(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 619 613**

(51) Int. CI.:

H04L 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.06.2014 E 14172225 (6)**

(97) Fecha y número de publicación de la concesión europea: **11.01.2017 EP 2955871**

(54) Título: **Método criptográfico para intercambiar mensajes de forma segura y dispositivo y sistema para implementar este método**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.06.2017

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
22-24, route de Genève
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

PELLETIER, HERVÉ

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método criptográfico para intercambiar mensajes de forma segura y dispositivo y sistema para implementar este método

CAMPO TÉCNICO

[0001] La presente invención se refiere al campo de transferencias de datos entre dispositivos conectados entre sí, implicando operaciones criptográficas para enviar y recibir de forma segura cualquier tipo de mensajes que se deben cambiar entre estos dispositivos.

ANTECEDENTES

[0002] Hay una cantidad de métodos conocidos que implican algoritmos criptográficos, tal como el estándar de encriptación de datos (DES) o el estándar de encriptación avanzada (AES), para el encriptado y desencriptado de datos para transmitir por medio de canales no seguros o dispositivos electrónicos de conexión de redes de cualquier tipo.
Con este fin, tales dispositivos se proporcionan con componentes criptográficos que realizan operaciones criptográficas para cifrar mensajes para hacerlos ininteligibles sin una clave de desencriptación secreta.
Estos componentes se implementan típicamente según la tecnología CMOS (Tecnología de Semiconductores de óxidos metálicos complementarios).
Algoritmos criptográficos implementados en tales componentes son generalmente suficientemente seguros desde un punto de vista matemático.
Sin embargo, el hecho de que tal algoritmo se implementa físicamente por circuitos integrados construidos con transistores interconectados para producir las funciones lógicas de este algoritmo, genera cantidades físicas observables.
La observación de tales cantidades puede llevarse a cabo mediante un osciloscopio, por ejemplo para la supervisión del consumo de energía del circuito integrado.
Variaciones del consumo de energía repentinas aparecen como picos en la pantalla del osciloscopio.
Cada valor máximo puede por ejemplo identificar el inicio de un denominado "ciclo", típicamente en el algoritmo tal como DES y AES donde un mensaje de entrada para encriptar se aplica a una sucesión de grupos de operaciones llamadas "ciclos".
Según tal algoritmo, cada ciclo es colocado bajo el control de una subclave resultante del ciclo precedente.
Por lo tanto, tal algoritmo implica una serie de subclaves que se derivan de una clave secreta usada como clave inicial en el algoritmo.
En el caso de que esta clave secreta inicial sea conocida por una persona maliciosa, ésta se vuelve capaz de desencriptar y encriptar debidamente cualquier mensaje intercambiado por un dispositivo correspondiente que usa el mismo algoritmo con la misma clave secreta según un esquema de encriptación simétrica.

[0003] Hay diferentes maneras de atacar un circuito criptográfico para la recuperación de la clave secreta inicial.
Algunos ataques son conocidos como ataques no invasivos puesto que tienen como objetivo observar el consumo de energía, la emanación electromagnética o el tiempo de procesamiento del circuito.
Otros ataques se referencian como ataques invasivos, ya que ellos implican modificar el circuito, en particular su comportamiento durante un corto período de tiempo.
En esta última categoría, se conoce el análisis de fallos diferencial (DFA) como siendo una amenaza seria contra cualquier sistema de codificación/descodificación.
El análisis de fallos diferencial se basa en la observación y la comparación de los resultados proporcionados por un circuito criptográfico bajo dos estados diferentes.
Uno de estos estados corresponde al funcionamiento normal del circuito, mientras que el otro se obtiene inyectando voluntariamente un fallo dirigido a alterar uno o más bits cambiando de 0 a 1 o viceversa.
Tal inversión de bits físicos puede llevarse a cabo por ejemplo por el barrido de la superficie del circuito integrado con un rayo láser.
Al localizar las áreas sensibles en el circuito criptográfico, los disparos láser permiten interrumpir el comportamiento del circuito en una manera precisa y fácil, ya que se pueden implementar bajo el control de un ordenador, actuando a la vez con una resolución espacial y temporal muy buena.
Cuando diferentes defectos se inyectan durante el procesamiento de un algoritmo criptográfico, el análisis de resultados erróneos permite adivinar la clave secreta observando propagaciones de fallos en el algoritmo.

[0004] US2007/0177720 divulga un método para asegurar un algoritmo criptográfico contra DFA que implica el enmascaramiento por números aleatorios de un algoritmo de encriptación simétrica que encripta un mensaje con una clave de encriptación.

[0005] Por consiguiente, hay una necesidad de proporcionar una solución eficaz que permite prevenir que los atacantes adivinen la clave secreta a través de cualquier análisis de fallo diferencial, o más generalmente para adivinar tal clave a través de la información adquirida por cualquier tipo de análisis.

RESUMEN DE LA INVENCIÓN

[0006] El objetivo de la presente invención es resolver, al menos en parte, los inconvenientes anteriormente mencionados.
Con este fin, la presente invención sugiere un método criptográfico y un dispositivo para intercambiar datos de forma segura entre al menos dos dispositivos, implicando la implementación de un proceso criptográfico que es particularmente complejo.
Según la invención, la clave secreta, que se comparte por todos los dispositivos del mismo sistema como una clave simétrica, nunca se usa directamente como la clave de codificación/descodificación de los mensajes intercambiados.
De hecho, la clave que se usa para encriptar/desencriptar los mensajes intercambiados entre los dispositivos de un mismo sistema siempre dependen de una pluralidad de números aleatorios, en particular.
Más específicamente, cada dispositivo genera al menos un número aleatorio que se tiene en cuenta para determinar la clave que se usa para encriptar/desencriptar los mensajes intercambiados.
Por consiguiente, si el sistema comprende tres dispositivos, la clave anteriormente mencionada dependerá de al menos tres números aleatorios.

