(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 528 717**

(51) Int. CI.:

H04N 21/418 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.10.2005 E 05292094 (9)**

(97) Fecha y número de publicación de la concesión europea: **03.12.2014 EP 1773055**

(54) Título: **Método de verificación de derechos contenidos en un módulo de seguridad**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.02.2015

(73) Titular/es:

NAGRA FRANCE SAS (100.0%)
86, rue Henri Farman
92130 Issy-les-Moulineaux, FR

(72) Inventor/es:

LE FLOCH, DOMINIQUE y
MAILLARD, MICHEL

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método de verificación de derechos contenidos en un módulo de seguridad

Dominio de la invención

[0001] La presente invención se refiere al dominio de los módulos de seguridad utilizados como dispositivo de protección y de personalización de diverso aparatos electrónicos, como los descodificadores de televisión de pago, los ordenadores personales, los equipos móviles etcétera.

[0002] Un módulo de seguridad es un dispositivo reputado inviolable que contiene diversas claves de codificación/desencriptación así como datos propios de un usuario que definen los derechos que tiene adquirido para la explotación de datos. El módulo de seguridad puede encontrarse bajo diferentes formas tales como una tarjeta inteligente insertada en un lector, un circuito integrado soldado a una tarjeta madre, una tarjeta del tipo tarjeta SIM que se encuentra en telefonía móvil, etcétera.

Antecedentes de la técnica

[0003] Los módulos de seguridad de los descodificadores de televisión de pago por ejemplo contienen claves de codificación/desencriptación por decodificar un flujo de datos de audio/vídeo que entra en el descodificador. Para obtener los datos en abierto, terceros, más comúnmente denominados "hackers", han recurrido a diversos métodos fraudulentos tales como los ataques materiales o de software (*hardware*, *software attacks*). Estos ataques están dirigidos de una forma más particular a los datos contenidos en la memoria del módulo de seguridad que el "hacker" intenta modificar para atribuirse los derechos de forma indebida.

[0004] Un derecho se presenta habitualmente en forma de control, de mensaje o de instrucción acompañada de parámetros o en forma de clave que permita liberar un acceso a datos de audio/vídeo emitido, por ejemplo. Tal derecho autoriza, entre otro, bien el acceso a un canal o a un conjunto de canales de difusión particulares, bien a un programa durante un período predeterminado, o incluso a un tipo específico de programa adquirido después de un pago en línea.

[0005] Un ataque habitual consiste en perturbar la ejecución, por el procesador del módulo de seguridad, del código de la máquina del programa informático (*glitch attack*). Por ejemplo, el "hacker" analiza las señales generadas por las instrucciones del procesador y cuando una instrucción de comparación o de salto se ejecuta, aplica una perturbación externa rápida o aumenta la frecuencia de la señal de reloj. Las instrucciones se bloquean de este modo temporalmente y una autentificación de datos sensibles se puede eludir.

[0006] En el dominio de la televisión de pago, el módulo de seguridad asociado al descodificador recibe y almacena los derechos procedentes de mensajes de administración EMM (*Entitlement Management Message*) transmitidos por el centro de gestión de un operador. Estos derechos autorizan la desencriptación y la visualización de programas televisados que el abonado ha adquirido. Otros tipos de ataques consisten en crear mensajes de administración EMM artificiales o utilizar una brecha de seguridad. Una defensa contra el reemplazo abusivo del contenido de la memoria relacionada con los derechos consiste en calcular una huella o un "*checksum*" de este contenido con ayuda de una función matemática unidireccional. Una comparación con una huella de referencia permite distinguir un contenido modificado de un contenido auténtico.

[0007] Cuando un mensaje EMM artificial ha sido aceptado por el módulo de seguridad, esta defensa es inútil. En el caso de que esta brecha de seguridad haya sido rellenada por un programa correctivo, la huella calculada localmente será correcta, pero no se corresponderá necesariamente con una huella calculada sobre los derechos registrados en el centro de gestión. Para completar la verificación, un mensaje que requiere la comparación de la huella local con la huella distante del centro de gestión se transmite por cada módulo de seguridad a dicho centro. Este envío de mensajes representa un inconveniente mayor porque por una parte el enlace del descodificador equipado con el módulo de seguridad con el centro de gestión se puede congestionar y por otra parte el centro en sí requerido para verificar las huellas después de cada envío de mensajes EMM se puede sobrecargar.

