(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 737 426**

(51) Int. CI.:

G06F 21/72 (2013.01)
G06F 21/85 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.12.2010 E 10015270 (1)**

(97) Fecha y número de publicación de la concesión europea: **22.05.2019 EP 2461265**

(54) Título: **Dispositivo y método de manejo de datos confidenciales**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.01.2020

(73) Titular/es:

NOVOMATIC AG (100.0%)
Wiener Strasse 158
2352 Gumpoldskirchen, AT

(72) Inventor/es:

HUEBER, ANDREAS;
NAGL, GERHARD;
NOWAK, ROBERT y
MUDRY, IGOR

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Dispositivo y método de manejo de datos confidenciales

La presente invención se refiere a un dispositivo para el manejo de datos confidenciales y a un método para transferir de manera segura datos confidenciales entre al menos una unidad de procesamiento y un dispositivo de memoria. La invención se refiere además a un circuito integrado con un área de memoria integrada para almacenar de forma segura datos confidenciales. Además, la invención está dirigida a una máquina de juego que procesa datos confidenciales.

La seguridad de los datos es un tema importante para muchos aspectos de los negocios, especialmente en lo que se refiere a datos confidenciales o de propiedad almacenados. Por ejemplo, el código fuente de un programa de ordenador almacenado en una memoria flash (u otra forma de memoria electrónica) puede ser información de propiedad exclusiva valiosa. Otro ejemplo de información de propiedad exclusiva puede ser el registro de datos de contabilidad de una máquina de juego.

Por ejemplo, un sistema de microprocesador puede implementarse como un sistema en un chip (SOC) que comprende un procesador que accede a la memoria tanto en el chip como fuera del chip. Se puede lograr un cálculo seguro si el software es seguro y las instrucciones y datos asociados permanecen completamente en el chip y no están expuestos a una visualización externa. Pero una vez que los datos se transfieren fuera del chip se vuelven vulnerables a los ataques y la seguridad de un cálculo dado puede verse comprometida. Por ejemplo, un atacante podría obtener acceso a una memoria no protegida fuera del chip y examinar los datos almacenados, y podría detectar posiblemente información secreta. El atacante podría incluso modificar los datos almacenados y, de cualquier otra manera, subvertir un cálculo seguro.

Para evitar el acceso no autorizado y/o la manipulación de datos almacenados en una memoria externa, los datos pueden manejarse de acuerdo con un método criptográfico.

Los métodos y sistemas criptográficos se pueden usar para proteger la información de estado de un dispositivo de comunicación personal mediante el almacenamiento de forma segura la información de estado de varias maneras. Una forma puede ser al escribir una instantánea a la información del estado y calculando su suma de control, por ejemplo, mediante el uso de una función control de una sola vía. El resultado se almacena dentro de una localización de memoria del dispositivo a prueba de manipulaciones. Por lo tanto, si alguien intenta cambiar la información de estado, la suma de control del resultado no coincidirá con el valor de la suma de control almacenada en el dispositivo personal. Otra forma puede ser mediante el uso de un contador monotónico y persistente dentro del dispositivo, cada vez que se produce un cambio de estado, la información del estado se almacena junto con el valor actual del contador cifrado mediante una clave de dispositivo. Por lo tanto, puede que no sea posible cambiar la información de estado cifrada sin la clave.

US2003/0079122 A1 describe la idea de usar un dispositivo de almacenamiento resistente a la manipulación externa para almacenar información importante del estado. Se introduce la idea de contadores autenticados. La citada solicitud de patente US 2003/0079122 A1 describe que un contador autenticado puede implementarse en un identificador de seguridad resistente a la manipulación externa, como una tarjeta inteligente, que puede ser utilizado por el procesador seguro para proteger la integridad de su almacenamiento de estado. Para que esto funcione, el procesador seguro debe poder autenticar el identificador de seguridad externo. Para ello, la solicitud de patente US 2003/0079122 A1 describe el uso de una infraestructura de clave pública (PKI).

Sin embargo, una infraestructura de clave pública es bastante compleja de configurar porque implica coordinación y acuerdos entre fabricantes de dispositivos y fabricantes de identificadores de seguridad externos. También impone una cantidad de carga de procesamiento en los identificadores o memorias de seguridad externos.

Las máquinas de juego modernas trabajan con dinero. Por lo tanto, es necesario un sistema de seguridad que haga imposible manipular los datos de contabilidad para beneficio personal. El sistema de seguridad debe evitar una influencia en el proceso de juego que perjudique a los proveedores de máquinas de juego.

Los datos de contabilidad se deben almacenar en una memoria externa no volátil o con respaldo de batería debido a que, después de un apagado inesperado del sistema, el jugador quiere mantener su dinero reservado en su cuenta de juego y no quiere perderlo. Para evitar que cualquiera pueda leer los datos almacenados en esa memoria externa y manipular su contenido, los dispositivos de método criptográfico, como se indicó anteriormente, se implementan en máquinas de juego para proteger esencialmente el contenido de la memoria. Sin embargo, ninguno de los dispositivos y métodos introducidos logra resultados satisfactorios para proteger datos confidenciales en máquinas de juego.

El documento US 6,209,098 describe un circuito implementado dentro de un módulo de chip múltiple que comprende un primer chip de circuito integrado y un segundo chip de circuito integrado acoplados entre sí a través de una interconexión. Tanto el chip de circuito integrado primero como el segundo incluye un motor criptográfico acoplado a la interconexión y un elemento de memoria no volátil utilizado para contener información clave. Estos motores criptográficos se usan únicamente para cifrar la información saliente que se emite a través de la interconexión o para descifrar la información

entrante recibida de la interconexión. Esto se proporciona para prevenir un ataque físico fraudulento de información transmitida a través de la interconexión.

Existe la necesidad de proporcionar una seguridad de datos mejorada de los datos almacenados mediante el direccionamiento o rebasamiento de uno o más de los inconvenientes o desventajas asociados con las técnicas de seguridad convencionales, o de al menos proporcionar una alternativa útil a dichas técnicas de seguridad convencionales.

Un primer objeto de la presente invención es proporcionar un dispositivo para manejar datos confidenciales que evite los inconvenientes descritos anteriormente.
Un segundo objeto de la presente invención es proporcionar un método para transferir datos de manera segura entre una unidad de procesamiento y un dispositivo de memoria.

Un tercer objeto de la presente invención es mejorar un dispositivo de memoria para poder transferir datos de manera segura a un dispositivo conectado arbitrario.

Un cuarto objeto de la presente invención es proporcionar una máquina de juego con estándares de seguridad incrementados para el manejo de datos confidenciales dentro de la máquina.

El primer objeto se resuelve mediante un dispositivo para manejar datos confidenciales de acuerdo con la reivindicación 1. Las modalidades preferidas de la invención se establecen en las reivindicaciones dependientes.

Por consiguiente, el dispositivo comprende al menos un primer circuito integrado para formar una primera zona de confianza y un segundo circuito integrado para formar una segunda zona de confianza en donde:
- el primer circuito integrado comprende al menos una unidad de procesamiento segura adaptada para procesar datos confidenciales,
- el segundo circuito integrado comprende al menos un área de memoria persistente dentro de su zona de confianza para almacenar los datos confidenciales, en donde el segundo circuito integrado está separado del primer circuito integrado,
- la unidad de procesamiento del primer circuito integrado está adaptada para transferir los datos confidenciales de la primera zona de confianza a la segunda zona de confianza para almacenar de manera segura dichos datos en el área de memoria persistente de la segunda zona de confianza,
- el segundo circuito integrado está adaptado para transferir los datos confidenciales almacenados en su área de memoria persistente a la unidad de procesamiento de la primera zona de confianza,
- en donde el primer y el segundo circuito integrado comprenden medios criptográficos para transferir de manera segura los datos confidenciales basados en un método criptográfico simétrico mediante el uso de una clave segura, y
- en donde el segundo circuito integrado comprende medios para iniciar y procesar la generación de una nueva clave segura después del encendido.