[0007] Además, un nivel de clave adicional es determinado antes de encriptar/desencriptar el mensaje que se debe intercambiar.
Por consiguiente, el presente método implica tres niveles clave para encriptar/desencriptar los mensajes.
Además, el mensaje que se debe intercambiar nunca se usa directamente como datos de entrada del algoritmo para generar el criptograma que tiene que ser enviado, pero es siempre usado con cada uno de los números aleatorios para generar primero un pseudo mensaje que será luego encriptado por el algoritmo criptográfico anteriormente mencionado.

[0008] Preferiblemente, los números aleatorios son renovados cada vez que un mensaje tiene que ser intercambiado.
Por consiguiente, la presente invención evita que cualquier persona maliciosa adivine la clave secreta compartida a través de un ataque implicando un análisis de fallos diferencial.
Además, gracias a la complejidad proporcionada tanto por el pseudo mensaje como por la clave derivada usada para la encriptación, el método criptográfico de la presente invención alcanza un nivel de seguridad particularmente alto.

[0009] El objetivo y las ventajas de la presente invención son conseguidas gracias al método criptográfico de acuerdo con el objeto según la reivindicación 1 y gracias a un dispositivo de acuerdo con el objeto según la reivindicación 11.

[0010] Otras ventajas y formas de realización serán presentadas en la siguiente descripción detallada.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0011] La presente invención será mejor entendida gracias a las figuras anexas donde:
La Figura 1 representa una visión de conjunto del sistema de la presente invención según una forma de realización,
La Figura 2 es un organigrama que muestra una forma de realización ejemplar del método criptográfico de la presente invención,
La Figura 3 muestra una alternativa de un extracto del organigrama de la figura 2,
La Figura 4 es una representación esquemática de uno de los dispositivos del sistema mostrado en Fig.1.

DESCRIPCIÓN DETALLADA

[0012] En referencia a la Fig. 1, ésta muestra esquemáticamente una visión de conjunto de una forma de realización del sistema donde el método y una pluralidad de dispositivos del presente pueden ser implementados.
El sistema de comunicación muestra en esta figura tres dispositivos D1, D2, D3 conectados entre sí de cualquier manera.
Debe observarse que el número de dispositivos D1, D2, D3, etc ... es ilimitado y el sistema ilustrado en esta figura se toma como un ejemplo entre muchas otras posibilidades, tanto en cuanto a conexión como al número de dispositivos.
Tal sistema podría incluir dos dispositivos solo, conectados entre sí bien por medio de una red, tal como Internet, o a través de cualquier otro tipo de conexión (con cable o inalámbrica), en particular una conexión no segura.

[0013] Cada dispositivo D1, D2, D3 puede intercambiar mensajes M con al menos otro dispositivo, preferiblemente con cualquier otro dispositivo en el sistema.
Como estos mensajes M son intercambiados de forma segura, estos han sido ilustrados en esta figura por sobres, cada uno sellado con un candado.
Para encriptar o desencriptar mensajes seguros M, cada dispositivo D1, D2, D3 debe manejar al menos tres claves criptográficas K, K1, K2.
Una de estas claves es una clave K secreta compartida común para todos los dispositivos D1, D2, D3 del sistema.

Esta clave secreta K se puede implementar durante la fabricación del dispositivo D1, D2, D3 o su relativo conjunto de chips, o después durante su fase de personalización o durante una fase de inicialización.

[0014] Como se muestra esquemáticamente en esta figura, cada dispositivo envía y recibe otros datos denominados R1, R2; R3.
Tales datos se refieren a números aleatorios.
Cada dispositivo (por ejemplo, D1) genera un número aleatorio (R1) que se envía a los otros dispositivos (D2, D3) y recibe el número aleatorio (R2, R3) generado por cada uno de los otros dispositivos (D2, D3).
Basándose en la visión de conjunto proporcionada por la Fig. 1, el método para intercambiar mensajes M de forma segura entre al menos dos dispositivos se describe en detalle con referencia a la Fig. 2.

[0015] Por simplicidad, la Fig. 2 divulga, paso a paso, el método de la presente invención mientras se refiere a un sistema que comprende dos dispositivos solo, D1 y D2, identificados respectivamente por los números de referencia 10, 20.
En esta figura, los pasos realizados por cada uno de estos dispositivos se muestran en diferentes columnas y se suceden de arriba a abajo.
Los pasos comunes que son realizados por cada uno de los dispositivos se representan en una columna central.
Debe observarse que estos pasos comunes se realizan por cada dispositivo en una manera individual.
No hay ningún requisito para procesar los pasos comunes simultáneamente dentro de cada dispositivo implicado para el intercambio de mensajes.

[0016] Como se ha mencionado anteriormente, cada dispositivo D1, D2, comprende una clave secreta compartida común K para todos los dispositivos que desean intercambiar mensajes mutuamente.
Esta clave secreta K se muestra en el recuadro 31 de la figura 2.
En esta forma de realización, el dispositivo D1 se destina a enviar un mensaje M al dispositivo D2.
Por consiguiente, el primer dispositivo D1 corresponde al dispositivo emisor y el segundo dispositivo D2 corresponde al dispositivo receptor.
Aunque hay solo un dispositivo receptor mostrado en esta figura, se debe entender que el mismo mensaje M podría ser enviado desde el dispositivo emisor a una pluralidad de dispositivos receptores.
En el recuadro 11, el dispositivo emisor D1 tiene que preparar o recuperar el mensaje M que tiene que ser enviado.
Tal mensaje M puede referirse a cualquier tipo de datos, pero normalmente éste se referirá a datos sensibles, cuya naturaleza principalmente depende del tipo de dispositivos implicados en el sistema de comunicación en cuestión.

[0017] Cada dispositivo D1, D2 genera un número aleatorio antes de enviarlo al otro dispositivo, en particular a una pluralidad de dispositivos seleccionados o a todos los demás dispositivos en el caso de que el sistema comprenda más de dos dispositivos.
Este paso se muestra en los recuadros 12, 21, donde el dispositivo emisor D1 genera un primer número aleatorio R1, que se envía al dispositivo receptor D2, y éste genera un segundo número aleatorio R2 que se envía al dispositivo emisor D1.
La realización de un intercambio mutuo de los números aleatorios con cada uno de los dispositivos se puede conseguir incluso si estos dispositivos no estaban previamente acordados para intercambiar un mensaje inminente, por ejemplo, mediante una señal específica reconocida por estos dispositivos durante un paso previo.
En este caso, uno podría esperar que el mero hecho de recibir un número aleatorio R1 (es decir datos que se pueden identificar como tales, bien a través de un identificador específico, o por medio de un formato particular) se puede reconocer por el(los) dispositivo(s) receptor(es) como siendo una señal de activación que informa que un mensaje M se debe recibir desde el dispositivo emisor.
Por consiguiente, cada dispositivo se vuelve completamente capaz de ejecutar los pasos requeridos del presente método a su debido tiempo.

