(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 803 752**

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.11.2016 PCT/IB2016/056960**

(87) Fecha y número de publicación internacional: **24.05.2018 WO18091946**

(96) Fecha de presentación y número de la solicitud europea: **18.11.2016 E 16802147 (5)**

(97) Fecha y número de publicación de la concesión europea: **08.04.2020 EP 3378188**

(54) Título: **Protecciones frente a métodos y sistemas de copia no autorizada (anticlonado)**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.01.2021

(73) Titular/es:

PERMANENT PRIVACY LTD. (100.0%)
Sea Meadow House, Blackburne Highway, Road Town
Tortola, VG

(72) Inventor/es:

YUEN, PAK KAY

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Protecciones frente a métodos y sistemas de copia no autorizada (anticlonado)

ANTECEDENTES

1. Campo

Protecciones anticlonado.

2. Descripción de la técnica relacionada

Las tarjetas de seguridad se pueden copiar, incluso si están cifradas. Dichas tarjetas de seguridad pueden ser pasaportes y tarjetas de identidad, tarjetas de cajeros automáticos o tarjetas de crédito. También se pueden copiar dispositivos de hardware tales como descodificadores de TV y software incluyendo juegos, software de automatización, sistemas operativos o aplicaciones de software, incluso si están cifrados.

También puede ser difícil de detectar y/o invalidar la existencia de una copia no autorizada de, por ejemplo, una tarjeta de seguridad, o las actividades en las que se utiliza una copia no autorizada, de manera automática.

La solicitud de patente de los Estados Unidos 2008/063210 A1 describe la reintroducción de las llaves de cifrado para medios de almacenamiento extraíbles. Se recibe una solicitud de reintroducción para un medio de almacenamiento extraíble acoplado, donde el cifrado en el medio de almacenamiento extraíble acoplado utiliza una primera llave y donde la solicitud de reintroducción indica una segunda llave. Se accede a la primera llave y a la segunda llave en respuesta a la solicitud de reintroducción. La primera llave se utiliza para realizar el descifrado del medio de almacenamiento extraíble acoplado y la segunda llave se utiliza para realizar el cifrado del medio de almacenamiento extraíble acoplado.

La solicitud de patente de Estados Unidos 2013/054967 A1 describe un sistema o método de comunicación seguro que puede emplear un nivel constante de confianza entre los participantes y una entidad de gestión de la seguridad. Como parte del nivel constante de confianza, una política de comunicación puede provocar que los participantes soliciten la validación de la llave cada vez que el participante desea llevar a cabo una acción que requiere la utilización de una llave. De esta manera, el participante se puede comunicar regularmente con la gestión de seguridad, y esta comunicación regular se puede utilizar además para implementar la renovación de llaves y/o los procedimientos de sustitución.

COMPENDIO

En un aspecto, un objeto está protegido frente a una copia no autorizada proporcionando una cerradura para el objeto, produciendo una primera y segunda llave para la cerradura o produciendo una llave y a continuación separando la llave en una primera y segunda llave, almacenando la primera llave en el objeto, almacenando la segunda llave en una base de datos independiente del objeto, leyendo la primera y segunda llave, uniendo o combinando la primera y segunda llave entre sí, abriendo la cerradura con la primera y segunda llave, produciendo una llave y dividiéndola en una tercera y cuarta llave, utilizando la tercera y cuarta llave para cifrar de nuevo la información de cuenta con el fin de obtener un nuevo resultado del cifrado, donde el nuevo resultado del cifrado junto con la tercera y cuarta llave forman una nueva cerradura, donde la nueva cerradura invalida de manera efectiva la primera y segunda llave, sustituyendo la primera llave en el objeto por la tercera llave; y sustituyendo la segunda llave en la base de datos por la cuarta llave; donde la primera llave se sustituye en el objeto por la tercera llave y la llave temporal y la segunda llave se sustituyen en la base de datos por la llave temporal nueva y la cuarta llave, después de cada vez que se utiliza el objeto.

En diversos aspectos, el objeto es un pasaporte, una tarjeta bancaria, una tarjeta de viaje electrónica, un documento electrónico protegido, un descodificador de televisión inteligente, un descodificador de televisión por cable, un automóvil, una pieza de automóvil, una licencia de software o medios digitales.

En diversos aspectos, la tarjeta bancaria es una tarjeta de crédito, una tarjeta de cajero automático, una tarjeta de débito, una tarjeta de depósito o una tarjeta de pago electrónico.

En diversos aspectos, la tarjeta de viaje electrónica es una tarjeta Oyster o una tarjeta Octoplus.

En diversos aspectos, la licencia de software es una licencia de programa, una licencia de software de automatización, una licencia de sistema operativo o una aplicación de teléfono móvil.