El primer y el segundo circuito integrado forman una zona de confianza, cada uno de los cuales solo permite el acceso restringido de manera segura. El primer y el segundo circuito integrado están interconectados a través de un enlace de comunicación bidireccional. Tanto el primer como el segundo circuito integrado usan la misma clave de seguridad activa para descifrar/cifrar los datos transferidos a través del enlace de comunicación. En caso de que la generación de una nueva clave sea iniciada por el segundo dispositivo integrado, es decir, el dispositivo que guarda los datos secretos, la clave activa se reemplaza por la nueva clave generada en ambos lados del enlace de comunicación, es decir, en el primer y segundo circuito. Después de un intercambio de claves exitoso, la clave recién generada se convertirá en la clave activa actual.

Dado que la generación de claves se inicia y se procesa en el segundo circuito integrado, se garantiza un sistema absolutamente seguro. El dispositivo de la invención se orienta hacia un método de pirateo que rastrea la comunicación entre el primer circuito integrado y el segundo circuito integrado después del encendido y restaura el último estado del área de memoria del segundo circuito integrado con los datos rastreados después de otro encendido.

Preferiblemente, más de un primer circuito integrado puede estar interconectado con el segundo circuito integrado, cada uno adaptado de manera idéntica para actuar como se describió anteriormente. Todos los primeros circuitos integrados y el segundo circuito integrado usan la misma clave segura para el descifrado/cifrado.

En una modalidad preferida de la invención, los medios criptográficos están adaptados para transferir de forma segura una nueva clave generada desde el segundo circuito integrado al primer circuito integrado. Es decir, una clave recién generada se cifra con la clave segura activa antes de ser transmitida. Por lo tanto, una clave rastreada es ilegible sin la clave actual activa.

Es ventajoso que los circuitos integrados primero y segundo comprendan una clave secreta de encendido programable de una sola vez. La clave de encendido se utiliza para transferir de manera segura una nueva clave generada por el segundo circuito integrado después del encendido desde el segundo circuito integrado al primer circuito integrado. Sin dicha clave de encendido, sería necesario un intercambio de clave en texto sin formato después del encendido para proporcionar una clave de seguridad inicial para ambos lados. Una transmisión de clave en texto sin formato alegoriza un

grave problema de seguridad, ya que la clave podría ser fácilmente rastreada y utilizada para transferencias de datos adyacentes. Dicho riesgo se evita mediante el uso preferido de una clave de encendido.

Es ventajoso que la clave de encendido sea comparativamente grande, por ejemplo, una clave de 128 bits de longitud. Sin embargo, la longitud de la clave puede ser incluso mayor, por ejemplo, dos veces, tres veces o x veces de bits pueden usarse para la clave. La clave se almacena preferentemente en el primer y segundo circuito integrado en una memoria no volátil insusceptible mecánicamente. Además, es preferente adaptar la clave de encendido para que sea programable. En consecuencia, de vez en cuando es posible un cambio manual de la clave de encendido.
Es posible que la clave de encendido programable de una sola vez a la que se accede mediante el segundo circuito integrado se almacene en su área de memoria persistente. El área de memoria persistente es mecánicamente insensible, ya que está suficientemente protegida contra ataques de piratería física que intentan obtener acceso a dicha área de memoria.

En otra modalidad preferida de la invención, los medios para iniciar una nueva generación de claves están adaptados para iniciar una nueva generación de claves después de cada transferencia de datos confidenciales desde el primer circuito integrado al segundo circuito integrado. En consecuencia, un paquete de datos que contenga datos confidenciales que se escriben en el área de memoria del segundo circuito integrado se verá diferente cuando lo lea el primer circuito integrado de dicha área de memoria.

De forma alternativa o adicional, puede ser posible iniciar una nueva generación de claves después de cada transferencia de datos confidenciales desde el segundo circuito integrado al primer circuito integrado o después de cada transferencia de datos confidenciales en ambas direcciones.

Para proporcionar una clave generada aleatoriamente, que es difícil de estimar por un pirata informático, además, es preferible que los medios para iniciar una nueva generación de claves comprendan al menos un generador de números aleatorios para generar una clave sobre la base de un número aleatorio.

En una modalidad preferida, el área de memoria persistente del segundo circuito integrado es una memoria no volátil resistente a la manipulación indebida o una memoria con respaldo de batería resistente a la manipulación indebida. Ambas modalidades proporcionan una posibilidad de almacenamiento de datos que se mantendrá durante un evento de apagado. Por lo tanto, tanto los datos confidenciales almacenados como la clave de encendido están disponibles inmediatamente después de reiniciar el dispositivo.

El segundo objeto de la invención se resuelve mediante un método para transferir datos de forma segura entre al menos una unidad de procesamiento y un dispositivo de memoria de acuerdo con la reivindicación 8. De acuerdo con la invención, el método comprende el paso de descifrado/cifrado basado en una clave segura. Se utiliza un motor criptográfico simétrico, que es la misma clave segura que se usa en la unidad de procesamiento y en el dispositivo de memoria. Otros datos confidenciales se transfieren en forma cifrada. Los datos confidenciales se cifran según la clave segura en la unidad de procesamiento, se descifran en el dispositivo de memoria de recepción y se almacenan en el área de memoria segura. En caso de que se le indique a la unidad de procesamiento que lea datos confidenciales del dispositivo de memoria, los datos se cifran en el dispositivo de memoria en función de la clave segura, se transfieren a la unidad de procesamiento y se descifran para su procesamiento posterior con la ayuda de la clave segura.

Además, de acuerdo con la invención, el dispositivo de memoria inicia y genera una nueva clave para reemplazar la clave de seguridad activa actual. La ventaja esencial del método de la invención es que la memoria siempre define la clave activa. Por ejemplo, un atacante podría intentar acceder a un dispositivo de memoria mediante la simulación de una clave segura manipulada y, por lo tanto, podría escribir contenido de datos arbitrarios en el dispositivo de memoria. De acuerdo con la invención, la definición de la clave activa por el dispositivo de memoria protegerá al dispositivo contra tales métodos de ataque.

Es muy posible que el intercambio de claves de una nueva clave generada sea descifrado/cifrado por la clave de seguridad activa actual. Es decir, el dispositivo de memoria cifra una nueva clave generada en función de la clave activa actual y la transmite a la unidad de procesamiento. La unidad de procesamiento descifra la nueva clave cifrada recibida con la ayuda de la clave activa actual. Después de la transmisión exitosa de la clave, la clave activa actual se reemplaza por la nueva clave generada, que ahora se convierte en la clave activa actual utilizada para la transmisión de datos adyacente.

Preferentemente, una clave secreta de encendido programable de una sola vez se usa como una clave de seguridad inicial para cifrar/descifrar un primer intercambio de claves desde el dispositivo de memoria a la unidad de procesamiento después del encendido. Esto evita un intercambio de claves en texto sin formato después del encendido para garantizar claves de seguridad idénticas en ambos lados, es decir, unidad de procesamiento y dispositivo de memoria.

En una modalidad preferida de la invención, el dispositivo de memoria inicia una generación de claves y/o un intercambio de claves después de cada transferencia de datos confidenciales de la unidad de procesamiento al dispositivo de memoria. En consecuencia, después de cada operación de escritura en el dispositivo de memoria, se inicia un intercambio de claves. Un paquete de datos escrito en el dispositivo de memoria tendrá un aspecto diferente cuando se transmita desde el dispositivo de memoria a la unidad de procesamiento debido a diferentes claves activas.