[0008] El documento WO2004/008765 describe un descodificador asociado a un módulo de seguridad que consta de una memoria para almacenar una pluralidad de claves de autorización e informaciones de derechos que autorizan la desencriptación de las contraseñas de control. Estas informaciones de derechos determinan el momento y las condiciones bajo las que el módulo de seguridad proporciona al descodificador una contraseña de control previamente desencriptada por una clave de autorización. Un detector de fuente determina la fuente del flujo de datos transmitido al descodificador y recibe los mensajes ECM. En respuesta, el detector transmite los comandos al módulo de seguridad para descodificar una o más contraseñas de control contenidas en el mensaje ECM. Los comandos sirven para seleccionar la clave de autorización y las informaciones de derechos que se tienen que utilizar para descodificar una contraseña de control en función de la fuente del mensaje ECM, tal como un flujo difundido en directo o una unidad de almacenamiento. El uso conjugado de una clave de autorización y de una información de derechos específicos permite impedir la manipulación del sistema descodificador /módulo de seguridad utilizando una clave sin conexión con el mensaje ECM recibido y las informaciones de derechos correspondientes.

Breve descripción de la invención

[0009] El objetivo de la presente invención es minimizar el número de mensajes intercambiados entre el módulo de seguridad y el centro de gestión así como el número de operaciones de verificación efectuadas por este último. Otro objetivo es aportar una contramedida eficaz contra los ataques de "hackers" que aprovechan una brecha provisional de la seguridad para modificar los derechos almacenados en el módulo de seguridad.

[0010] Estos objetivos se alcanzan por un método de verificación de derechos contenidos en un módulo de seguridad asociado a un aparato de tratamiento de datos numéricos difundidos, según la reivindicación 1.

[0011] El mensaje de actualización transmitido por el centro de gestión incluye al menos un derecho y un medio de verificación tal como una huella calculada en este derecho con, por ejemplo, una función unidireccional y sin colisión del tipo "Hash". Este mensaje está encriptado con una clave bien única propia del módulo de seguridad del aparato, bien común para un grupo de módulos de seguridad. Este último contiene los derechos que se almacenan en una memoria de derechos según el estado de la técnica anterior.

[0012] Cada mensaje que actualiza la memoria de los derechos se almacena en una memoria de mensajes, este mensaje se puede almacenar en su totalidad o solamente la parte útil obtenida después de la extracción de los encabezados, el número del módulo de seguridad, etc. Esta parte de mensaje permanece protegida, bien en forma encriptada o firmada, es decir, acompañada de una huella encriptada.

[0013] El mensaje de actualización de un derecho recibido del centro de gestión se desencripta con la clave de transporte de dicho mensaje que puede ser una clave global o una clave propia del módulo de seguridad. Luego, se realiza una verificación con ayuda de la huella o firma que acompaña al derecho. Ésta se compara con una huella determinada por el módulo de seguridad y cuando el resultado de la comparación es positivo, el mensaje se almacena en la memoria de los mensajes y el derecho correspondiente almacenado en la memoria de los derechos se actualiza.

[0014] Otra manera de verificar el derecho recibido es extraer de la huella recibida el valor del derecho y comparar este derecho calculado con el derecho contenido en el mensaje. Esto se puede realizar mediante una huella determinada por la encriptación del derecho. La posesión de la mismo clave (clave simétrica) o de la clave correspondiente (clave asimétrica) permite tal extracción.

[0015] En el momento de la verificación posterior, un derecho almacenado en la memoria de los derechos se identifica antes y el mensaje correspondiente que ha provocado el almacenamiento de dicho derecho se busca en la memoria de los mensajes. Este mensaje de derecho se verifica con ayuda de su huella. Si este mensaje se ha almacenado de forma encriptada, se desencripta previamente con la clave de transporte o la clave única del módulo de seguridad.

[0016] En caso de que la verificación tenga éxito, el derecho extraído del mensaje se compara con el derecho correspondiente almacenado.