En diversos aspectos, el medio digital es un juego, música, una película, un videoclip, la televisión o una serie de televisión en línea.

En un aspecto adicional, la primera y segunda llave se producen mediante cifrado de la información de cuenta y separando la información de cuenta cifrada en la primera y segunda llave, siempre que cada cifrado sea diferente.

En un aspecto adicional, la información de cuenta es la información de cuenta de un usuario del objeto.

En otro aspecto, un sistema protege un objeto frente a una copia no autorizada, donde el sistema incluye una memoria y un procesador acoplado a la memoria, donde el procesador se configura de modo que proporcione una primera y segunda llave o una llave separada en una primera y segunda llave, utilizar la primera y segunda llave para cifrar la información de cuenta con el fin de generar una nueva cerradura, almacenar la primera llave en el objeto, almacenar la segunda llave en una base de datos independiente del objeto, leer la primera y segunda llave, abrir la cerradura con la primera y segunda llave, producir una tercera y cuarta llave y generar una nueva cerradura, donde la nueva cerradura invalida la primera y segunda llave, sustituir la primera llave en el objeto por la tercera llave; y sustituir la segunda llave en la base de datos por la cuarta llave; donde la primera llave se sustituye en el objeto por la tercera llave y la llave temporal y la segunda llave se sustituyen en la base de datos por la llave temporal nueva y la cuarta llave, después de cada vez que se utiliza el objeto.

En otro aspecto más, un aparato protege un objeto frente a una copia no autorizada, el aparato incluye un motor de cifrado, un lector de llaves del objeto y un lector de llaves del emisor acoplados al motor de cifrado y configurados de modo que lean una llave del objeto y una llave del emisor respectivamente, un validador de llaves acoplado al motor de cifrado y configurado de modo que cifre o descifre la llave del objeto y la llave del emisor para validar la llave del objeto y la llave del emisor, un generador de llaves acoplado al motor de cifrado y configurado de modo que cifre o descifre la información de cuenta para generar un código de cifrado nuevo y diferente y divida el código de cifrado en la llave del objeto y la llave del emisor; y un actualizador de llaves acoplado al generador de llaves y configurado de modo que actualice la llave del objeto y la llave del emisor mediante la sustitución de la llave del objeto y la llave del emisor por una llave nueva del objeto y una llave nueva del emisor, respectivamente, y descarte la llave del objeto y la llave del emisor, donde la llave del objeto se sustituye por la llave nueva del objeto y la llave del emisor se sustituye por la llave nueva del emisor, después de cada vez que se utiliza el objeto.

Haciendo referencia a los dibujos anexos, se describe con detalle a continuación lo anterior y otras características y ventajas de la presente invención, así como también la estructura y funcionamiento de diversas realizaciones de la presente invención.

DESCRIPCIÓN BREVE DE LOS DIBUJOS

Los dibujos anexos, que se incorporan a la presente y forman parte de la memoria descriptiva, ilustran diversas realizaciones de la presente invención, y junto con la descripción, sirven además para explicar los principios de la invención y facilitar que una persona experta en la técnica relevante realice y utilice la invención. En los dibujos, números de referencia similares indican elementos idénticos o funcionalmente similares. Se obtendrán fácilmente una apreciación más completa de la invención y muchas de sus ventajas inherentes a medida que esta se comprende mejor haciendo referencia a la siguiente descripción detallada cuando se considera en conexión con los dibujos anexos, donde:

la figura 1 muestra un esquema de un sistema para proteger un objeto frente a una copia no autorizada de acuerdo con una realización;

la figura 2 muestra un diagrama de flujo de un método para proteger un objeto frente a una copia no autorizada de acuerdo con una realización;

la figura 3 muestra un esquema de un sistema para proteger un objeto frente a una copia no autorizada de acuerdo con una realización; y

la figura 4 muestra el hardware para utilizar con una realización.

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES PREFERIDAS

En la figura 1 se muestra un esquema de un sistema 100 para proteger un objeto frente a una copia no autorizada de acuerdo con una realización.

La invención se inspiró en el sistema de caja de seguridad utilizado por los bancos. Cuando se abre una caja de seguridad en un banco, el banco proporciona dos llaves. Una llave la guarda el cliente y la otra llave conocida como la “llave de guardia” la guarda el banco. Únicamente cuando las dos llaves se manipulan conjuntamente, se puede abrir la “cerradura” de la caja de seguridad.

Pregunta: ¿sería más seguro si el banco proporcionara dos nuevas llaves y cambiara la cerradura cada vez que se visita la caja de seguridad?