El método de la invención se procesa ventajosamente mediante el dispositivo de la invención, de acuerdo con cualquiera de las reivindicaciones de la 1 a la 7. Obviamente, el método tiene las mismas ventajas y propiedades que se indicaron anteriormente en la parte de la descripción relacionada con el dispositivo, de acuerdo con cualquiera de las reivindicaciones de la 1 a la 7.

La invención está dirigida además a un circuito de acuerdo con la reivindicación 13. El circuito integrado para el intercambio seguro de datos comprende un área de memoria persistente, en particular una memoria no volátil, para almacenar datos confidenciales que comprenden medios de transferencia de datos para recibir datos confidenciales para almacenarlos en el área de memoria persistente desde al menos un dispositivo conectado y para enviar datos confidenciales almacenados en el área de memoria persistente de al menos un dispositivo conectado, medios criptográficos para descifrar/cifrar datos confidenciales recibidos/almacenados basados en un método criptográfico simétrico mediante el uso de una clave segura, y medios para iniciar la generación de una nueva clave para reemplazar una clave segura activa. El circuito está configurado para usar una sola primitiva criptográfica.

La lógica y/o los medios de criptografía pueden implementarse mediante hardware, software o una combinación de hardware y software.

De acuerdo con una modalidad preferida, los circuitos son de un tipo de acuerdo con los segundos circuitos integrados del dispositivo de la invención para el manejo de datos confidenciales. Además, la circuitería está adaptada para realizar el método de acuerdo con cualquiera de las reivindicaciones de la 8 a la 12. Las ventajas y propiedades preferidas de los circuitos son obviamente idénticas a las explicaciones anteriores. Por lo tanto, una descripción repetida no es esencial.

Por último, la presente invención está relacionada con una máquina de juego que comprende un dispositivo o un circuito de acuerdo con una de las modalidades mencionadas anteriormente. La máquina de juego trata con una variedad de datos confidenciales que deben protegerse contra ataques de piratería. Los datos confidenciales que valen el mecanismo de protección se refieren, preferentemente a al menos uno de los datos de contabilidad, balance de dinero, margen de beneficio, número de juegos, número de juegos ganados, números de transacciones, etc. Por lo tanto, los datos confidenciales están protegidos por el dispositivo de acuerdo con cualquiera de las reivindicaciones de la 1 a la 7 y/o el método según cualquiera de las reivindicaciones de la 7 a la 12 y/o el circuito integrado para el manejo de datos confidenciales de acuerdo con las reivindicaciones 13, 14.

En una modalidad particular de la presente invención, la unidad de procesamiento del primer circuito integrado está adaptada para controlar la máquina de juego y los datos confidenciales almacenados en el área de memoria del segundo circuito integrado incluyen al menos un número de transacción que se usa por la unidad de procesamiento para validar los datos de contabilidad. Los datos de contabilidad se almacenan preferentemente en un área/dispositivo de memoria adicional. Alternativamente, podría almacenarse en la memoria integrada en el segundo circuito integrado.

Es particularmente preferible que el número de transacción caracterice el número de transacciones de datos de contabilidad/dinero procesado dentro de la máquina de juego. El número de transacción se incrementa automáticamente después de cada transacción.

En este contexto, es concebible que la unidad de procesamiento comprenda al menos un generador de números de transacción para generar un número de transacción después de cada juego o un evento que lleve a un cambio de información relacionada con el juego. En lugar de incrementar el número de transacción, se puede usar un número de transacción que se genera aleatoriamente.

La invención se describirá con mayor detalle a continuación, a modo de ejemplo no limitativo, con referencia a las modalidades que se muestran en los dibujos.

Figura 1: una representación esquemática del dispositivo de la invención para el manejo de datos confidenciales

Figura 2: una primera tabla que muestra un posible escenario de piratería,

Figura 3: una segunda tabla que muestra otro escenario de piratería,

Figura 4: un primer diagrama de flujo que representa una primera implementación del método de la invención,

Figura 5: un segundo diagrama de flujo que representa una segunda implementación del método de la invención,

Figura 6: una vista lateral en perspectiva de una máquina de juego, de acuerdo con la presente invención, y

Figura 7: un diagrama del sistema, de acuerdo con la máquina de juego en la Figura 6.

Las máquinas de juego trabajan con dinero. Esto requiere un sistema de seguridad que debería imposibilitar la manipulación de los datos de contabilidad para beneficio personal. El sistema de seguridad debe evitar una influencia en

el proceso de juego que perjudique a los proveedores de máquinas de juego. Los datos de contabilidad se deben almacenar en una memoria externa no volátil o con respaldo de batería debido a que, después de un apagado inesperado del sistema, el jugador quiere mantener su dinero reservado en su cuenta de juego y no quiere perderlo.

Para evitar que cualquiera pueda leer los datos almacenados en esa memoria externa y manipular su contenido, es esencial un motor de cifrado simétrico que haga que el contenido de la memoria sea ilegible para cualquiera que no conozca el algoritmo de cifrado y la clave de cifrado. En consecuencia, es imposible manipular activamente los datos de contabilidad sin esa información.

Los ataques de piratería activa significan llenar la memoria externa con datos corruptos propios. Debido a que sin el conocimiento del sistema de cifrado y la clave de cifrado, la unidad de procesamiento no entenderá los datos dañados. Pero todavía existe un agujero de seguridad en este sistema mediante la manipulación pasiva de la memoria.

Como se mencionó anteriormente, el sistema actual es susceptible al seguimiento pasivo de datos cifrados. Incluso sin conocer el significado de los datos cifrados, es posible corromper el libro al guardar los datos de la memoria mediante la reproducción de un estado válido del pasado en la memoria. Estos datos, que son datos correctamente cifrados, pueden ser descifrados por la unidad de procesamiento. Esto permite el siguiente escenario de manipulación. Alguien inserta dinero en una máquina de juego y rastrea el estado de todas las memorias externas cifradas. Esto se puede hacer mediante el seguimiento de la transferencia de datos o la lectura del contenido de la memoria si es posible. Después de perder el dinero a través del juego, puede ser posible reproducir el estado anterior al reemplazar el contenido cifrado de todas las memorias externas con los datos rastreados. Así, se pueden restaurar los créditos perdidos y la persona puede seguir apostando sin insertar un poco de dinero extra.

Para evitar tal manipulación de los datos de juego, se agrega información de validación a los datos cifrados que indicará si los datos cifrados son válidos o no válidos. Por lo tanto, se puede crear un número de transacción como información de validación, que cambia cada juego y es cifrado y se adjunta junto con los datos de contabilidad. Si alguien toma una instantánea del sistema es inútil porque la unidad de procesamiento notará que los datos son "antiguos", es decir, que pertenecen a un estado anterior y que actualmente ya no son válidos. Este sistema sería intangible, es decir, propenso a ataques si la CPU tuviera una memoria no volátil en su interior, lo que puede mantener el número de transacción después de un apagado. Una memoria no volátil dentro de la unidad de procesamiento sería inaccesible y defendida de ataques de piratería.

Sin embargo, debido al hecho de que una memoria interna no volátil, es decir, en la unidad de procesamiento, difícilmente se puede realizar de manera rentable, puede requerirse una memoria externa para mantener el número de transacción. Esta memoria externa puede cumplir un par de características de seguridad, por lo que nadie puede rastrear y corromper estos datos. Estos requisitos pueden cumplirse fácilmente mediante el dispositivo, el método o los circuitos integrados, de acuerdo con la presente invención.

La Figura 1 muestra una vista esquemática del dispositivo de la invención 1 para manejar datos confidenciales como el número de transacción mencionado anteriormente. Una clave compartida K se usa para asegurar la comunicación entre un ASIC 10 primario, que comprende una unidad de procesamiento 11, y el ASIC secundario 20, que comprende un área de memoria no volátil e insensible 21.

