivindicación 13, **caracterizado porque** los números aleatorios (R_1, R_2) con los que se determina la primera operación enmascarada (h_{R1R2}) son, respecto de la combinación que se utiliza para determinar las operaciones enmascaradas (h_{R1R2}, $h_{R1'R2'}$), inversos respecto de los números aleatorios (R_1', R_2') con los que se determina la segunda operación enmascarada ($h_{R1'R2'}$).

15. Soporte de datos según una de las reivindicaciones 9 a 11, **caracterizado porque** la operación enmascarada (h_{R1R2}) es respectivamente calculada de nuevo antes de su ejecución y para este cálculo se determinan de nuevo los números aleatorios (R_1, R_2).

16. Soporte de datos según una de las reivindicaciones 9 a 15, **caracterizado porque** la operación (h) se realiza mediante una tabla que está almacenada en el soporte de datos y que establece una correspondencia entre los datos de entrada (x) y los datos de salida (y).

17. Soporte de datos según la reivindicación 16, **caracterizado porque** el enmascaramiento de los datos de entrada (x) contenidos en la tabla se realiza mediante una combinación con el al menos un número aleatorio (R_1) y el enmascaramiento de los datos de salida (y) contenidos en la tabla se realiza mediante una combinación con el al menos un número aleatorio adicional (R_2).

18. Soporte de datos según una de las reivindicaciones anteriores, **caracterizado porque** en el caso de la operación (h) se trata de una operación no lineal respecto de la combinación empleada para el enmascaramiento de la operación (h).

FIG.1

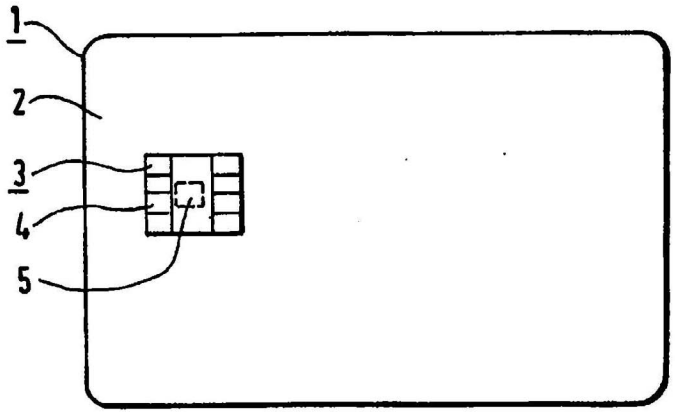

FIG.2

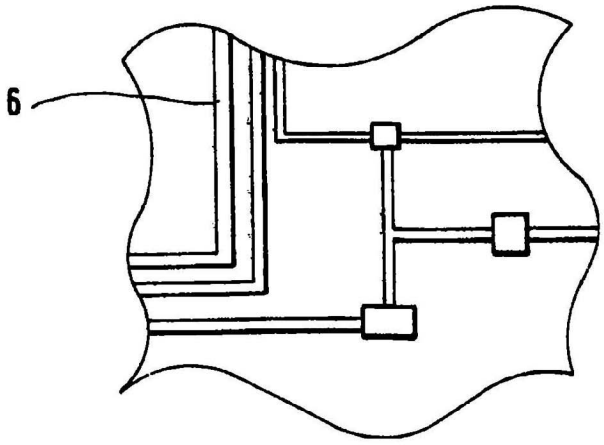

FIG. 3A

x	00	01	10	11
h(x)	01	11	10	00

FIG. 3B

x	11	10	01	00
$h_{R1}(x)$	01	11	10	00

FIG. 3C

x	00	01	10	11
$h_{R1}(x)$	00	10	11	01

FIG. 3D

x	00	01	10	11
$h_{R1\,R2}(x)$	10	00	01	11

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

La lista de referencias citada por el solicitante lo es solamente para utilidad del lector, no formando parte de los documentos de patente europeos. Aún cuando las referencias han sido cuidadosamente recopiladas, no pueden excluirse errores u omisiones y la OEP rechaza toda responsabilidad a este respecto.

Documentos de patente citados en la descripción

• GB 2285562 A **[0006]**