[0018] Además, en el caso en el que el sistema implica más de dos dispositivos, como se muestra en el ejemplo de la Fig.1, uno puede además proporcionar medios para identificar el dispositivo emisor en el dispositivo receptor, si fuera necesario.
Si la comunicación no está todavía establecida entre el dispositivo emisor y el(los) dispositivo(s) receptor(es) por ejemplo durante una sesión corriente, una vía posible podría ser identificar la dirección del dispositivo emisor o transmitir el identificador (ID) del dispositivo emisor hacia el dispositivo receptor.
Esto se puede conseguir, por ejemplo, añadiendo, al número aleatorio R1, el número ID que pertenece al dispositivo emisor D1 o incluyendo tal ID en cualquiera de los otros datos.

[0019] En el recuadro 33, cada dispositivo D1, D2, determina una primera clave K1 calculando una primera operación OP1 usando la clave secreta compartida K y cada número aleatorio R1, R2 como operandos.
En la ilustración proporcionada por la Fig.2, esta primera operación OP1, al igual que otras operaciones posteriores, se refiere a una operación OP exclusiva, como un ejemplo no limitativo.
Conforme a una forma de realización preferida y como se muestra en este recuadro 33, el resultado de la primera operación OP1 es directamente usada como la primera clave K1.

[0020] En el recuadro 35, cada dispositivo D1, D2, calcula posteriormente una segunda operación OP2 que usa al menos cada número aleatorio R1, R2 como operandos.
Luego, basándose en el resultado de esta segunda operación OP2, cada dispositivo D1, D2 además determina una segunda clave K2.
Conforme al ejemplo del recuadro 35, esto se realiza por el encriptado del resultado de la segunda operación OP2 mediante un primer algoritmo, denominado A1, que usa la primera clave K1 como clave de encriptación.
Por consiguiente, la segunda operación, o directamente su resultado, se introduce en el primer algoritmo A1 con la primera clave criptográfica requerida K1.
En respuesta, este primer algoritmo proporciona la segunda clave criptográfica K2 como resultado.

[0021] En el recuadro 14, el dispositivo que actúa como dispositivo emisor D1 calcula una tercera operación OP3 que usa el mensaje M y cada número aleatorio R1, R2 como operandos.
De esta manera, el dispositivo emisor D1 determina un denominado pseudo mensaje M' dado que se basa en el mensaje M, pero parece diferente del mensaje inicial M, aunque este último todavía no haya sido encriptado.

[0022] En el recuadro 16, el dispositivo emisor D1 calcula un criptograma C que resulta de la encriptación del pseudo mensaje M'.
Con este fin, usa el pseudo mensaje M' como entrada de un segundo algoritmo A2 con la segunda clave K2 como clave de encriptación.

[0023] En el recuadro 18, el criptograma C se transmite por el dispositivo emisor a al menos otro dispositivo que actúa como dispositivo receptor.

[0024] Cuando el dispositivo receptor D2 obtiene el criptograma C, es capaz de desencriptarlo mediante el mismo algoritmo A2 y la misma clave K2, como se muestra en el recuadro 23.
Con este fin, el segundo algoritmo A2 será, o incluirá, una función de dos direcciones que se pueden transformar (ver la anotación A2-1 en la Fig. 2).
Por supuesto, el mismo algoritmo tiene que usarse tanto por los dispositivos emisores como los receptores.
Según la forma de realización preferida, la segunda clave K2 se usa como clave de desencriptación directa o indirecta del segundo algoritmo.
El uso de la segunda clave K2 como clave indirecta se describe con referencia a la Fig. 3.
En cualquier caso, la desencriptación del criptograma C permite recuperar el pseudo mensaje como resultado del segundo algoritmo A2.

[0025] Finalmente, en el recuadro 25, cada dispositivo receptor D2 recupera el mensaje M en su forma de texto común inicial, a partir el pseudo mensaje por la inversión de la tercera operación OP3 (ver la anotación OP3-1 en la Fig. 2).

[0026] Debe observarse que el primer algoritmo A1 puede ser diferente o idéntico al segundo algoritmo A2.
Sin embargo y contrariamente al segundo algoritmo, el primer algoritmo puede usar una función unidireccional (o puede ser él mismo tal función) que proporciona la segunda clave K2.
Por consiguiente, tal segunda clave K2 podría ser la recopilación de una función hash o podría ser derivada de tal función, por ejemplo.

[0027] Sean cuales sean los algoritmos (A1, A2) usados en este método, estos deben ser los mismos para todos los dispositivos que quieren intercambiar mensajes M.
Estos algoritmos se pueden implementar dentro de cada dispositivo a través de formas diferentes, por ejemplo, durante la fabricación de los dispositivos, durante su personalización o durante una fase de inicialización.

[0028] Haciendo referencia ahora a la Fig. 3, esta figura muestra los pasos últimos del método ilustrado en la Fig. 2, donde el recuadro 37 representa un paso adicional como una alternativa del organigrama precedente.
Esta variante corresponde al recuadro donde la segunda clave K2 se usa como clave de codificación/descodificación indirecta en el segundo algoritmo A2.
Con este fin, una tercera clave K3 es determinada, en cada dispositivo D1, D2, por una cuarta operación OP4 que usa la segunda clave K2 y la clave secreta compartida K como operandos.
Como se muestra en el recuadro 37, el resultado de esta cuarta operación OP4 proporciona la tercera clave criptográfica K3.

[0029] De una manera similar en cuanto a los algoritmos, todas las operaciones OP1, OP2, OP3, OP4, o algunas de estas, se pueden implementar dentro de cada dispositivo durante la fabricación de los dispositivos, durante su personalización o durante una fase de inicialización.