El ASIC primario 10 comprende además un generador de números de transacción 12 y un módulo de cifrado 13. El generador de números de transacción 12 crea un nuevo número de transacción cada vez que el programa del juego, que se opera mediante el ASIC 10, cambia o se produce un evento relevante. El número de transacción está adjunto y cifrado junto con los datos de contabilidad 15 por el módulo de cifrado 13. El paquete de datos cifrados se almacena en un dispositivo de almacenamiento conectado. Para mantener el número de transacción válido actual durante un apagado del dispositivo/máquina de juego, el número de transacción se transmite ventajosamente al segundo ASIC 20 para almacenarlo en el área de memoria no volátil 21. Un aspecto ventajoso es que las medidas proporcionadas de acuerdo con la invención pueden permitir que el área de memoria no volátil 21 sea comparativamente pequeña.

Los comandos Lectura 31 y Escritura 32 pertenecen a un protocolo 30 que se utilizará entre los ASIC 10, 20 y se utilizan para escribir el número de transacción en el área de memoria persistente 21 del ASIC secundario 20 y para leer el número de transacción del área de memoria persistente 21. Cada transmisión entre ambos ASIC 10, 20 está asegurada por algoritmos criptográficos de clave simétrica ejecutados por los motores de descifrado/cifrado 14, 22 de los respectivos ASIC 10, 20. En detalle, en el presente ejemplo se usa un algoritmo DES simétrico basado en una clave compartida dedicada K. El ASIC 10 primario puede enviar comandos de protocolo al ASIC 20 secundario y el ASIC 20 secundario responde al ASIC 10 primario enviando respuestas a los comandos.

Además, el dispositivo 1 en el presente ejemplo comprende y trabaja con una clave secreta de encendido programable de una sola vez K', que es utilizada por ambos motores 14, 22 como una clave de seguridad de arranque inicial. Dicha clave de encendido K' está programada en la unidad de procesamiento 11 y en el área de memoria 21 y es accesible por los respectivos motores 14, 22. Esta clave K' se usa como una clave activa actual para intercambiar una nueva clave K generada para la siguiente transferencia de datos después del encendido. Después de transmitir con éxito una clave K

recién generada al ASIC 10, la clave de encendido K' como clave activa para cifrar/descifrar se reemplaza por la nueva clave K que se convierte ahora en la clave activa actual K.

Esta clave K puede cambiarse después de cada transferencia de datos. Alternativamente, la clave K puede cambiarse después de que se hayan realizado varias acciones de transferencia de datos. En consecuencia, un paquete de datos que se escribe en la memoria segura tendrá un aspecto diferente cuando lo lea la unidad de procesamiento. Ventajosamente, puede usarse una clave grande de 128 bits, por ejemplo.

De acuerdo con un aspecto ventajoso de la invención, el cambio de clave es iniciado por el ASIC 20, es decir, la segunda zona de confianza que está adaptada para almacenar los datos confidenciales dentro del área 21 de memoria persistente. La generación de claves en el presente ejemplo se basa en un generador de números aleatorios 23 integrado en ASIC 20 y conectado al motor 22 para proporcionar una nueva clave segura K generada.

La importancia de un aspecto ventajoso de la presente invención, es decir, que un cambio de clave es iniciado por ASIC 20, se explicará mediante los siguientes dos escenarios representados por las tablas que se muestran en las Figuras 2 y 3.

La Figura 2 muestra una modalidad donde la generación de una nueva clave es iniciada por ASIC 10, es decir, la primera zona de confianza. En la línea 1 de la tabla, se muestra un evento de "Encendido" y ambos motores de descifrado/cifrado 14, 22 de ASIC 10, 20 comienzan con la clave de encendido que es "abc". En el siguiente paso, línea 2, "Cambio de clave", ASIC 10 inicia la generación de una nueva clave "xyz" y transmite la clave "xyz" cifrada con la clave "abc" a ASIC 20, en particular al motor 22. El paso "Clave cambiada" significa un intercambio de claves exitoso en donde la clave de encendido "abc" se reemplaza por la nueva clave "xyz".

En la línea 4, en el paso "Escritura de datos", el generador 12 de ASIC 10 genera un nuevo número de transacción "1", cuyo número de transacción se debe almacenar en el área de memoria 21 de ASIC 20. Por lo tanto, el número "1" se transmite al ASIC 20 cifrado con la clave "xyz" y se almacena en la memoria (última columna de la tabla que se muestra en la Figura 2). La transmisión de datos se inicia en la generación ASIC 10 de la nueva clave "def", cuya nueva clave "def" se intercambia de acuerdo con los pasos antes mencionados "Cambio de Clave" y "Clave Cambiada". Por el contrario, el paso "Lectura de datos" no inicia un cambio de clave.

Hasta el primer evento de apagado en la tabla, un número de transacción "10" se almacena en el área de memoria 21. Un pirata informático puede capturar la secuencia de comunicación 200 entre ASICS 10, 20 a partir del primer evento de encendido.
Cuando se reinicia el dispositivo (segundo evento de encendido en la línea 11), la secuencia rastreada 200 podría usarse para restaurar el área de memoria 21 con el número de transacción respectivo de la secuencia de comunicación rastreada anteriormente. Dado que la generación de claves fue iniciada por ASIC 10, el ASIC 20 actuará de acuerdo con la secuencia de comunicación capturada 200. ASIC 20 verá datos válidos porque el primer cambio de clave es aceptable, por lo que el área de memoria 21 se puede restaurar con el número de transacción no válido "2".

Sin embargo, dado que ASIC 10 utiliza una nueva clave generada "ghi" después del segundo evento de encendido, cuya nueva clave generada "ghi" no coincide con la clave antigua "xyz" de la secuencia de comunicación capturada 200, el número de transacción transmitido "2" no puede ser cifrado por el motor 14 de ASIC 10. Esto conducirá a un estado de "datos no válidos" en la unidad de procesamiento 11. Desafortunadamente, dicho estado no válido se corregirá con un tercer encendido, ya que ambos motores 14, 22 volverán a arrancar con la clave de encendido "abc". El área de memoria 21 de ASIC 20 verá datos válidos, en particular una transacción válida.

Un cambio de clave iniciado por el ASIC 20 puede evitar un ataque de piratería tal como se puede ver en la tabla de la Figura 3. La primera secuencia de comunicación 300 entre los ASIC 10, 20 es similar a la Figura 2, sin embargo, un intercambio de clave, representado en los pasos "Cambio de clave" y "clave cambiada", es iniciado por ASIC 20. Según lo indicado por una secuencia de procesamiento 300, un número de transacción "24" se almacena en el área de memoria 21 del ASIC 20.

Si se pretende que una secuencia de procesamiento rastreada 300 se use para restaurar el contenido de datos del área de memoria 21, tal intento no podrá acceder al área de memoria 21. ASIC 10 genera inmediatamente una nueva clave "ghi" después del segundo evento de encendido. Por lo tanto, el motor 22 de ASIC 20 no puede cifrar el contenido de datos antiguos de la secuencia 300 que se presenta en un intento de ataque en la línea de comunicación entre ASIC 10, 20. El contenido del área de memoria 21 permanecerá intacto o dará lugar a un evento de "Datos no válidos".

Las Figuras 4 y 5 muestran diferentes diagramas de flujo que indican dos posibles algoritmos de implementación del método de la invención que pueden ejecutarse en ASIC 20, por medio de un procedimiento de máquina de estados.

Después de un evento de "Encendido" en el paso 400, se generará una clave aleatoria de acuerdo con el paso 401. De acuerdo con un paso posterior "Primer Cambio de Clave" 402, la nueva clave se almacena en una celda de memoria 420 y se entrega a un módulo de "Cifrado de Clave Simétrica" 403. El módulo 403 es operativo para cifrar la nueva clave

mediante el uso de la clave activa actual, que es en ese momento la clave de encendido y transmite los datos cifrados a través de una interfaz de memoria 450.