[0017] Esta verificación posterior llamada re-ejecución del mensaje de derecho se puede efectuar a la conexión del aparato, a la recepción de un mensaje de control ECM o de un mensaje de administración EMM, o periódicamente a intervalos predefinidos. Cuando el resultado de la comparación es negativo, el aparato funciona en un modo por defecto con por ejemplo derechos de acceso a datos restringidos.

[0018] La presente invención propone un método de verificación de derechos contenidos en un módulo de seguridad asociado a un aparato de tratamiento de datos numéricos difundidos, dicho aparato está conectado a un centro de gestión que transmite mensajes encriptados de actualización de los derechos de acceso a dichos datos numéricos y mensajes de control que sirven para descodificar los datos difundidos, caracterizado por el hecho de que comprende las etapas siguientes:

- recepción y lectura por el módulo de seguridad de todo o parte de un mensaje de derecho que comprende al menos un derecho y medios de verificación de dicho derecho,

- desencriptación y verificación del mensaje de derecho y almacenamiento de todo o parte de dicho mensaje de derecho en una memoria de los mensajes,

- recepción de un mensaje de control que comprende al menos una contraseña de control que sirve para descodificar dichos datos y extracción de un derecho condicional de dicho mensaje, este derecho condicional define el o los derechos necesarios para el uso de la contraseña de control,

- búsqueda del mensaje de derecho almacenado correspondiente al derecho condicional previamente extraído y verificación de dicho mensaje,

- comparación del derecho contenido en el mensaje con el derecho condicional extraído del mensaje de control,

- determinación de un estado de error cuando el resultado de la comparación indique una diferencia.

[0019] Según la invención, la memoria de los derechos ya no es necesaria porque la verificación de los derechos se efectúa "en directo" en el momento de la recepción de un mensaje de control ECM. Este último comprende un derecho condicional que se compara, después de la búsqueda del mensaje correspondiente en la memoria de los mensajes, con el derecho obtenido después de la re-ejecución del mensaje hallado.

[0020] Según una forma de realización, el mensaje de derecho recibido, una vez desencriptado con la clave de transporte, se puede re-encriptar por una clave local antes de su almacenamiento en la memoria de los mensajes. Antes de verificar tal mensaje, será necesario descodificar con esta clave local.

Breve descripción de las figuras

[0021] La invención se comprenderá mejor gracias a la descripción detallada siguiente y que se refiere a las figuras anexas aportadas a modo de ejemplo en ningún caso limitativo.

- la figura 1 ilustra un organigrama que representa el método de verificación de los derechos según el estado de la técnica con una memoria de derechos que almacena derechos que se comparan con derechos correspondientes de los mensajes de derecho,

- la figura 2 ilustra un organigrama que representa el método de verificación de los derechos según la presente invención sin memoria de derechos comparando directamente un derecho de un mensaje ECM con un derecho de un mensaje de derecho.

Descripción detallada de la invención

[0022] El ejemplo descrito a continuación se refiere al dominio de la televisión digital de pago donde un descodificador (o set top box) que recibe un flujo de datos de audio-video está conectado a un centro de gestión. Este último transmite al descodificador, a través del flujo, mensajes (EMM) de administración o de derecho que contienen al menos un derecho (Dr) acompañados de su huella H(Dr).

[0023] Según nuestro ejemplo, vamos a considerar la actualización de un módulo de seguridad de una manera única, es decir, por el direccionamiento de un mensaje personal.

[0024] El conjunto compuesto por el derecho (Dr) y de su huella H(Dr) se encripta con una clave personal (Ku) única del módulo de seguridad asociado al descodificador. El mensaje (EMM) se encripta con una clave global (Kg), preferiblemente asimétrica. En este ejemplo, la huella H(Dr) se obtiene con ayuda de una función unidireccional y sin colisión del tipo Hash efectuada sobre el derecho (Dr).

[0025] El mensaje (EMM) o preferentemente una parte de éste puede entonces representarse en la forma {[Dr, H(Dr)]Ku}Kg. La clave global (Kg) es una clave pública correspondiente a una clave privada contenida en el módulo de seguridad que permite descodificar el mensaje EMM en su conjunto.