[0030] En cuanto al dispositivo emisor D1, el paso mostrado en el recuadro 37 se realiza entre los pasos de los recuadros 35 y 16, ya que necesita la segunda clave K2 (determinada por el paso del recuadro 35) y el resultado de este paso adicional será usado con el segundo algoritmo A2 (durante el paso mostrado en el recuadro 16).

En cuanto al(los) dispositivo(s) receptor(es) D2, este paso adicional se realiza entre los pasos de los recuadros 35 y 23 por las mismas razones.

[0031] Como se muestra en la Fig. 3, el uso de la segunda clave K2 en el segundo algoritmo A2 (es decir en los pasos de los recuadros 16 y 23) ha sido sustituido por la tercera clave K3.
Esto resulta del hecho de que la segunda clave K2 se usa en una manera indirecta en estos pasos.
Por esta razón, los números de referencia de estos dos recuadros han sido respectivamente rectificados por 16' y 23' en la Fig. 3.

[0032] Debe observarse que pasos determinados mostrados en la Fig. 2 o Fig. 3 podrían ser colocados en un orden diferente.
Por ejemplo, los pasos del recuadro 14 podrían ser realizados donde sea entre los intercambios de los números aleatorios R1, R2 (en los recuadros 12, 21) y la encriptación del pseudo mensaje (en el recuadro 16, 16').
El mismo principio se aplica para los pasos del recuadro 37, como se ha explicado anteriormente.

[0033] Según una forma de realización, al menos parte de al menos cualquiera de las operaciones OP1, OP2, OP3, OP4 implica una operación lógica (álgebra booleana).
Más particularmente, esta operación lógica es una operación OR exclusiva (ver la anotación simbólica $\oplus$ en la Fig. 2 y 3).
Debe observarse que otras funciones lógicas (es decir operaciones básicas y/o derivadas) podrían usarse en vez del operador XOR o con el operador XOR.

[0034] Según otra forma de realización, al menos una parte de al menos cualquiera de las operaciones OP1, OP2, OP3, OP4 implica un número elevado a una potencia.
En este caso, cualquiera de los operandos de la operación pertinente se usa como un exponente de este número que es elegido entre los otros operandos de esta operación.

[0035] Para ejecutar operaciones lógicas, los operandos implicados deben tener el mismo número de dígitos.
En otras palabras y puesto que las operaciones se refieren a operaciones binarias, los operandos deben tener la misma longitud de bits.
Por lo tanto y dependiendo del tipo de operación realizada por ejemplo en el recuadro 33 (OP1), la longitud de bits de los números aleatorios R1, R2 y la longitud de bits de la clave secreta compartida K debería ser la misma.
Con relación a la segunda operación OP2 como se muestra en el ejemplo del recuadro 35, los números aleatorios R1, R2 deben tener la misma longitud de bits.
El mismo principio se aplica a la tercera y cuarta operaciones con relación a los números aleatorios R1, R2 y el mensaje M, por una parte, y las claves criptográficas K2, K, por otra parte.

[0036] Por esta razón, si los operandos de cualquiera de las operaciones OP1, OP2, OP3, OP4 tienen longitudes de bits diferentes, entonces el presente método puede además comprender un paso dirigido a restaurar la misma longitud de bits para cada uno de estos operandos.
Con este fin, la restauración de la misma longitud de bits se puede conseguir de diferentes maneras.

[0037] Según una forma de realización, que se puede conseguir por un "paso de equilibrio" destinado a suplementar el operando con la longitud de bits más pequeña hasta su longitud de bits es igual a la longitud de bits de cualquiera de los otros operandos de la operación pertinente.
Luego, este paso de equilibrio se puede repetir hasta que todos los operandos de la operación pertinente tengan la misma longitud de bits.
El paso destinado a suplementar el operando se puede conseguir por una sucesión de bits 0, por una sucesión de bits 1, incluso por una sucesión de una combinación específica de estos dos bits 0 y 1.
Por supuesto, la sucesión de bits seleccionada debe ser conocida tanto por el(los) dispositivo(s) emisor(es) como por el(los) dispositivo(s) receptor(es), a través de cualquier proceso mencionado antes, por ejemplo, durante la personalización de los dispositivos o sus conjuntos de chips.

[0038] En la variante, este paso de equilibrio podría ser conseguido por la complementación del operando con la longitud de bits más pequeña hasta que la longitud de bits del otro operando (es decir preferiblemente el operando con la longitud de bits más larga) es igual a un múltiple de la longitud de bits del operando suplementado.

[0039] Según otra forma de realización, el denominado paso de equilibrio puede ser primero realizado por la concatenación del operando con la longitud de bits más pequeña con él mismo, hasta alcanzar la misma longitud de bits que el otro operando.
Este método implica que el operando que tiene la longitud de bits más larga es un múltiple del otro operando (es decir el operando concatenado).
En el caso donde un operando no es exactamente un múltiple del otro operando, la concatenación anteriormente mencionada se puede realizar hasta alcanzar una longitud de bits reducida por un valor residual inferior a la longitud de bits del operando concatenado.

Esta longitud de bits residual corresponde al resto de la división euclidiana donde el operando con la longitud de bits más larga es el dividendo y el operando para ser concatenado es el divisor.
Luego, la longitud de bits residual (es decir el valor residual) se puede suplementar por cualquier sucesión de bits, como se ha explicado anteriormente.

[0040] Como ejemplos de una de estas formas de realización aplicadas en particular a la tercera operación OP3, la restauración de la misma longitud de bits se puede conseguir para cada uno de dichos números aleatorios R1, R2 por la concatenación de dicho número aleatorio con él mismo, hasta alcanzar la misma longitud de bits que aquella del mensaje M.
Esta forma de realización implica que los números aleatorios R1, R2 tienen la misma longitud de bits y que la longitud de bits del mensaje M es un múltiple de aquella del número aleatorio.
Si esta condición última no es conseguida, entonces la longitud de bits residual se puede suplementar como ya se ha explicado.