La máquina de estado ahora permanece en el paso "Lectura/Escritura" 404, a la espera de que se ejecute un comando de Lectura/Escritura. Si se ejecuta un comando de Lectura, entonces, de acuerdo con el paso "Lectura de memoria" 405, el contenido de datos actual (número de transacción) se buscará en un área de memoria 460 seguido de la encriptación del contenido de datos, de acuerdo con el paso "Cifrado Simétrico" 406, mediante el uso de la clave almacenada en la celda "Clave Activa" 420, y la transmisión del contenido cifrado a través de una interfaz 450 al ASIC 10 primario.

Si se ejecuta un comando de Escritura, entonces, de acuerdo con el paso "Descifrado Simétrico" 407, los datos cifrados recibidos, que se recibieron a través de la Interfaz de Memoria 450, se descifrarán mediante el uso de la clave almacenada en la celda "Clave Activa" 420. Los datos descifrados (número de transacción) se almacenarán de acuerdo con el paso "Escribir memoria" 408 en el área de memoria 460.

Después de cada comando de Lectura/Escritura, se genera una nueva clave, de acuerdo con el paso "Generador de Claves Aleatorias" 409. De acuerdo con el paso "Cambio de Clave" 410, la clave recién generada se almacena en la celda de memoria 420 y la clave nueva anterior se almacena en la celda "Clave antigua" 440. De acuerdo con un paso posterior "Cifrado de Clave Simétrica" 411, la clave recién generada se cifra basándose en la nueva clave anterior almacenada en la celda "Clave antigua" 440 o la clave que se almacena en la celda "Clave OTP" 430. Los datos de clave cifrados se transmiten a través de la interfaz de memoria 450. Si la celda "Clave antigua" 440 está vacía, el sistema puede usar la clave de encendido almacenada en la celda "Clave OTP" 430 para el procedimiento de cifrado/descifrado. A continuación, la máquina de estados salta al paso 404, a la espera de un nuevo comando de Lectura/Escritura.

La Figura 5 muestra otro diagrama de flujo que sugiere un algoritmo implementado de la presente invención ligeramente diferente. Contrariamente a los pasos que se muestran en la Figura 4, el diagrama de flujo que se muestra se basa en un método recursivo que usa solo un paso "Cambio de clave" 500. Además, la lógica que monitorea si ya se ha generado una nueva clave también se implementa mediante el uso del módulo único "Cambio de Clave" 500 al comienzo del diagrama de flujo. Ambas implementaciones (Figuras 4, 5) realizarán funciones idénticas de acuerdo con el método de la invención. Sin embargo, el esfuerzo de codificación y la complejidad pueden reducirse mediante el uso del formulario de implementación de acuerdo con la Figura 5.

La Figura 6 muestra una modalidad preferida de una máquina de juego con un dispositivo integrado de acuerdo con la presente invención. La Figura 6 muestra un ordenador 84, que se monta en la carcasa y se conecta con una interfaz de pantalla 80 que puede incluir una pantalla táctil. El ordenador incluye una placa principal 86 que tiene un controlador, una memoria conectada a la placa principal para almacenar el software, un software almacenado en la memoria para operar la interfaz 80, controladores de software y un procesador principal.

La Figura 7 muestra un diagrama del sistema del ordenador 84. La placa principal 86 comprende una memoria de programa 88 que es un medio legible por el ordenador, una unidad de procesamiento principal 90 y RAM 92 conectadas en comunicación operativa. La relación entre la unidad de procesamiento 90 y el dispositivo de memoria externo 114 se refiere a la presente invención, en donde el dispositivo de memoria 114 y la unidad de procesamiento 90 están acoplados entre sí a través de la interfaz 450. El número de transacción mencionado anteriormente se almacena en el dispositivo de memoria 114. Se puede mencionar que la interfaz 450 puede ser cableada o, alternativamente, inalámbrica, en cuyo caso pueden estar comprendidos medios para la transmisión inalámbrica.

El ordenador 84 comprende además un controlador de entrada salida E/S 94. El controlador de E/S 94 se comunica con un panel de control 96, un controlador de interfaz de pantalla 98, una unidad de pantalla 100, un aceptador de monedas 102, un aceptador de billetes 104, un lector de tarjetas 106, un lector de boletos/impresora 108 y un circuito de sonido 110. El circuito de sonido 110 está en comunicación operativa con los altavoces 112.

El aceptador de monedas 102 y el aceptador de billetes 104 aceptan la divisa y comunican la cantidad aceptada al controlador de E/S 94. El lector de tarjetas 106 lee tarjetas de crédito, tarjetas de débito, tarjetas de regalo u otras tarjetas que tienen indicios electrónicos de valor monetario.

El lector de boletos 108 imprime boletos y recibos que revelan las ganancias de un jugador u otro resultado financiero. El lector de boletos 108 también recibe boletos que tienen indicios de valor monetario.

El circuito de sonido 110 está configurado para proporcionar una interfaz acústica para el usuario. Cada movimiento o acción por parte de un usuario puede dar como resultado un sonido particular, o instrucciones generadas por el ordenador 84. Los altavoces 112 emiten los sonidos al usuario.

Será fácilmente evidente para un experto en la técnica que los diferentes procesos descritos en el presente documento pueden implementarse, por ejemplo, por ordenadores de propósito general programados de manera apropiada, ordenadores de propósitos especiales y dispositivos informáticos. Típicamente un procesador, por ejemplo, uno o más microprocesadores, uno o más microcontroladores, uno o más procesadores de señales digitales, recibirá instrucciones,

por ejemplo, de una memoria o un dispositivo similar, y ejecutará esas instrucciones, y realiza de esta manera uno o más procesos definidos por esas instrucciones.

Un "procesador" significa uno o más microprocesadores, unidades de procesamiento central CPU, dispositivos informáticos, microcontroladores, procesadores de señales digitales, o dispositivos similares o cualquier combinación de estos.

REIVINDICACIONES

1. Un dispositivo para manejar datos confidenciales que comprende al menos un primer circuito integrado (10) para formar una primera zona de confianza y al menos un segundo circuito integrado (20), dicho segundo circuito integrado (20) que forma una segunda zona de confianza que comprende:
- un área de memoria persistente (21) para almacenar datos confidenciales y ubicarse dentro de dicha segunda zona de confianza;
- medios de transferencia de datos para recibir datos confidenciales de la unidad de procesamiento (11) del primer circuito integrado (10), en donde dicha área de memoria persistente (21) se adapta para almacenar los datos confidenciales recibidos a través de dichos medios de transferencia de datos, y en donde dichos medios de transferencia de datos se adaptan para enviar los datos confidenciales que se almacenan en el área de memoria persistente (21) a la unidad de procesamiento (11) del primer circuito integrado (10),
- medios criptográficos para descifrar/cifrar datos confidenciales recibidos/almacenados en base a un método criptográfico simétrico mediante el uso de una clave segura activa, y
- medios para iniciar y procesar la generación de una nueva clave segura después del encendido, para reemplazar la clave segura activa en el primer y segundo circuito integrado (10, 20).
en donde el primer circuito integrado (10) comprende
- al menos una unidad de procesamiento seguro (11) que se adapta para procesar datos confidenciales, en donde el primer circuito integrado (10) se separa del segundo circuito integrado (20);
- la unidad de procesamiento (11) del primer circuito integrado (10) que se adapta para transferir los datos confidenciales de la primera zona de confianza a la segunda zona de confianza para almacenar de manera segura dichos datos en el área de memoria persistente (21) de la segunda zona de confianza,
- en donde el primer circuito integrado (10) incluye medios criptográficos para transferir de forma segura los datos confidenciales en base al método criptográfico simétrico mediante el uso de la clave segura activa que es reemplazable por dicha nueva clave segura que se genera por el segundo circuito integrado (20) después del encendido.