Respuesta: No sería práctico ni útil para el banco de la caja de seguridad proporcionar dos nuevas llaves y cambiar la cerradura en cada visita de un cliente.

No obstante, la versión electrónica de esta idea proporciona tanto seguridad como practicidad (facilidad de uso).

Se consideran objetos protegidos 10 tales como “pasaportes”, “tarjetas de identidad” y “tarjetas de crédito”, tales como aquellos mostrados en la figura 1. Para cada objeto protegido 10, el emisor 20 (banco, oficina de pasaportes, etc.) producirá dos llaves 30, 40 (contraseñas). Una se almacenará en el objeto 10 (en su banda magnética, por ejemplo) y el otro se almacenará en la base de datos 50 del emisor.

Para cada objeto protegido 10, tal como un pasaporte, tarjeta de identificación y tarjeta de crédito, se designará una “cerradura” 60 utilizando un cifrado de datos adecuado para la seguridad del objeto 10 en cuestión. La cerradura cifrada 60 servirá como una capa exterior invisible además de cualquier protección existente del objeto 10 (tal como un número PIN).

En el caso de una tarjeta de crédito, por ejemplo, la inserción en la máquina de lectura de tarjetas leerá las dos llaves 30, 40 en la cerradura “cifrada” del emisor. Cuando las dos llaves 30, 40 son correctas, estas son reconocidas por la cerradura “cifrada”, la tarjeta de crédito se considera auténtica y la cerradura se abre. Esto es invisible para el poseedor de la tarjeta y tiene lugar tan rápidamente que no ralentiza o afecta a la utilización de la tarjeta.

Todas las demás actividades asociadas, tales como la lectura del PIN y la transacción monetaria se pueden llevar a cabo como siempre.

El paso final y más importante: Después de que se completa la transacción monetaria y antes de devolver la tarjeta de crédito, la máquina de lectura de tarjetas (es decir, el emisor) produce dos llaves nuevas y una cerradura nueva. Una llave se almacena en el objeto en cuestión y la otra llave en la base de datos del emisor.

Supóngase que son copiados diversos “pasaportes”, “tarjetas de identidad” y “tarjetas de crédito” con intención delictiva. Cada uno de estos objetos copiados tendrá la misma llave 30, 40 que el objeto auténtico particular que se copió o clonó.

Cuando la tarjeta o el objeto auténtico se utiliza ahora, la cerradura y las llaves tanto en la tarjeta auténtica como en la base de datos del emisor cambiarán. Esto hará que todas las copias ilegales del objeto sean inútiles ya que la vieja llave en el objeto copiado no tiene forma de coincidir con la llave nueva en la base de datos del emisor. Ninguna copia o clon abrirá la nueva cerradura cifrada.

En esta situación, todas las copias no autorizadas de objetos quedarán inutilizadas de manera automática. Tanto los usuarios como el emisor no necesitan hacer nada para inutilizar las copias.

Detectar copias no autorizadas y/o detectar la utilización de copias ilegales es un problema de seguridad para muchas organizaciones tales como los bancos. Supóngase que son copiados y utilizados diversos “pasaportes”, “tarjetas de identificación” y “tarjetas de crédito” antes de que se utilice el objeto auténtico. En este caso, el objeto copiado no autorizado se utilizará con éxito.

No obstante, cuando se utilice el objeto auténtico después de la copia ilegal, el objeto auténtico no superará la cerradura cifrada debido a que la cerradura ya se ha cambiado. En este caso, se conoce que el objeto auténtico ha sido copiado y que ha habido una utilización ilegal de una copia. El poseedor del objeto auténtico contacta ahora con el emisor y se reinstalan llaves nuevas y una cerradura nueva de nuevo en el objeto auténtico para inutilizar todas las copias ilegales del objeto.

La capacidad de detección de la invención es particularmente útil para duplicados ilegales de pasaportes y tarjetas de identificación y elimina los fraudes de identidad de esta clase. No importa cuántos pasaportes y tarjetas de identidad se dupliquen, uno y solo uno se puede utilizar una vez. Todas las demás copias son inutilizadas de manera automática. Cuando el auténtico se utiliza o se recupera del emisor, todas las copias ilegales quedarán expuestas y pueden ser descubiertas por parte del emisor.

Probar a un banco que existe una copia ilegal de una tarjeta monedero o tarjeta de crédito ha sido relativamente difícil en el pasado. Con la presente invención, cuando se utiliza la copia no autorizada de una tarjeta monedero (o tarjeta de crédito), se cambia tanto la llave en la tarjeta copiada como la llave en la base de datos del emisor.