[0041] En la variante y todavía en referencia a la tercera operación OP3, la restauración de la misma longitud de bits podría ser conseguida primero por la complementación del mensaje M hasta que su longitud de bits sea igual a un múltiple de la longitud de bits de cualquiera del número aleatorio R1, R2, luego cortando el mensaje suplementado M en bloques que tienen la misma longitud de bits que la longitud de bits del número aleatorio antes de utilizar cada uno de estos bloques como un mensaje nuevo (M) para ser procesado por los pasos del presente método criptográfico.

[0042] Según otra forma de realización y por simplificación, las claves criptográficas usadas en el presente método, preferiblemente al menos la segunda clave K2 y la clave secreta compartida K, tienen la misma longitud de bits.
Por la misma razón, todos los números aleatorios R1, R2 también tienen la misma longitud de bits.

[0043] Ventajosamente, generando un número aleatorio en cada dispositivo y usando todos los números aleatorios generados tanto para derivar la clave criptográfica K2, K3, que se usa para el cálculo del criptograma C, como para la determinación del pseudo mensaje para encriptar, el objeto de la presente invención aumenta significativamente la seguridad aplicada a los mensajes M intercambiados.

[0044] Todavía ventajosamente, aunque uno de los números aleatorios sea adivinado por una persona maliciosa, ésta será incapaz de deducir la clave que ha sido usada para el encriptado del pseudo mensaje M.
Además, aunque esta clave pudiera ser descubierta por esta persona, ésta seguiría siendo incapaz de recuperar el mensaje inicial M desde el pseudo mensaje M, suponiendo que para recuperar el mensaje original M, esta persona primero necesita poseer todos los números aleatorios y luego debe saber cuál es la tercera operación (OP3) emprendida en el método.
Esto también requiere ser consciente de todos los operadores usados en esta operación, e incluso conocer el orden de cada operador y cada operando usado dentro de esta operación, dependiendo de la naturaleza de esta operación.

[0045] Todavía ventajosamente, la clave secreta compartida K nunca es usada directamente como clave criptográfica en cualquiera de los algoritmos criptográficos A1, A2 implementados en el presente método.
En contraste, la clave secreta compartida K solo se usa dentro de operaciones matemáticas (OP1, OP4) cuyos resultados se usan posteriormente como claves en estos algoritmos.
Por consiguiente, la clave secreta compartida K nunca es expuesta directamente al primer plano, dentro de un algoritmo criptográfico.

[0046] Preferiblemente, los pasos del presente método son emprendidos cada vez que un mensaje M tiene que ser intercambiado.
Esto se puede aplicar sea cual sea la forma de realización del método.
Por consiguiente, los números aleatorios generados por cada dispositivo tienen un uso único, suponiendo que un número aleatorio nuevo es generado, por cada dispositivo, cada vez que un mensaje nuevo tiene que ser enviado.
Por lo tanto, la clave secreta compartida K es diferente ventajosamente siempre que un mensaje M es intercambiado.
Esto proporciona un método fuerte para intercambiar de forma segura mensajes y en particular un método para evitar cualquier ataque de DFA.

[0047] Finalmente, debe observarse que el mensaje M puede comprender cualquier tipo de datos, en particular datos sensibles tales como contraseñas, palabras de control, clave criptográfica o cualquier otra información confidencial.

[0048] La presente invención también se refiere a un dispositivo o a un sistema adecuado para la implementación de cualquiera de las formas de realización del método descrito anteriormente.

[0049] En referencia a la Fig. 4, ésta muestra esquemáticamente con más detalle uno de los dispositivos 10, 20 representados en el sistema de la figura 1.

Este dispositivo puede ser indiferentemente usado como un dispositivo emisor D1 o como un dispositivo receptor D2, y preferiblemente incluso tanto como dispositivo emisor como receptor.
Con este fin, comprende diferentes componentes incluyendo al menos:
* una interfaz de comunicación 1 para intercambiar datos (M', R1, R2, ...), en particular para intercambiar datos con al menos otro dispositivo,
* una memoria segura 2 para el almacenamiento de la clave secreta compartida K,
* un generador aleatorio 3 para generar un número aleatorio R1 cuando un mensaje M tiene que ser intercambiado, preferiblemente cada vez que este mensaje tiene que ser intercambiado,
* al menos una unidad de cálculo 7 para la emisión de al menos un resultado de una operación (OP1, OP2, OP3, OP4) usando operandos (por ejemplo, R1, R2, K, M) como entradas,
* al menos una unidad criptográfica 8 para ejecutar algoritmos (A1, A2) mediante por lo menos una clave criptográfica (K1, K2, K3), y
* una unidad central de procesamiento 5 encargada de la administración de los componentes anteriormente mencionados (1, 2, 3, 7, 8) conforme a los pasos del método criptográfico descrito aquí arriba.

[0050] El dispositivo 10, 20 se puede usar en cualquier caso en que se deben intercambiar datos sensibles de forma segura.
Tal dispositivo puede adoptar la forma de un circuito electrónico (circuito integrado, preferiblemente un circuito monolítico), tal como una tarjeta inteligente o un conjunto de chips adecuado para ser insertado en otro dispositivo.
Este último podría ser un descodificador (en el campo de TV de pago), un teléfono inteligente o cualquier otro dispositivo de comunicación.
En la variante, tal tarjeta inteligente podría ser usada también como un dispositivo independiente, por ejemplo como tarjeta de acceso, como tarjeta bancaria (tarjetas de crédito o tarjeta de débito) para comunicar con una terminal de control.

[0051] El cálculo de cada operativo OP1, OP2, OP3, OP4 se puede realizar usando una unidad de cálculo único 7 configurada para ejecutar operaciones diferentes, o diferentes unidades de cálculo 7, cada una dedicada a una de estas operaciones.
El mismo principio se aplica a la unidad criptográfica 8 con respecto a los algoritmos A1, A2.

[0052] La invención también se refiere a un sistema como se muestra en la Fig. 1.
Tal sistema comprende al menos dos dispositivos criptográficos 10, 20, conectados entre sí, para la implementación de cualquier forma de realización del método descrito anteriormente.
Cada dispositivo 10, 20 de este sistema comprende al menos los componentes que fueron enumerados arriba durante la descripción detallada del dispositivo presentado como otro objeto de la presente invención.
Además, cualquiera de los dispositivos del sistema pueden incluir al menos una de las anteriormente mencionadas características opcionales relacionadas.