[0026] Con el fin de facilitar la comprensión de la presente invención, el esquema de la figura 1 ilustra un método según el estado de la técnica en el que el mensaje EMM o al menos la parte que contiene el derecho (Dr) y su huella H(Dr) se verifica primero (Ver EMM) antes de ser almacenado en la memoria de los mensajes (MM). El conjunto derecho-huella [Dr, H(Dr)]Ku se desencripta con la clave personal (Ku) del módulo de seguridad. Una huella H'(Dr) del derecho Dr es calculada por el módulo de seguridad con la función "Hash", luego se compara con la huella recibida H(Dr). Cuando la comparación tiene éxito, es decir cuando la huella calculada H'(Dr) y la huella recibida H(Dr) son idénticas, el mensaje (EMM) se almacena en la memoria de los mensajes (MM) y el derecho (Dr) correspondiente se actualiza en la memoria de los derechos (MD).

[0027] En el caso contrario de una verificación infructuosa, el mensaje EMM es rechazado (R) y no se efectuará ninguna actualización en la memoria (MD) de los derechos. Según las opciones del descodificador, tal rechazo (R) se puede señalar por un mensaje de error apropiado y si el número de rechazos (R) supera cierto umbral, el módulo de seguridad puede ser bloqueado.

[0028] El mensaje EMM que contiene el derecho (Dr) y su huella H(Dr) se almacena en la memoria de los mensajes (MM) preferiblemente después de la desencriptación con la clave global (Kg), es decir en la forma [Dr, H(Dr)]Ku.

[0029] En el momento de la etapa de verificación posterior, el derecho almacenado (Dr') en la memoria de los derechos (MD) se confronta con el mensaje (EMM) que ha generado este derecho o su actualización, el mensaje (EMM) es así re-ejecutado (Re-Exe EMM) y el derecho (Dr) obtenido se compara con el derecho (Dr') previamente almacenado. En una primera fase, el derecho (Dr) que se va a verificar se identifica por ejemplo sobre la base de los datos seleccionados en el flujo difundido entre los derechos que se almacenan en la memoria de los derechos (MD). El mensaje (EMM) de

derecho correspondiente se busca a continuación (S-Dr) en la memoria (MM) de los mensajes luego desencriptado con la clave (Ku) del módulo de seguridad y verificado con la huella H(Dr) que acompaña a este derecho. Esta verificación se desarrolla de la misma manera que la efectuada antes del almacenamiento del mensaje (EMM) y del derecho (Dr) después de la recepción. Cuando esta verificación se consigue, el derecho (Dr') almacenado en la memoria de los derechos (MD) se compara con su homólogo (Dr) extraído del mensaje (EMM) de derecho.

[0030] Si el derecho (Dr) re-ejecutado no corresponde con el derecho Dr' contenido en la memoria (MD) de los derechos (Dr=Dr' ?), el módulo de seguridad determina un estado de error (DEF) del descodificador que acarrea bien un funcionamiento con derechos restringidos, bien un bloqueo que necesita una intervención particular para su reanudación. Si los dos derechos se corresponden (Dr=Dr'), el módulo de seguridad del descodificador autoriza (OK) el acceso a los datos audio/vídeo según los derechos almacenados.

[0031] Este estado de error (DEF) se puede también determinar cuando la verificación del derecho (Dr) del mensaje (EMM) con su huella H(Dr) fracasa con una huella calculada H'(Dr) diferente de la extraída del mensaje (EMM).

[0032] Cuando la búsqueda (S-Dr) del mensaje (EMM) correspondiente a un derecho (Dr) previamente identificado en la memoria (MD) de los derechos no llega a ningún resultado (S-Dr KO), el módulo de seguridad puede también determinar un estado de error (DEF). Esta situación se presenta cuando un derecho (Dr) se ha introducido en la memoria (MD) por otros medios diferentes de los mensajes (EMM) de derecho, por ejemplo con ayuda de un software apropiado que se aprovecha de una brecha de seguridad que permite un acceso facilitado a la memoria (MD) de los derechos.