No obstante, la llave en la tarjeta auténtica, que es la llave anterior, no abrirá la cerradura cifrada del sistema. Esto se puede utilizar como prueba para el banco de que hay en circulación una copia ilegal de la tarjeta. El emisor podrá identificar que la tarjeta auténtica aún tiene la llave anterior y por lo tanto no se ha utilizado.

Todos los descodificadores de televisión y el software tal como juegos, licencias de software de automatización, sistemas operativos y aplicaciones de software se pueden proteger de una manera similar.

Con el fin de reducir el fraude de identidad y proporcionar tranquilidad, los objetos protegidos tales como tarjetas monedero y tarjetas de crédito se deberían utilizar de manera tan regular como sea posible. En muchos casos, una simple comprobación del saldo hará el trabajo, ya que esto activará la producción automática de llaves nuevas.

El robo de identidad se reducirá en gran medida si las personas comprueban diariamente sus objetos protegidos. Incluso se puede desarrollar un lector USB de tarjetas en línea, de modo que las personas puedan comprobar sus tarjetas en casa en su PC.

En el pasado ha sido difícil identificar el original de un documento electrónico (o transmitido electrónicamente), tal como un contrato electrónico, un documento legal, etc.

La invención también se puede utilizar para identificar el documento electrónico original colocando una llave en el documento electrónico y considerar el documento electrónico como un objeto protegido. Todos los mismos documentos con una llave diferente se pueden considerar como una copia del original.

El proceso de verificación del documento electrónico original se puede realizar mediante un programa.

El programa lee la llave del documento y se conecta al sitio del emisor en internet, por ejemplo, para la segunda llave. Cuando se dispone de las dos llaves, el documento electrónico se puede verificar como original mediante la apertura de la cerradura.

En algunos casos, se puede disponer mediante cifrado que únicamente se pueda leer con éxito el documento electrónico original.

Proteger múltiples copias de un objeto protegido no es un problema. Supóngase que se quieren proteger tres tarjetas de cajero automático (p. ej., tarjeta1, tarjeta2, tarjeta3) de la misma cuenta. Todo lo que se necesita es generar tres pares de llaves asociadas con las tres tarjetas de cajero automático.

Por ejemplo, el primer par de llaves se utiliza para proteger la tarjeta1. Una llave se almacena en la tarjeta1 y la otra llave se almacena en la base de datos de la cuenta a la que hace referencia la tarjeta1.

En la situación de esta invención esta es utilizada ampliamente, por ejemplo, utilizada por sistemas operativos tales como Microsoft Windows, Apple Mac e Internet. La mayoría de los objetos electrónicos y digitales que incluyen software, documentos electrónicos y juegos se pueden proteger a una escala global. Se puede lograr en cierto grado un control global frente a la copia no autorizada.

Entidades básicas de la invención

Dos llaves (o una llave dividida en dos partes):

Una llave se almacena en el objeto protegido y la otra se almacena en la base de datos del emisor.

Cerradura cifrada:

El usuario puede definir la cerradura o cifrado dependiendo de la aplicación particular. Puede ser un cifrado unidireccional (sin descifrado) o un cifrado bidireccional (ambos cifrado y descifrado disponibles), o una combinación de ambos:

Proceso de verificación:

El proceso de verificación se puede considerar como la apertura de la cerradura cifrada y puede estar definida por el usuario dependiendo del cifrado que se utilice. Por ejemplo, la cerradura se considera abierta cuando se logran los mismos resultados de cifrado con las dos llaves. En algunos casos, la cerradura se considera abierta cuando se logran los mismos resultados de descifrado. A veces, se puede utilizar una combinación de estas.

Generador de llaves:

Un generador de llaves es un mecanismo (hardware o software) que puede generar dos llaves nuevas y generar una nueva cerradura cifrando la información de cuenta cada vez que se utilizan o seleccionan las llaves asociadas con el cifrado.

Existen diversas formas de implementar la invención. Para otro ejemplo de implementación muy simple considérese la situación de la tarjeta bancaria.

Las dos llaves y la cerradura se pueden generar de la siguiente manera:

El generador de llaves puede generar una llave temporal o una contraseña y mantener el cambio de contraseña cada vez para cifrar la siguiente información de cuenta del usuario en la base de datos del banco y posteriormente almacenar la llave temporal:

John Smith, 04929 1234 5678, BancoXX

y el resultado cifrado puede ser:

01 69 f3 2b 10 88 40 ca 18 22 48 90 1d d4 1a c8 ca d9 df fa d3 68 8c 6f 1b bb fb 51 fc fc 1a e7 43 5e 1d d9 86 fd ca 5a d2 1c bf 6d c7 26 9c 56 78 8b bd af 35 63 bf 92

Estos resultados de cifrado se pueden dividir en dos partes (es decir, como dos llaves)

Llave1=01 69 f3 2b 10 88 40 ca 18 22 48 90 1d d4 1a c8 ca d9 df fa d3 68 8c 6f 1b

Llave2= bb fb 51 fc fc 1a e7 43 5e 1d d9 86 fd ca 5a d2 1c bf 6d c7 26 9c 56 78 8b bd af 35 63 bf 92

Entonces la Llave1 se almacenará en la tarjeta bancaria y tanto la llave temporal como la Llave2 se almacenarán en la base de datos del banco.