2. El dispositivo de acuerdo con la reivindicación 1, en donde los medios criptográficos se usan para transferir de forma segura una nueva clave generada desde el segundo circuito integrado (20) al primer circuito integrado (10).

3. El dispositivo, de acuerdo con cualquiera de las reivindicaciones 1 o 2, en donde los circuitos integrados primero y segundo (10, 20) comprenden una clave secreta de encendido programable de una sola vez, dicha clave de encendido que se usa para transferir de manera segura desde el segundo circuito integrado al primer circuito integrado (10), dicha nueva clave segura que se genera por el segundo circuito integrado (20) después del encendido, en donde la clave de encendido programable de una sola vez en el segundo circuito integrado (20) se almacena preferentemente en su área de memoria persistente (21).

4. El dispositivo, de acuerdo con cualquiera de las reivindicaciones de la 1 a la 3, en donde los medios para iniciar una nueva generación de clave segura se adaptan para iniciar una nueva generación de clave segura después de cada transferencia de datos confidenciales desde el primer circuito integrado (10) al segundo circuito integrado (20) y/o después de cada transferencia de datos confidenciales desde el segundo circuito integrado (20) al primer circuito integrado (10).

5. El dispositivo, de acuerdo con cualquiera de las reivindicaciones de la 1 a la 4, en donde los medios para iniciar la generación de una nueva clave segura comprenden un generador de números aleatorios (23) para generar una clave segura sobre la base de un número aleatorio.

6. El dispositivo, de acuerdo con cualquiera de las reivindicaciones de la 1 a la 5, en donde el área de memoria persistente (21) del segundo circuito integrado (20) es una memoria no volátil resistente a la manipulación indebida o una memoria con respaldo de batería resistente a la manipulación indebida.

7. Un método para transferir de forma segura datos confidenciales de manera bidireccional entre al menos un primer y al menos un segundo circuito integrado que forma un dispositivo, de acuerdo con cualquiera de las reivindicaciones de la 1 a la 6, en donde el segundo circuito integrado (20) almacena los datos confidenciales recibidos en un área de memoria persistente (21), en donde se usa una clave segura activa para descifrar/cifrar datos confidenciales recibidos o datos confidenciales que se enviarán al primer y segundo circuito integrado (10, 20), y en donde el segundo circuito integrado (20) inicia y genera una nueva clave de seguridad después del encendido, para reemplazar la clave de seguridad activa en el primer y segundo circuito integrado (10, 20).

8. El método, de acuerdo con la reivindicación 7, en donde el intercambio de claves de la nueva clave generada desde el segundo circuito integrado (20) al primer circuito integrado (10) se encuentra descifrado/cifrado por la clave de seguridad activa.

9. El método, de acuerdo con cualquiera de las reivindicaciones 7 u 8, en donde se usa una clave secreta de encendido programable de una sola vez como una clave de seguridad inicial para cifrar/descifrar un primer

intercambio de claves desde el segundo circuito integrado (20) al primer circuito integrado (10) después del encendido.

10. El método, de acuerdo con cualquiera de las reivindicaciones de la 7 a la 9, en donde una generación de claves y/o un intercambio de claves se inicia por el segundo circuito integrado (20) después de cada transferencia de datos confidenciales desde el primer circuito integrado (10) al segundo circuito integrado (20) y/o del segundo circuito integrado (20) al primer circuito integrado (10).

11. Una máquina de juego que comprende un dispositivo, de acuerdo con cualquiera de las reivindicaciones de la 1 a la 6, que es capaz de realizar el método de acuerdo con cualquiera de las reivindicaciones de la 7 a la 10.

12. La máquina de juego, de acuerdo con la reivindicación 11, en donde la unidad de procesamiento (11) del primer circuito integrado (10) controla la máquina de juego y los datos confidenciales almacenados en el área de memoria (21) del segundo circuito integrado (20) que incluye al menos un número de transacción que es usado por la unidad de procesamiento (11) para validar los datos de contabilidad, en donde preferentemente la unidad de procesamiento (11) comprende un generador de número de transacción (12) para generar un número de transacción después de cada juego o un evento que conduce a un cambio de información relacionado con el juego.

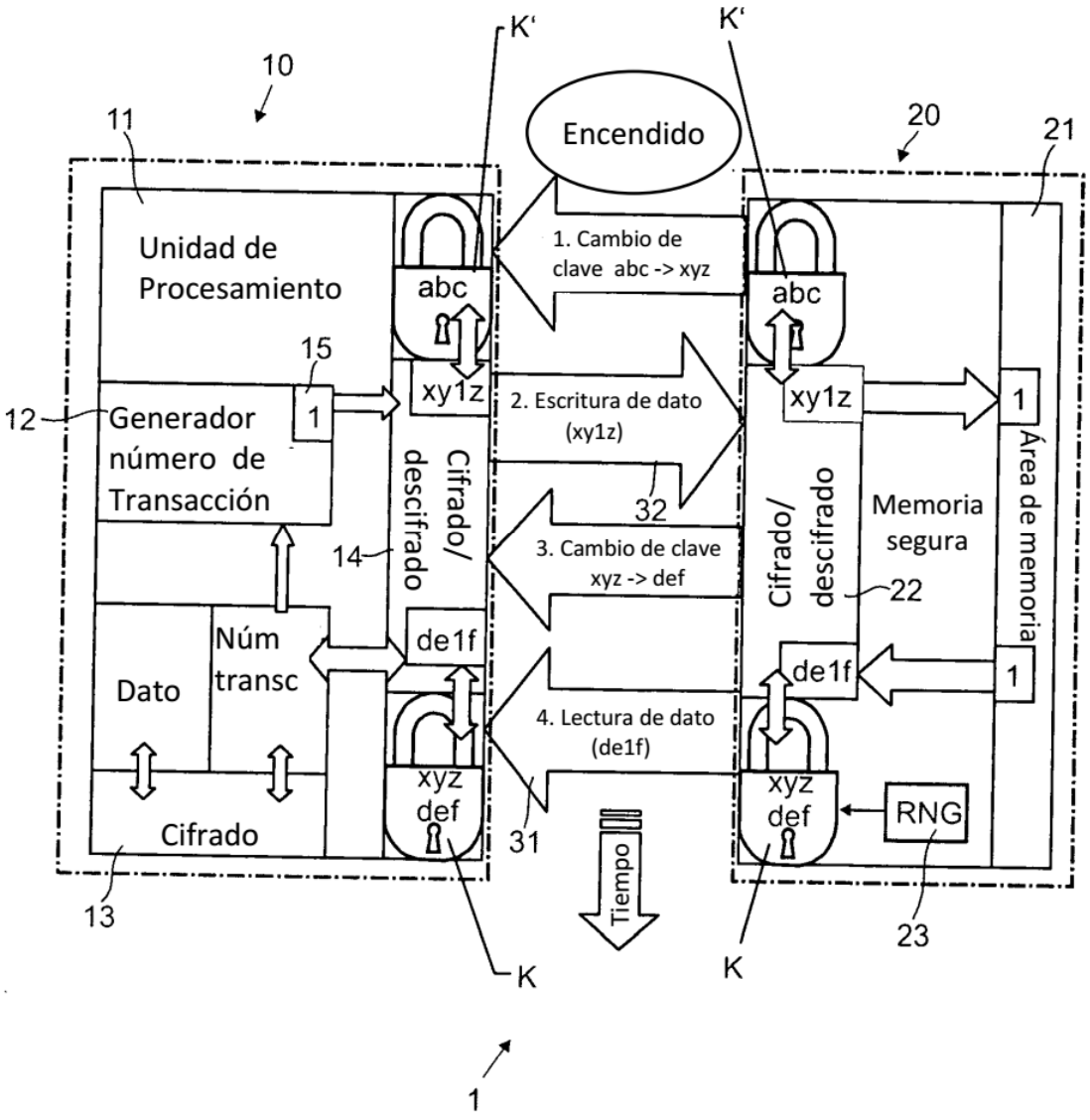
K'
K'
10
11
Encendido
20
21
Unidad de Procesamiento
abc
1. Cambio de clave abc -> xyz
abc
15
xy1z
2. Escritura de dato (xy1z)
xy1z
1
12
Generador número de Transacción
1
Cifrado/ descifrado
32
Memoria segura
Área de memoria
3. Cambio de clave xyz -> def
14
Cifrado/ descifrado
22
Núm transc
de1f
de1f
1
Dato
4. Lectura de dato (de1f)
xyz def
xyz def
RNG
31
Tiempo
Cifrado
13
K
K
23
1