[0033] Según un ejemplo de aplicación, un bloqueo del módulo de seguridad necesita una solicitud de reparación en servicio al centro de gestión por otra vía de comunicación (fax, teléfono, correo, mensaje corto, etc.) distinta de la canal de retorno del descodificador. El módulo de seguridad puede también ser desbloqueado con una clave particular del tipo PUK (*Personal Unblocking Key*) que puede desbloquearlo a la manera de una tarjeta SIM (*Subscriber Identity Module*) de un teléfono móvil bloqueada debido a errores de código de arranque demasiado numerosos.

[0034] La verificación posterior puede efectuarse en diferentes momentos: por ejemplo, tiene lugar en el momento del arranque del descodificador, o después de la recepción de un mensaje de control (ECM), bien por control gracias a un mensaje de administración (EMM), o incluso durante un período determinado por un parámetro en el software del módulo de seguridad o del descodificador.

[0035] Según una variante, sola la huella H(Dr) encriptada con la clave (Ku) única del módulo de seguridad se puede almacenar en la memoria (MM) de los mensajes. En el momento de la verificación, la huella H(Dr) se descodifica y compara con una huella H'(Dr) calculada sobre el derecho correspondiente almacenado en la memoria (MD) de los derechos.

[0036] El esquema de la figura 2 ilustra el método según la presente invención en la que la memoria (MD) de los derechos ya no es necesaria porque la verificación se efectúa comparando directamente los derechos de los mensajes (EMM) almacenados con los derechos condicionales incluidos en mensajes de control (ECM) difundidos regularmente en el flujo de los datos audio/vídeo. Estos derechos son necesarios para el uso de la o las contraseñas de control incluidas en el mensaje de control (ECM) en el momento de la desencriptación de los datos audio/vídeo del flujo difundido.

[0037] Un mensaje (EMM) de derecho recibido, desencriptado con la clave global (Kg) luego verificado con la huella H(Dr) del derecho (Dr) se almacena en la memoria (MM) de los mensajes. Cuando la verificación fracasa, el mensaje (EMM) de derecho es rechazado (R) llevando a la señalización de un error o un bloqueo del módulo de seguridad.

[0038] Cuando se recibe un mensaje de control (ECM) que contiene un derecho condicional (Dc), una búsqueda (S-Dr) de un mensaje (EMM) de derechos correspondiente al derecho condicional (Dc) extraído del mensaje ECM se efectúa en la memoria de los mensajes (MM). Cuando se halla el mensaje de derecho, es re-ejecutado, es decir, desencriptado con la clave única (Ku) del módulo de seguridad y el derecho (Dr) obtenido es verificado (Ver EMM) con ayuda de su huella H(Dr). Cuando se logra esta verificación (Ver EMM), el derecho (Dr) se compara con el procedente del mensaje de control ECM (Dr = Dc ?). El módulo de seguridad determina un estado de error (DEF) tanto cuando la verificación del mensaje fracasa como cuando la comparación da un resultado negativo. Este mismo estado (DEF) se puede determinar cuando la búsqueda (S-Dr) de un mensaje correspondiente a un derecho recibido a través de un mensaje de control ECM falla (S-Dr KO).

[0039] Este proceso de verificación y de comparación se puede activar en varios momentos, a saber:

- en cada recepción de un mensaje de control ECM o

- después de recibir un número predeterminado de mensaje ECM, por ejemplo cada 20 mensajes ECM recibidos o

- a petición gracias a una instrucción incluida en un mensaje EMM o ECM, o

- periódicamente a intervalos de tiempo predefinidos, por ejemplo cada 10 minutos.

[0040] Según una configuración posible para las dos variantes del método, cualquier fracaso de una verificación de un derecho con su huella puede provocar un bloqueo del módulo de seguridad o limitaciones de acceso a los datos del flujo difundido al igual que un resultado negativo de las comparaciones de los derechos en la última etapa.