El método de validación para este ejemplo simple será un descifrado simple de las dos llaves unidas con la llave temporal almacenada para recuperar la información del usuario y a continuación activar de nuevo el generador de llaves para generar llaves nuevas y una llave temporal nueva. En este caso, la primera y segunda llave actúan como la cerradura. La llave temporal puede ser cualquier cosa, un número o cadena relacionada con el tiempo o simplemente cualquier cadena aleatoria que sea diferente cada vez que se genera.

En la figura 2 se muestra un diagrama de flujo de un método 200 para proteger un objeto frente a una copia no autorizada de acuerdo con una realización. El objeto puede ser un pasaporte, una tarjeta bancaria, una tarjeta de viaje electrónica, un documento electrónico protegido, un descodificador de televisión inteligente, un descodificador de televisión por cable, un automóvil, una pieza de automóvil, una licencia de software o un medio digital. La tarjeta bancaria puede ser una tarjeta de crédito, una tarjeta de cajero automático, una tarjeta de débito, una tarjeta de depósito o una tarjeta de pago electrónico. La tarjeta de viaje electrónica puede ser una tarjeta Oyster o una tarjeta Octoplus. La licencia de software puede ser una licencia de programa, una licencia de software de automatización, una licencia de sistema operativo o una aplicación de teléfono móvil. El medio digital puede ser un juego, música, una película, un videoclip, la televisión o una serie de televisión en línea.

En una primera operación 202, se proporciona un generador de llaves para el objeto. En una segunda operación 204, se producen una llave temporal y una primera y segunda llave como una cerradura para el objeto. La primera y segunda llave se pueden producir cifrando la información de cuenta utilizando la llave temporal y separando la información de cuenta cifrada en la primera y segunda llave. La información de cuenta puede ser la información de cuenta de un usuario del objeto.

En una tercera operación 206, se almacena la primera llave en el objeto. En una cuarta operación 208, se almacenan tanto la llave temporal como la segunda llave en una base de datos independiente del objeto. En una quinta operación 210, se leen la primera y segunda llave. En una sexta operación 212, se unen la primera y segunda llave. En una séptima operación 214, se abre la cerradura mediante una coincidencia del descifrado en la primera y segunda llave unidas utilizando la llave temporal almacenada. En una octava operación 216, se producen una nueva llave temporal y una tercera y cuarta llave que forman la nueva cerradura. En una novena operación 218, se invalidan la primera y segunda llave con la cerradura nueva. En una 10.ª operación 220, la primera llave en el objeto se sustituye por la tercera llave. En una 12.ª operación 222, tanto la llave temporal como la segunda llave en la base de datos se sustituyen por la llave temporal nueva y la cuarta llave.

En la figura 3 se muestra un esquema de un sistema 300 para proteger un objeto frente a una copia no autorizada de acuerdo con una realización. El sistema incluye una memoria 302 y un procesador 304 acoplado a la memoria 302. El procesador 304 se configura para proporcionar un generador de llaves para el objeto, proporcionar una primera y segunda llave y una cerradura utilizando cifrado, almacenar la primera llave en el objeto, almacenar la segunda llave en una base de datos independiente del objeto, leer la primera y segunda llave, abrir la cerradura con la primera y segunda llave, producir una tercera y cuarta llave y una cerradura nueva, invalidar la primera y segunda llave con la nueva cerradura, sustituir la primera llave en el objeto por la tercera llave; y sustituir la segunda llave en la base de datos por la cuarta llave.

En la figura 4 se muestra un esquema de un aparato 400 para proteger un objeto frente a una copia no autorizada. El aparato 400 incluye un motor de cifrado 402. Un lector de llaves del objeto 404 y un lector de llaves del emisor 406 están acoplados al motor de cifrado 402 para leer una llave del objeto y una llave del emisor. El motor de cifrado 402 se configura para leer la llave del objeto y la llave del emisor y descifrarlas. Se acopla un validador de llaves 408 al

motor de cifrado 402 y se configura para cifrar o descifrar la llave del objeto y la llave del emisor con el fin de validar la llave del objeto y la llave del emisor.