FIG. 1

Paso	Número de transacción (Dato)	Procesador de clave	Línea de comunicación	Clave de memoria	Memoria	
Encendido	-	abd (defecto)		abd (defecto)	-	
Cambio clave	-	xyz	axbycz ->	abc	-	
Clave cambiada	-	xyz	-	xyz	-	
Escritura dato	1	xyz	xy1z ->	xyz	1	
Cambio clave	-	def	xdyezf ->	xyz	1	200
Clave cambiada	-	def	-	def	1	
Lectura dato	1	def	<- de1f	def	1	
Escritura dato	2	def	d2ef ->	def	2	
...	2 -> 10	...	...	...	10	
Apagado						
Encendido		abd (defecto)	-	abd (defecto)	10	
Piratería		(ghi)	axbycz ->	abc	10	
Piratería		(ghi)	-	xyz	10	
Piratería		(ghi)	xy1z ->	xyz	1	
Piratería		(mno)	xdyezf ->	xyz	1	200
Piratería		(mno)	-	def	1	
Piratería	Datos no válidos	mno	<- de1f	def	1	
Piratería		(mno)	de2f ->	def	2	
Apagado					2	
Encendido		abd (defecto)		abd (defecto)	2	
	...	...	...	...	...	

FIG. 2

Paso	Número de transacción (Dato)	Procesador de clave	Línea de comunicación	Clave de memoria	Memoria	
Encendido	-	abd (defecto)		abd (defecto)	10	
Cambio clave	-	abc	<- axbycz	xyz	10	300
Clave cambiada	-	xyz	-	xyz	10	300
Escritura dato	1	xyz	<- xy10z	xyz	10	300
Lectura dato	-	xyz	xy11z->	xyz	11	
Cambio clave	-	xyz	<- xdyezf	def	11	
Clave cambiada	1	def	-	def	11	
Lectura dato		def	<- de11f	def	11	
Escritura dato	2	def	de12f ->	def	12	
...	12 -> 24	...	...	...	24	
Apagado						
Encendido	-	abd (defecto)	-	abd (defecto)	24	
Piratería	-	abc	<- axbycz	(ghi)	24	300
Piratería		xyz	-	(ghi)	24	300
Piratería	10	xyz	<- xy10z	(ghi)	24	300
Piratería	11	xyz	Xy11z ->	ghi	Dato no válido	

FIG. 3

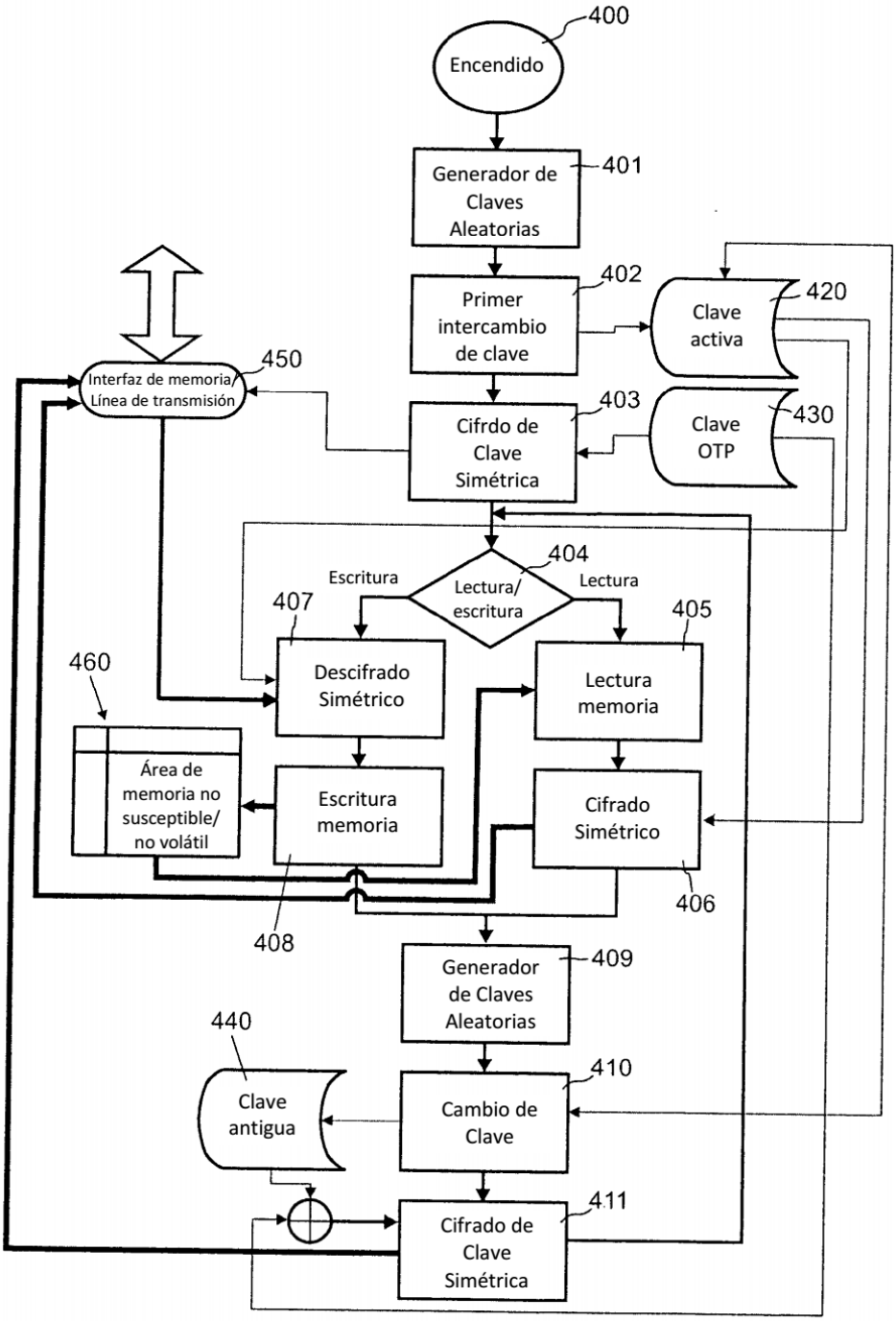
400
Encendido
401
Generador de Claves Aleatorias
402
Primer intercambio de clave
420
Clave activa
450
Interfaz de memoria/ Línea de transmisión
403
Cifrdo de Clave Simétrica
430
Clave OTP
404
Escritura
Lectura/ escritura
Lectura
407
405
460
Descifrado Simétrico
Lectura memoria
Área de memoria no susceptible/ no volátil
Escritura memoria
Cifrado Simétrico
406
408
409
Generador de Claves Aleatorias
440
Clave antigua
410
Cambio de Clave
411
Cifrado de Clave Simétrica