REIVINDICACIONES

1. Método criptográfico para intercambiar de forma segura mensajes (M) entre al menos dos dispositivos (D1, D2) cada uno almacenando una clave secreta compartida (K) común a dichos dispositivos, comprendiendo los pasos siguientes:
- generación de un número aleatorio (R1, R2) en cada dispositivo,
- envío por cada dispositivo del número aleatorio generado (R1, R2) a los otros dispositivos,
- determinación, en cada dispositivo, de una primera clave (K1) calculando una primera operación que usa tanto dicha clave secreta compartida (K) como cada número aleatorio (R1, R1) como operandos,
- determinación, en cada dispositivo, de una segunda clave (K2) por el encriptado de un resultado de una segunda operación con un primer algoritmo usando dicha primera clave (K1) como clave de encriptación, dicha segunda operación usando al menos cada número aleatorio (R1, R2) como operandos,
- determinación, por uno de dichos dispositivos que actúa como un dispositivo emisor (D1), de un pseudo mensaje (M') mediante el cálculo de una tercera operación reversible que usa tanto dicho mensaje (M) como cada número aleatorio (R1, R2) como operandos,
- cálculo, por dicho dispositivo emisor (D1), de un criptograma (C) resultante de la encriptación de dicho pseudo mensaje (M') con un segundo algoritmo usando dicha segunda clave (K2) como clave de encriptación directa o indirecta,
- transmisión de dicho criptograma (C) desde dicho dispositivo emisor (D1) a al menos otro dispositivo que actúa como dispositivo receptor (D2),
- recepción de dicho criptograma (C) en dicho dispositivo receptor (D2),
- desencriptación del criptograma (C) en el dispositivo receptor (D2) usando dicha segunda clave (K2) como clave de desencriptación directa o indirecta de dicho segundo algoritmo para recuperar dicho pseudo mensaje (M'),
- recuperación de dicho mensaje (M) de dicho pseudo mensaje (M') por la inversión de dicha tercera operación.

2. Método criptográfico según la reivindicación 1, donde el uso de dicha segunda clave (K2) como clave de encriptación o de desencriptación indirecta, en el segundo algoritmo, se realiza con una tercera clave (K3) determinada, en cada dispositivo, por una cuarta operación usando dicha segunda clave (K2) y dicha clave secreta (K) compartida como operandos.

3. Método criptográfico según la reivindicación 1 o 2, donde al menos una parte de al menos cualquiera de dichas operaciones implica una operación lógica.

4. Método criptográfico según la reivindicación 3, donde dicha operación lógica es una operación OR exclusiva.

5. Método criptográfico según cualquiera de reivindicaciones anteriores, donde si los operandos de cualquiera de dichas operaciones tienen longitudes de bits diferentes, entonces se restaura la misma longitud de bits para cada uno de dichos operandos.

6. Método criptográfico según la reivindicación 5, donde la restauración de la misma longitud de bits se consigue por un paso de equilibrio dirigido a suplementar el operando con la longitud de bits más pequeña hasta que su longitud de bits es igual a la longitud de bits de cualquiera de los otros operandos, luego repitiendo dicho paso de equilibrio hasta que todos los operandos (u operandos suplementados) tengan la misma longitud de bits.

7. Método criptográfico según la reivindicación 6, donde dicho paso de equilibrio es antes realizado por la concatenación del operando que tiene la longitud de bits más pequeña con él mismo, hasta alcanzar la misma longitud de bits que el otro operando, o hasta alcanzar una longitud de bits reducida por un valor residual inferior a la longitud de bits del operando concatenado.

8. Método criptográfico según la reivindicación 7, donde dicho paso de equilibrio se aplica a dicha tercera operación y el operando con la longitud de bits más pequeña es cualquiera de dichos números aleatorios (R1, R2) mientras dicho otro operando es el mensaje (M).

9. Método criptográfico según cualquiera de las reivindicaciones anteriores, donde dicho primer algoritmo usa una función unidireccional.

10. Método criptográfico según cualquiera de las reivindicaciones anteriores, donde al menos una parte de al menos cualquiera de dichas operaciones implica un número elevado a una potencia, donde cualquiera de dichos operandos se usan como un exponente de dicho número elegido entre los otros operandos.

11. Dispositivo criptográfico (10, 20) para implementar el método criptográfico según cualquiera de las reivindicaciones 1 a 10, que comprende diferentes componentes incluyendo al menos una interfaz de comunicación (1) para el intercambio de datos, una memoria segura (2) para almacenar una clave secreta compartida (K), un generador aleatorio (3) para generar un número aleatorio (R1, R2), al menos una unidad de cálculo (7) que emite un resultado de una operación usando operandos como entradas, al menos una unidad criptográfica (8) para ejecutar

algoritmos mediante por lo menos una clave criptográfica (K1, K2, K3), y una unidad central de procesamiento (5) encargada de la administración de dichos componentes conforme a los pasos de dicho método criptográfico.

12. Dispositivo criptográfico (10, 20) según la reivindicación 11, **caracterizado por el hecho de que** está formado por un circuito monolítico.

13. Sistema que comprende al menos dos dispositivos criptográficos (10, 20) conectados entre sí para la implementación del método criptográfico según cualquiera de las reivindicaciones 1 a 10, donde cada uno de dichos dispositivos comprende diferentes componentes incluyendo al menos una interfaz de comunicación (1) para el intercambio de datos, una memoria segura (2) para almacenar una clave secreta compartida (K), un generador aleatorio (3) para generar un número aleatorio (R1, R2), al menos una unidad de cálculo (7) que emite un resultado de una operación usando operandos como entradas, al menos una unidad criptográfica (8) para ejecutar algoritmos mediante por lo menos una clave criptográfica (K1, K2, K3), y una unidad central de procesamiento (5) encargada de la administración de dichos componentes conforme a los pasos de dicho método criptográfico.