Un generador de llaves 410 se acopla al motor de cifrado 402 y se configura para generar una llave temporal y cifrar la información de cuenta del usuario con el fin de generar un código de cifrado y dividirlo en la llave del objeto y la llave del emisor. Un actualizador de llaves 412 se acopla al generador de llaves 402 y se configura para actualizar la llave del objeto y la llave del emisor mediante la sustitución de la llave del objeto y la llave del emisor por una llave del objeto nueva y una llave del emisor nueva y una llave temporal nueva, respectivamente, y descartar la llave del objeto y la llave del emisor.

Las realizaciones se pueden implementar en hardware informático (aparato informático) y/o en software, tal como (en un ejemplo sin carácter limitante) en cualquier ordenador que pueda almacenar, recuperar, procesar y/o generar datos y/o comunicarse con otros ordenadores. Los resultados producidos se pueden presentar en una pantalla del hardware informático. Un programa/software que implemente las realizaciones se puede grabar en un medio legible por ordenador que comprende un medio de grabación legible por ordenador. El programa/software que implementa las realizaciones también se puede transmitir a través de un medio de comunicación de transmisión. Ejemplos del medio de grabación legible por ordenador incluyen un aparato de grabación magnético, un disco óptico, un disco magnetoóptico y/o una memoria semiconductora (por ejemplo, RAM, ROM, etc.). Ejemplos de aparatos de grabación magnéticos incluyen un dispositivo de disco duro (HDD), un disco flexible (FD) y una cinta magnética (MT). Ejemplos de disco óptico incluyen un DVD (disco versátil digital), un DVD-RAM, un CD-ROM (disco compacto – memoria de solo lectura) y un CD-R (grabable)/RW. Un ejemplo de medio de comunicación incluye una señal de onda portadora.

Asimismo, de acuerdo con un aspecto de las realizaciones, se puede proporcionar cualesquiera combinaciones de las características, funciones y/u operaciones descritas.

Lo anterior ha descrito los principios, realizaciones y modos de operación de la presente invención. No obstante, la invención no se debería entender como que está limita a las realizaciones particulares descritas anteriormente, ya que estas se deberían considerar como que son ilustrativas y no restrictivas. Se debería apreciar que aquellos que son expertos en la técnica pueden realizar variaciones en esas realizaciones sin alejarse del alcance de la presente invención.

Aunque se ha descrito anteriormente una realización preferida de la presente invención, se debería sobreentender que se ha presentado únicamente a modo de ejemplo y sin carácter limitante. Por tanto, la amplitud y el alcance de la presente invención no deberían estar limitados por la realización ejemplar descrita anteriormente.

Obviamente, habida cuenta de las enseñanzas anteriores se pueden realizar numerosas modificaciones y variaciones de la presente invención. Por lo tanto, se debe sobreentender que la invención se puede llevar a la práctica de otro modo distinto al descrito de manera específica en la presente.

REIVINDICACIONES

1. Un método (200) para proteger un objeto (10) frente a una copia no autorizada, que comprende:

proporcionar un generador de llaves (410) para el objeto (10);

producir una primera y segunda llave (30, 40) y una cerradura (60) para la primera y segunda llave (30, 40);

almacenar la primera llave (30) en el objeto (10);

almacenar la segunda llave (40) y una llave temporal en una base de datos (50) independiente del objeto (10);

leer la primera y segunda llave (30, 40);

unir la primera y segunda llave (30, 40);

abrir la cerradura (60) mediante una coincidencia de descifrado en la primera y segunda llave (30, 40) unidas utilizando la llave temporal almacenada;

producir una llave temporal nueva, una tercera y cuarta llave y una cerradura nueva (60);

invalidar la primera y segunda llave (30, 40) con la nueva cerradura (60);

sustituir la primera llave (30) en el objeto (10) con la tercera llave; y

sustituir tanto la llave temporal como la segunda llave (40) en la base de datos (50) por la llave temporal nueva y la cuarta llave, donde

la primera llave (30) es sustituida en el objeto (10) por la tercera llave, y la llave temporal y la segunda llave (40) son sustituidas en la base de datos (50) por la llave temporal nueva y la cuarta llave, después de cada vez que se utiliza el objeto (10).

2. El método (200) de la reivindicación 1, donde el objeto (10) se selecciona del grupo compuesto por:

un pasaporte,

una tarjeta bancaria,

una tarjeta de viaje electrónica,

un documento electrónico protegido,

un descodificador de televisión inteligente,

un descodificador de televisión por cable,

un automóvil,

una pieza de automóvil,

una licencia de software, y

un medio digital.

3. El método (200) de la reivindicación 2, donde la tarjeta bancaria se selecciona del grupo compuesto por:

una tarjeta de crédito,

una tarjeta de cajero automático,

una tarjeta de débito,

una tarjeta de depósito, y

una tarjeta de pago electrónico.