FIG. 4

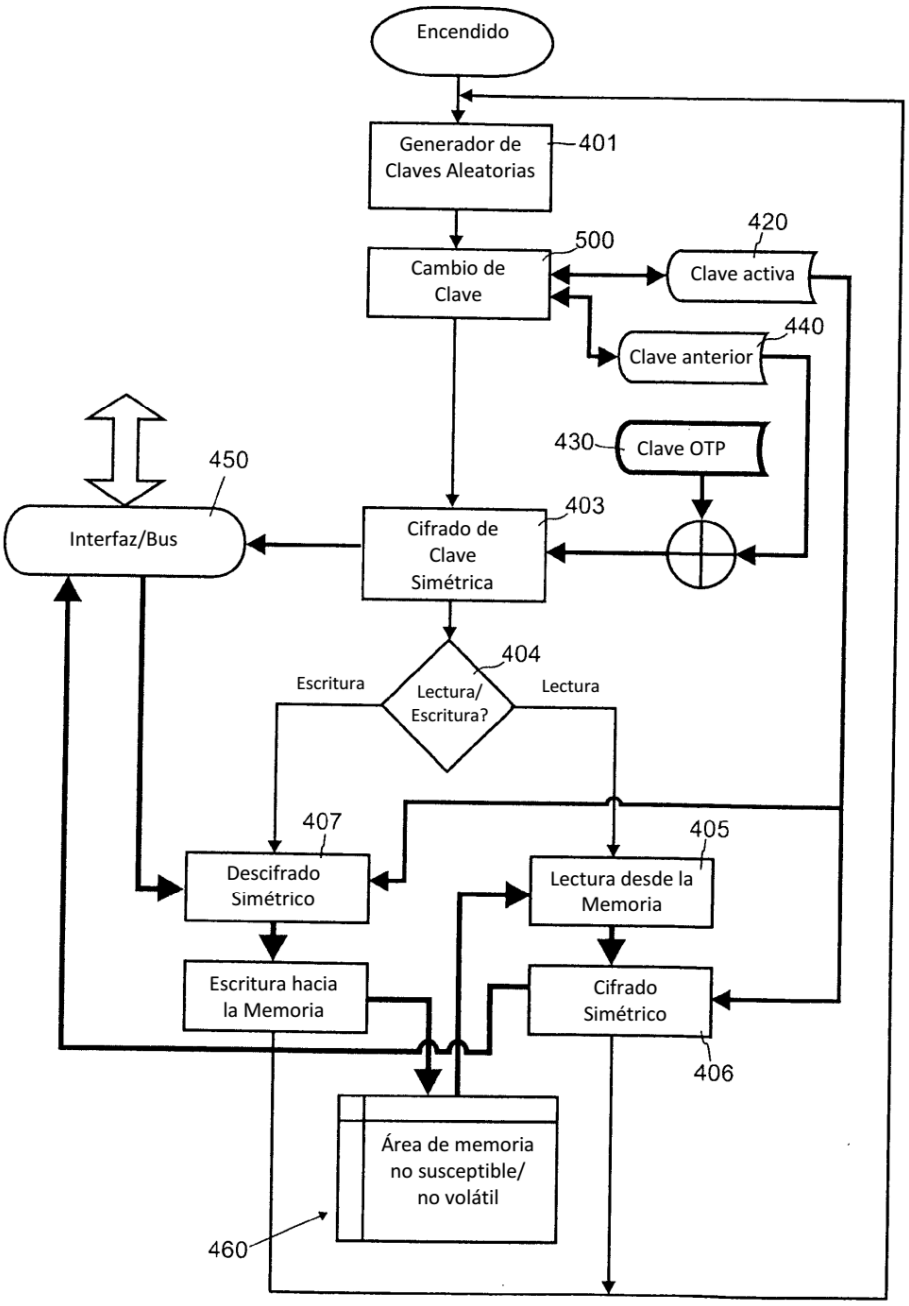
Encendido
Generador de Claves Aleatorias
401
Cambio de Clave
500
Clave activa
420
Clave anterior
440
Clave OTP
430
Interfaz/Bus
450
Cifrado de Clave Simétrica
403
Escritura
Lectura/ Escritura?
404
Lectura
Descifrado Simétrico
407
Lectura desde la Memoria
405
Escritura hacia la Memoria
Cifrado Simétrico
406
Área de memoria no susceptible/ no volátil
460

FIG. 5

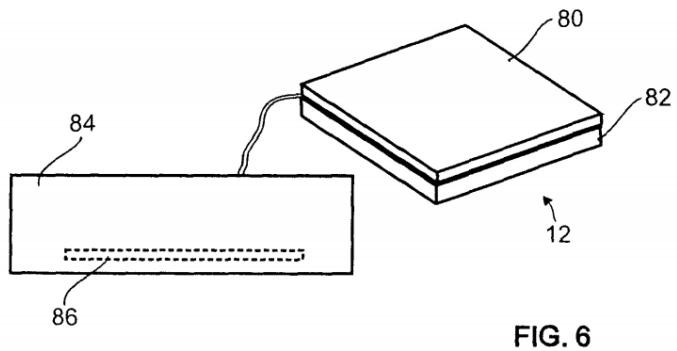
80
82
84
12
86

FIG. 6

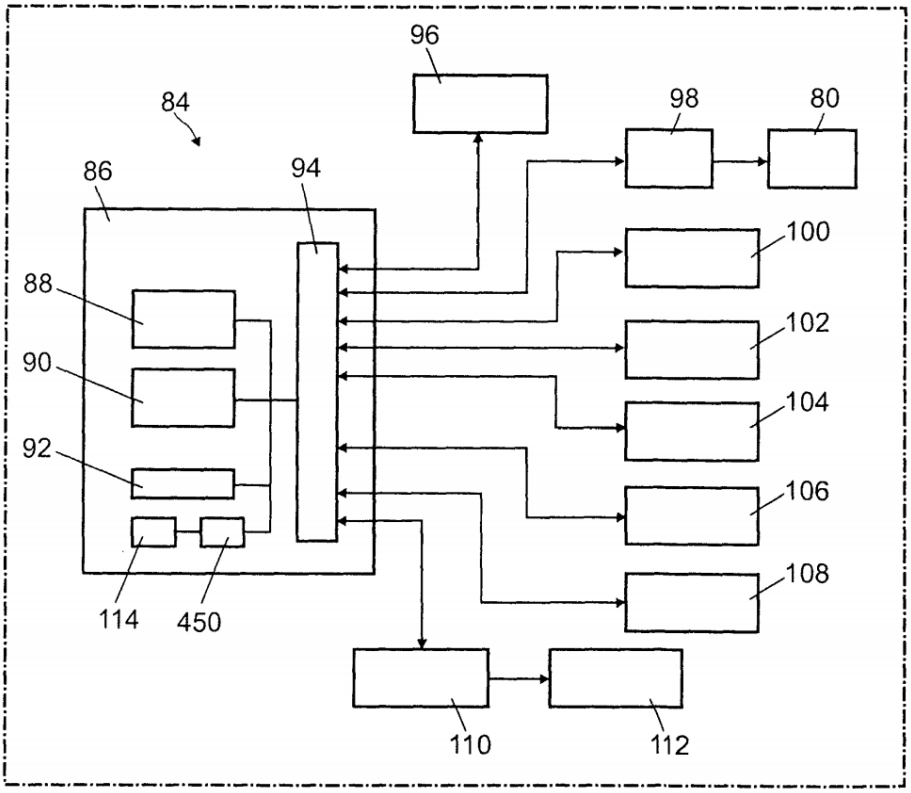
96
84
98
80
86
94
100
88
102
90
104
92
106
108
114
450
110
112

FIG. 7