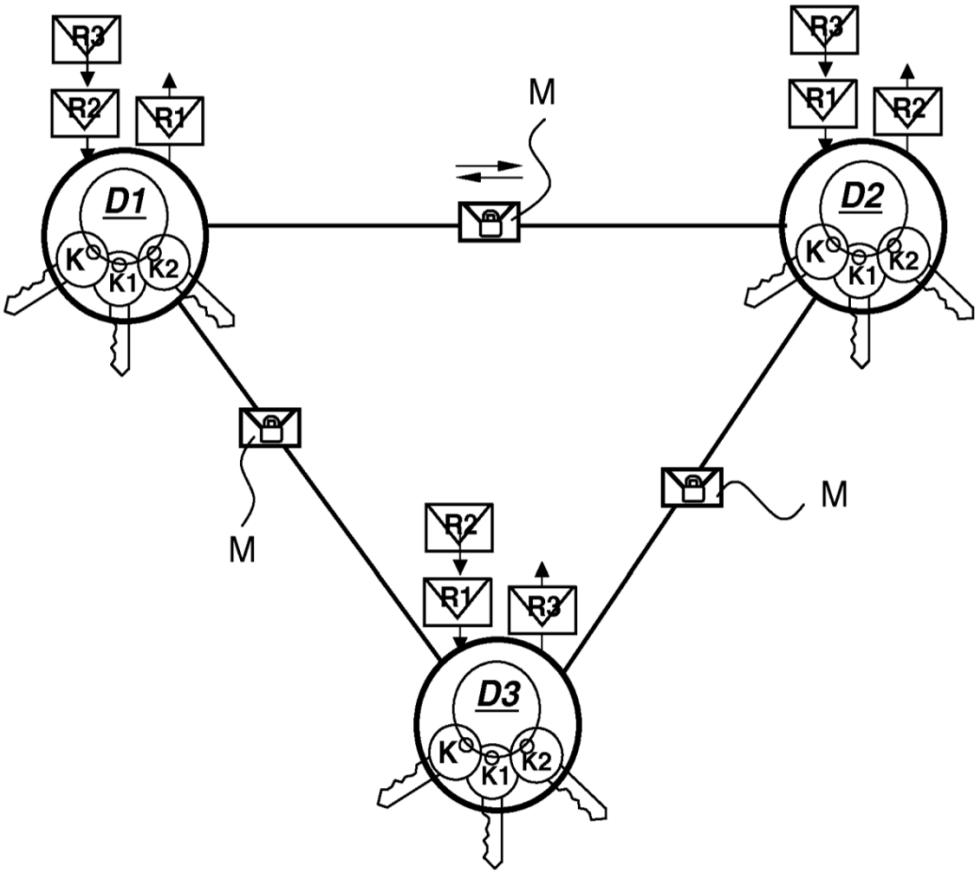

Fig. 1

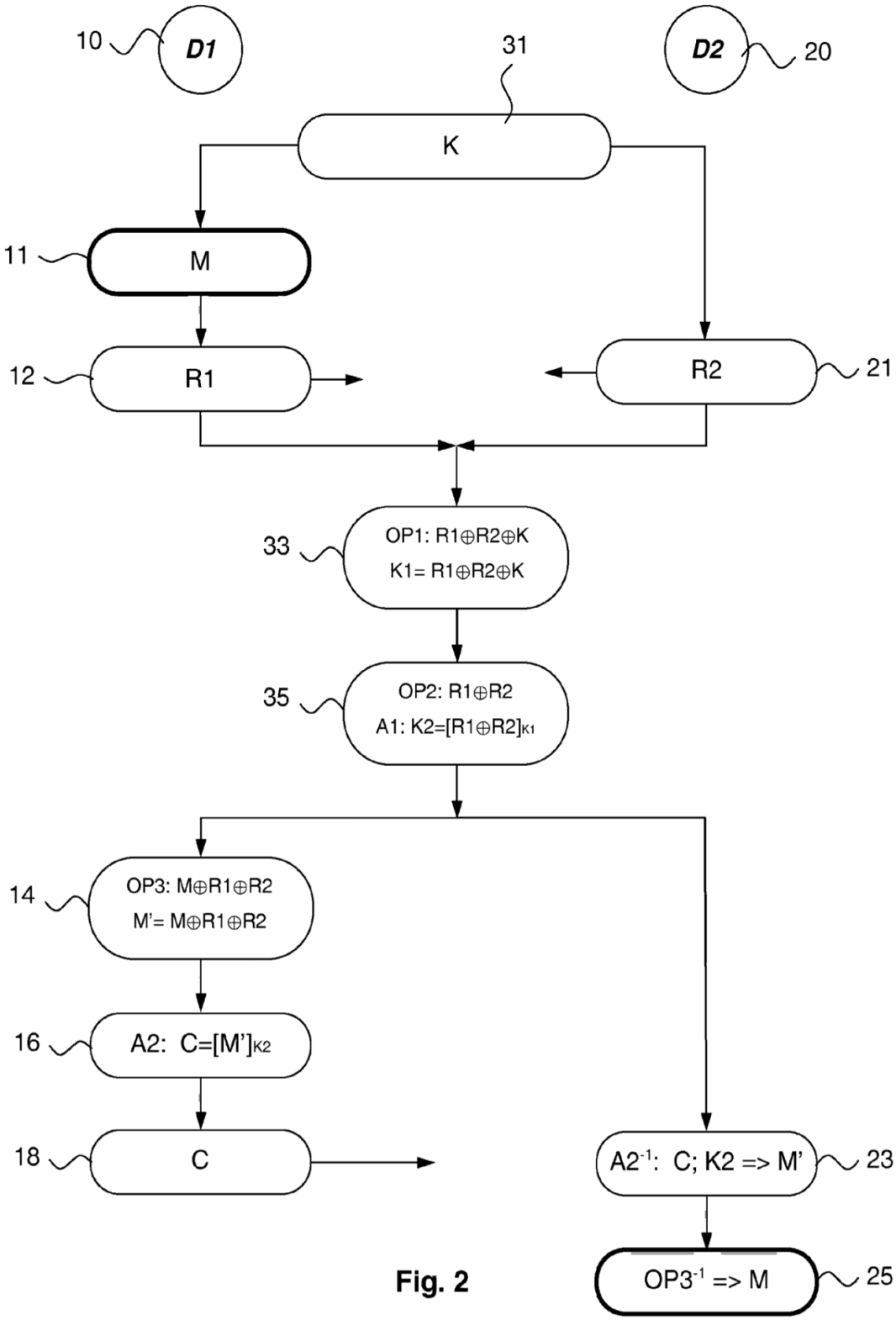
10
D1
31
D2
20
K
11
M
12
R1
R2
21
33
OP1: R1⊕R2⊕K
K1= R1⊕R2⊕K
35
OP2: R1⊕R2
A1: K2=[R1⊕R2]K1
14
OP3: M⊕R1⊕R2
M'= M⊕R1⊕R2
16
A2: C=[M']K2
18
C
A2-1: C; K2 => M'
23
OP3-1 => M
25