4. El método (200) de la reivindicación 2, donde la tarjeta de viaje electrónica se selecciona del grupo compuesto por una tarjeta Oyster y una tarjeta Octoplus.

5. El método (200) de la reivindicación 2, donde la licencia de software se selecciona del grupo compuesto por una licencia de programa, una licencia de software de automatización, una licencia de sistema operativo y una aplicación de teléfono móvil.

6. El método (200) de la reivindicación 2, donde el medio digital se selecciona del grupo compuesto por:

un juego,

música,

una película,

un videoclip,

la televisión, y

una serie de televisión en línea.

7. El método (200) de la reivindicación 1, donde la primera y segunda llave (30, 40) se producen mediante cifrado de la información de cuenta con una contraseña relacionada con el tiempo o llave temporal y separando la información de cuenta cifrada en la primera y segunda llave (30, 40).

8. El método (200) de la reivindicación 7, donde la información de cuenta es la información de cuenta de un usuario del objeto (10).

9. Un sistema (100, 300) para proteger un objeto (10) frente a una copia no autorizada, que comprende:

una memoria (302); y

un procesador (304) acoplado a la memoria (302) y configurado para:

proporcionar un generador de llaves (410) para el objeto (10);

producir una primera y segunda llave (30, 40) y una cerradura (60) para la primera y segunda llave (30, 40);

almacenar la primera llave (30) en el objeto (10);

almacenar la segunda llave (40) y una llave temporal en una base de datos (50) independiente del objeto (10);

leer la primera y segunda llave (30, 40);

unir la primera y segunda llave (30, 40);

abrir la cerradura (60) mediante una coincidencia de descifrado en la primera y segunda llave (30, 40) unidas utilizando la llave temporal almacenada;

producir una llave temporal nueva, una tercera y cuarta llave y una cerradura nueva (60);

invalidar la primera y segunda llave (30, 40) con la nueva cerradura (60);

sustituir la primera llave (30) en el objeto (10) con la tercera llave; y

sustituir tanto la llave temporal como la segunda llave (40) en la base de datos (50) por la llave temporal nueva y la cuarta llave, donde

la primera llave (30) es sustituida en el objeto (10) por la tercera llave, y la llave temporal y la segunda llave (40) son sustituidas en la base de datos (50) por la llave temporal nueva y la cuarta llave, después de cada vez que se utiliza el objeto (10).

10. El sistema (100, 300) de la reivindicación 9, donde el objeto (10) se selecciona del grupo compuesto por:

un pasaporte,

una tarjeta bancaria,

una tarjeta de viaje electrónica,

un documento electrónico protegido,

un descodificador de televisión inteligente,

un descodificador de televisión por cable,

un automóvil,

una pieza de automóvil,

una licencia de software, y

un medio digital.

11. El sistema (100, 300) de la reivindicación 10, donde la tarjeta bancaria se selecciona del grupo compuesto por:

una tarjeta de crédito,

una tarjeta de cajero automático,

una tarjeta de débito,

una tarjeta de depósito, y

una tarjeta de pago electrónico.

12. El sistema (100, 300) de la reivindicación 10, donde la tarjeta de viaje electrónica se selecciona del grupo compuesto por una tarjeta Oyster y una tarjeta Octoplus.

13. El sistema (100, 300) de la reivindicación 10, donde la licencia de software se selecciona del grupo compuesto por una licencia de programa, una licencia de software de automatización, una licencia de sistema operativo y una aplicación de teléfono móvil.

14. El sistema (100, 300) de la reivindicación 10, donde el medio digital se selecciona del grupo compuesto por:

un juego,

música,

una película,

un videoclip,

la televisión, y

una serie de televisión en línea.

15. El sistema (100, 300) de la reivindicación 9, donde la primera y segunda llave (30, 40) se producen mediante cifrado de la información de cuenta utilizando una llave temporal generada y separando la información de cuenta cifrada en la primera y segunda llave (30, 40).

16. El sistema (100, 300) de la reivindicación 15, donde la información de cuenta es la información de cuenta de un usuario del objeto (10).