REIVINDICACIONES

1. Método de verificación de derechos contenidos en un módulo de seguridad asociado a un aparato de tratamiento de datos digitales difundidos, dicho aparato está conectado a un centro de gestión que transmite mensajes de administración (EMM) encriptados de actualización de los derechos (Dr) de acceso a dichos datos digitales y mensajes de control (ECM) que sirven para descodificar los datos difundidos, comprendiendo las etapas preliminares siguientes:

- recepción y lectura por el módulo de seguridad de todo o parte de un mensaje de administración (EMM) que consta al menos de un derecho (Dr) y de una huella H(Dr) obtenida por una función del tipo Hash aplicada sobre dicho derecho (Dr),

- desencriptación y verificación del mensaje de administración (EMM) recibido comparando la huella H(Dr) del derecho (Dr) con una huella H'(Dr) determinada por el módulo de seguridad,

- cuando la huella H(Dr) del derecho (Dr) es idéntica a la huella H'(Dr) determinada por el módulo de seguridad, almacenamiento de todo o parte de dicho mensaje (EMM) en una memoria (MM) de los mensajes del módulo de seguridad,

- recepción de un mensaje de control (ECM) que consta de al menos una contraseña de control y un derecho condicional (Dc) que define el o los derechos necesarios para el uso de la contraseña de control,

dicho método está **caracterizado por el hecho de que** comprende las etapas siguientes:

- extracción del derecho condicional (Dc) del mensaje de control (ECM)

- búsqueda en la memoria de los mensajes (MM) del mensaje de administración (EMM) correspondiente al derecho condicional (Dc)

- cuando se halla el mensaje, desencriptación y verificación de dicho mensaje de administración (EMM) comparando la huella H(Dr) del derecho (Dr) con una huella H'(Dr) determinada por el módulo de seguridad,

- cuando la huella H(Dr) del derecho (Dr) es idéntica a la huella H'(Dr) determinada por el módulo de seguridad, comparación del derecho (Dr) contenido en el mensaje de administración (EMM) hallado con el derecho condicional (Dc),

- cuando el resultado de la comparación indica una diferencia, determinación de un estado de error (DEF) definido bien por un funcionamiento del aparato de tratamiento de datos con derechos restringidos, bien por un bloqueo de dicho aparato.

2. Método según la reivindicación 1, **caracterizado por el hecho de que** el mensaje de administración (EMM) está encriptado con una clave global (Kg), y por el hecho de que el conjunto formado por el derecho (Dr) y por la huella H(Dr) está encriptado con una clave única (Ku) del módulo de seguridad.

3. Método según la reivindicación 2, **caracterizado por el hecho de que** el mensaje de administración (EMM) se almacena en la memoria de los mensajes (MM) después de la desencriptación con la clave global (Kg).

4. Método según una de las reivindicaciones 1 a 3, **caracterizado por el hecho de que** el mensaje de administración (EMM) recibido, leído y desencriptado por el módulo de seguridad es rechazado cuando la verificación de dicho mensaje de administración (EMM) fracasa.

5. Método según una de las reivindicaciones 1 a 4, **caracterizado por el hecho de que** el estado de error (DEF) se determina cuando la verificación del mensaje de administración (EMM) hallado en la memoria de los mensajes (MM) fracasa.

6. Método según una de las reivindicaciones 1 a 5, **caracterizado por el hecho de que** el estado de error (DEF) se determina cuando la búsqueda de un mensaje de administración (EMM) correspondiente a un derecho recibido a través de un mensaje de control ECM fracasa.

7. Método según una de las reivindicaciones 1 a 6, **caracterizado por el hecho de que** el estado de error (DEF) representa un funcionamiento del aparato con derechos restringidos o un bloqueo del módulo de seguridad.

8. Método según la reivindicación 1, **caracterizado por el hecho de que** el proceso de verificación y de comparación del derecho condicional (Dc) del mensaje de control (ECM) con el derecho (Dr) incluido en el mensaje de administración (EMM) almacenado es ejecutado bien en cada recepción de un mensaje de control (ECM), bien después de la recepción de un número predeterminado de mensaje de control (ECM), bien por petición gracias a una instrucción incluida en el mensaje de administración EMM o en el mensaje de control (ECM), bien periódicamente a intervalos predefinidos.

9. Método según una de las reivindicaciones 1 a 8, **caracterizado por el hecho de que** es realizado por el módulo de seguridad de un descodificador de datos digitales audio/vídeo de televisión de pago conectado a un centro de gestión que transmite, a dicho módulo de seguridad, los mensajes de control (ECM) y los mensajes de administración (EMM) de actualización de los derechos de acceso a dichos datos digitales.