Fig. 2

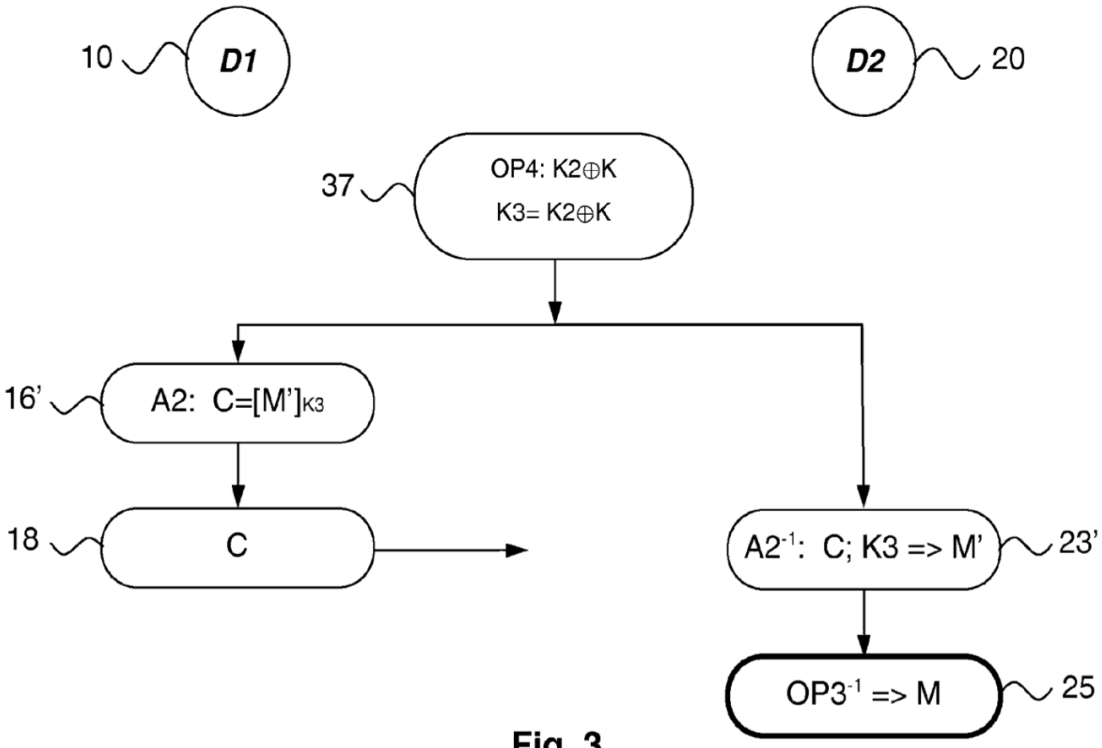
10
D1
D2
20
37
OP4: K2⊕K
K3= K2⊕K
16'
A2: C=[M']K3
18
C
A2-1: C; K3 => M'
23'
OP3-1 => M
25

Fig. 3

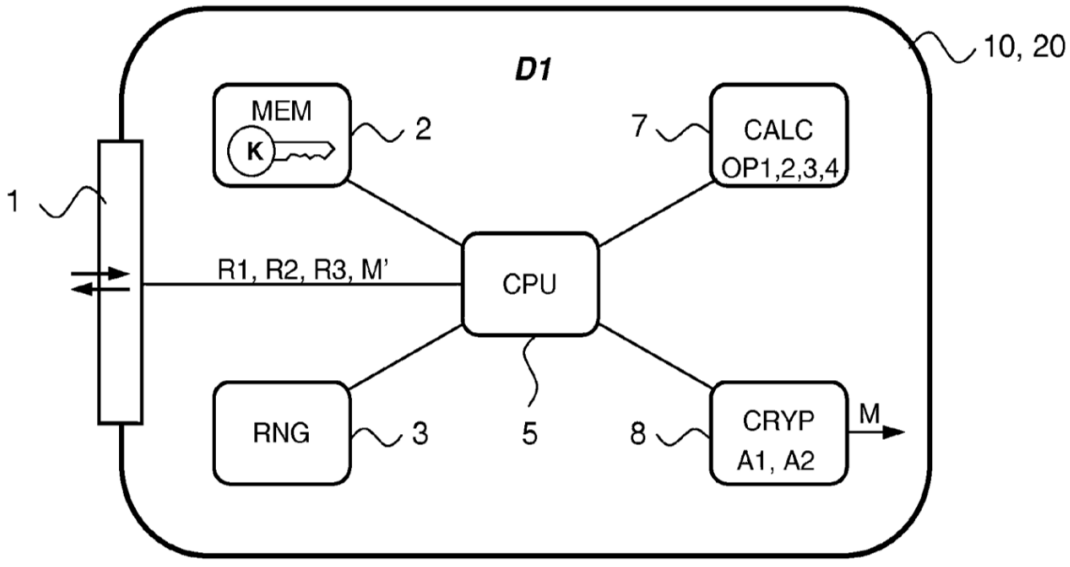
10, 20
D1
MEM
K
2
7
CALC
OP1,2,3,4
1
R1, R2, R3, M'
CPU
RNG
3
5
8
CRYP
A1, A2
M

Fig. 4