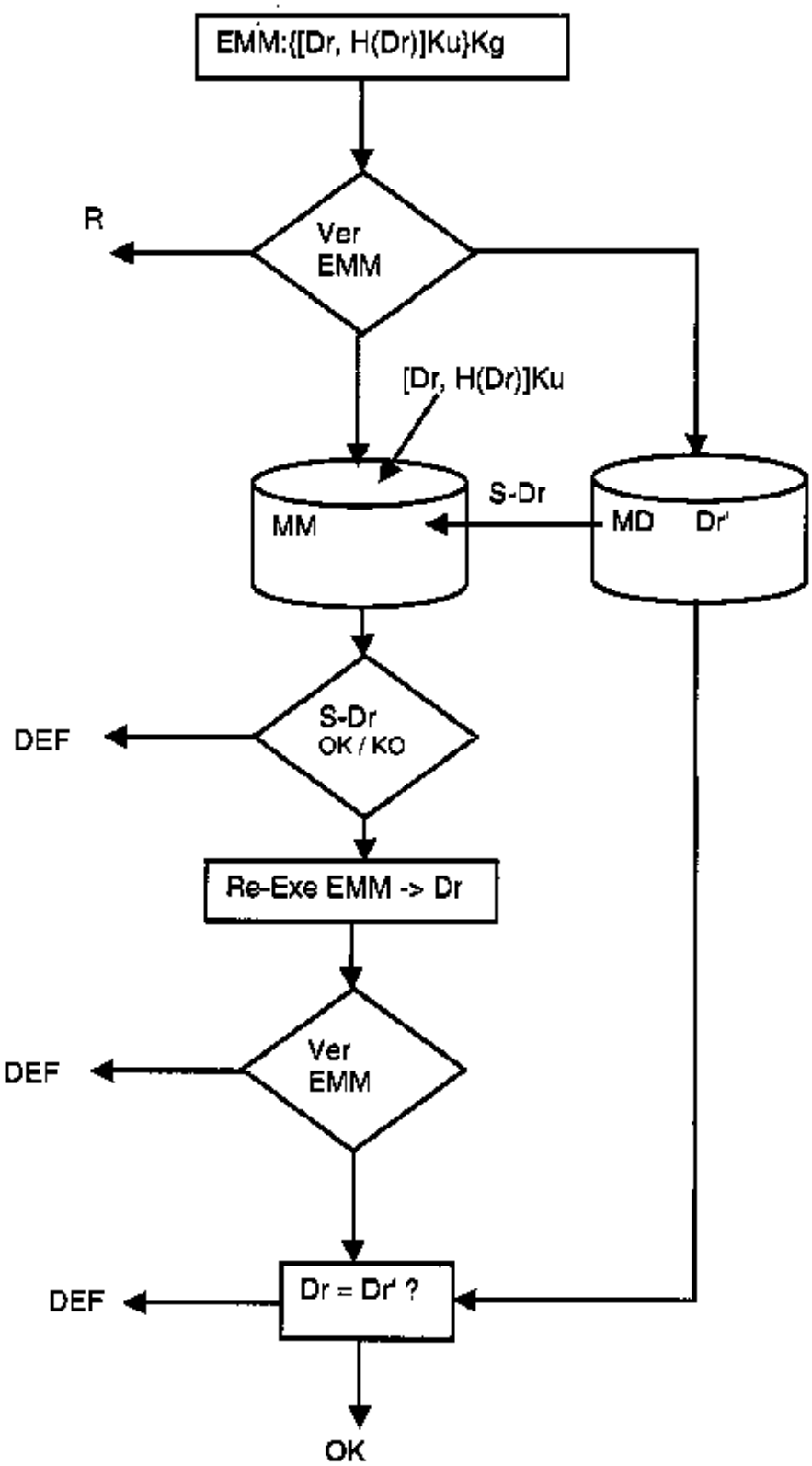
EMM:{[Dr, H(Dr)]Ku}Kg
Ver EMM
R
[Dr, H(Dr)]Ku
MM
S-Dr
MD
Dr'
S-Dr OK / KO
DEF
Re-Exe EMM -> Dr
Ver EMM
DEF
Dr = Dr' ?
DEF
OK

Fig. 1

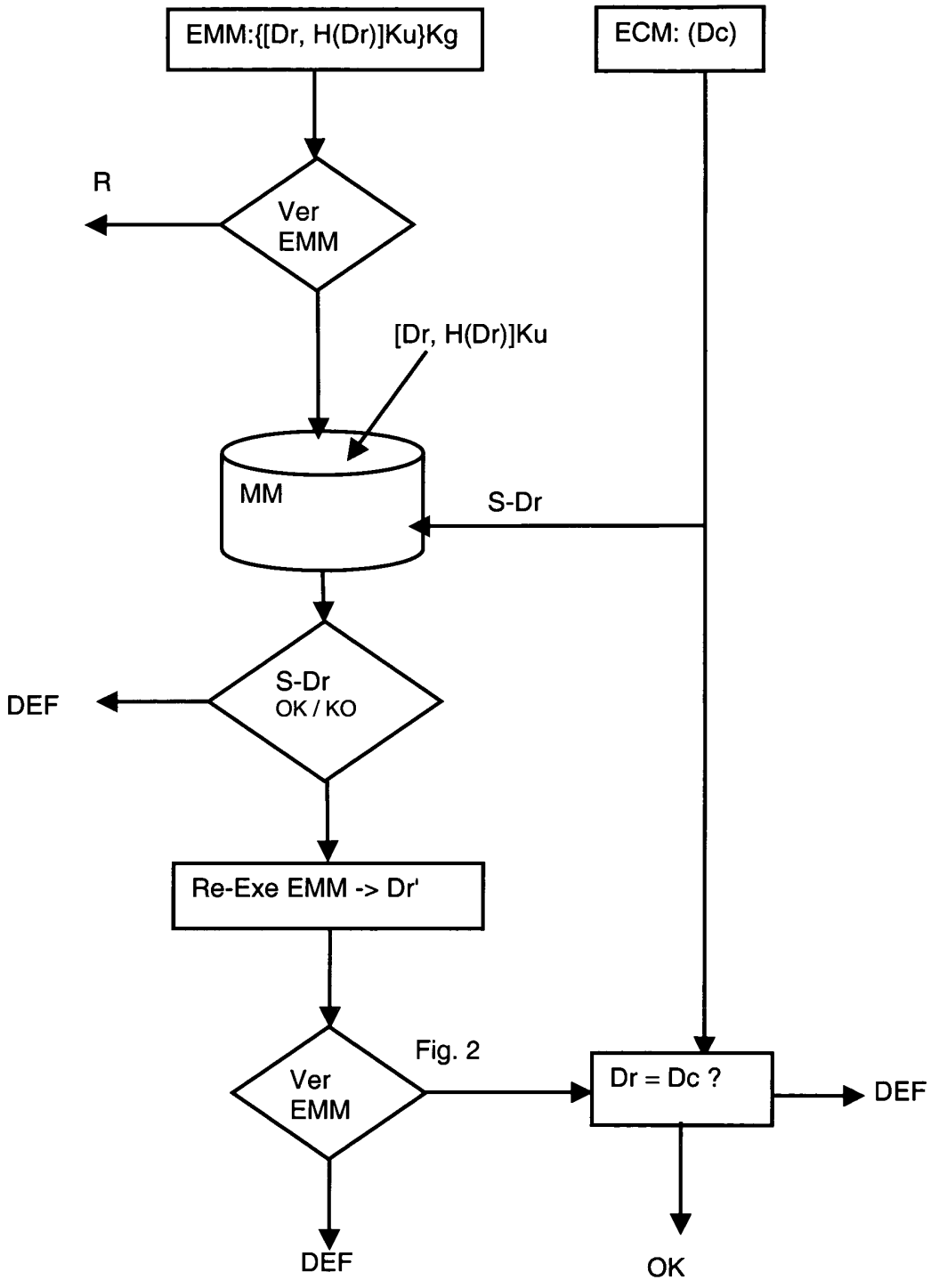
EMM:{[Dr, H(Dr)]Ku}Kg
ECM: (Dc)
R
Ver
EMM
[Dr, H(Dr)]Ku
MM
S-Dr
DEF
S-Dr
OK / KO
Re-Exe EMM -> Dr'
Ver
EMM
Dr = Dc ?
DEF
DEF
OK

Fig. 2

Fig. 2