17. Un aparato (400) para proteger un objeto (10) frente a una copia no autorizada, que comprende:

un motor de cifrado (402);

un lector de llaves del objeto (404) y un lector de llaves del emisor (406) acoplados al motor de cifrado (402) y configurados para leer una llave del objeto y una llave del emisor respectivamente;

un validador de llaves (408) acoplado al motor de cifrado (402) y configurado para cifrar o descifrar la llave del objeto y la llave del emisor con el fin de validar la llave del objeto y la llave del emisor;

un generador de llaves (410) acoplado al motor de cifrado (402) y configurado para generar una llave temporal y cifrar o descifrar la llave del objeto y la llave del emisor, con el fin de generar un código cifrado y dividirlo en la llave del objeto y la llave del emisor; y

un actualizador de llaves acoplado al generador de llaves (410) y configurado para actualizar la llave del objeto y la llave del emisor mediante la sustitución de la llave del objeto y la llave del emisor por una llave del objeto nueva y una llave del emisor nueva, respectivamente, y descartar la llave del objeto y la llave del emisor, donde

la llave del objeto se sustituye por la llave del objeto nueva y la llave del emisor se sustituye por la llave del emisor nueva, después de cada vez que se utiliza el objeto (10).

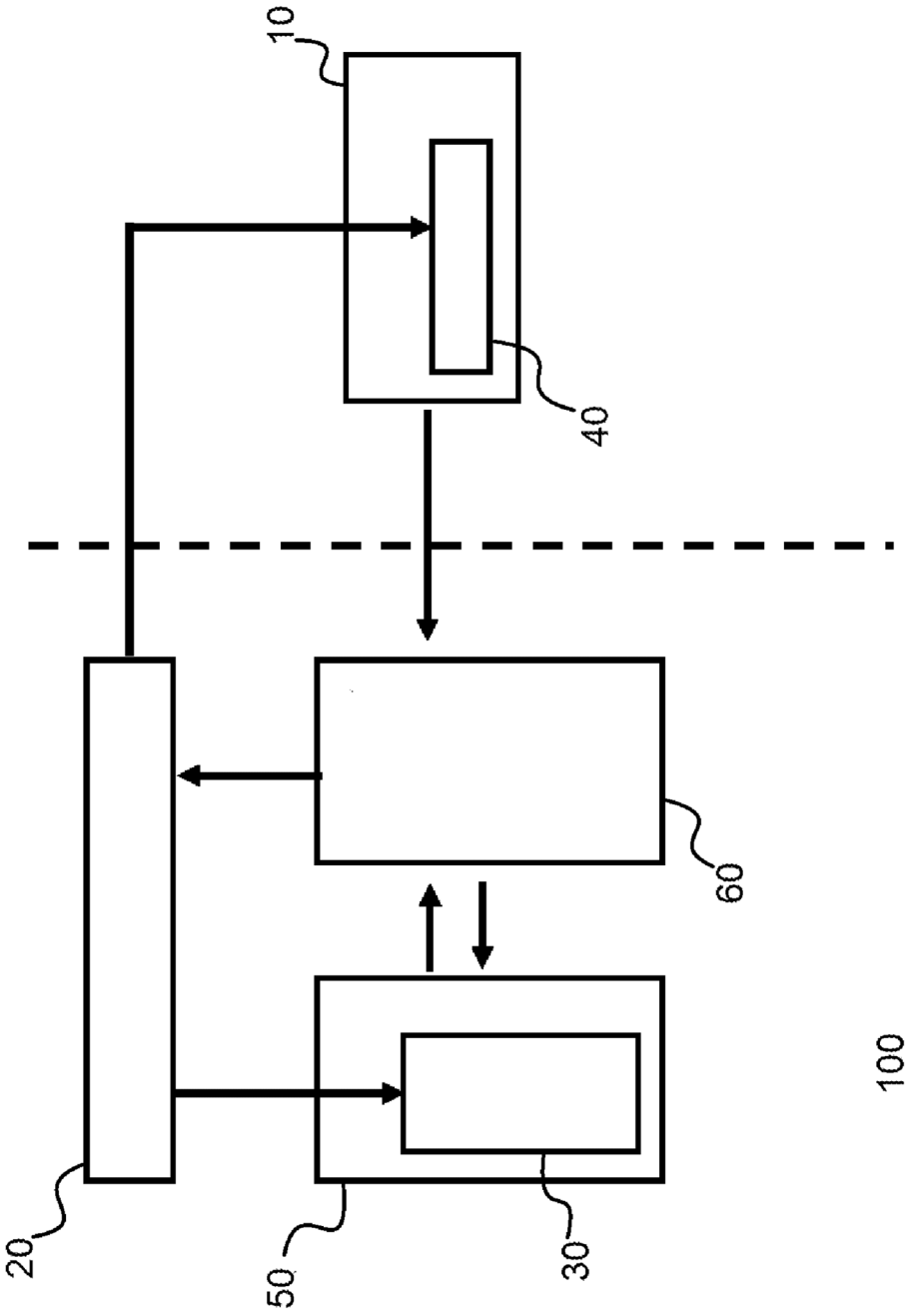

Fig. 1

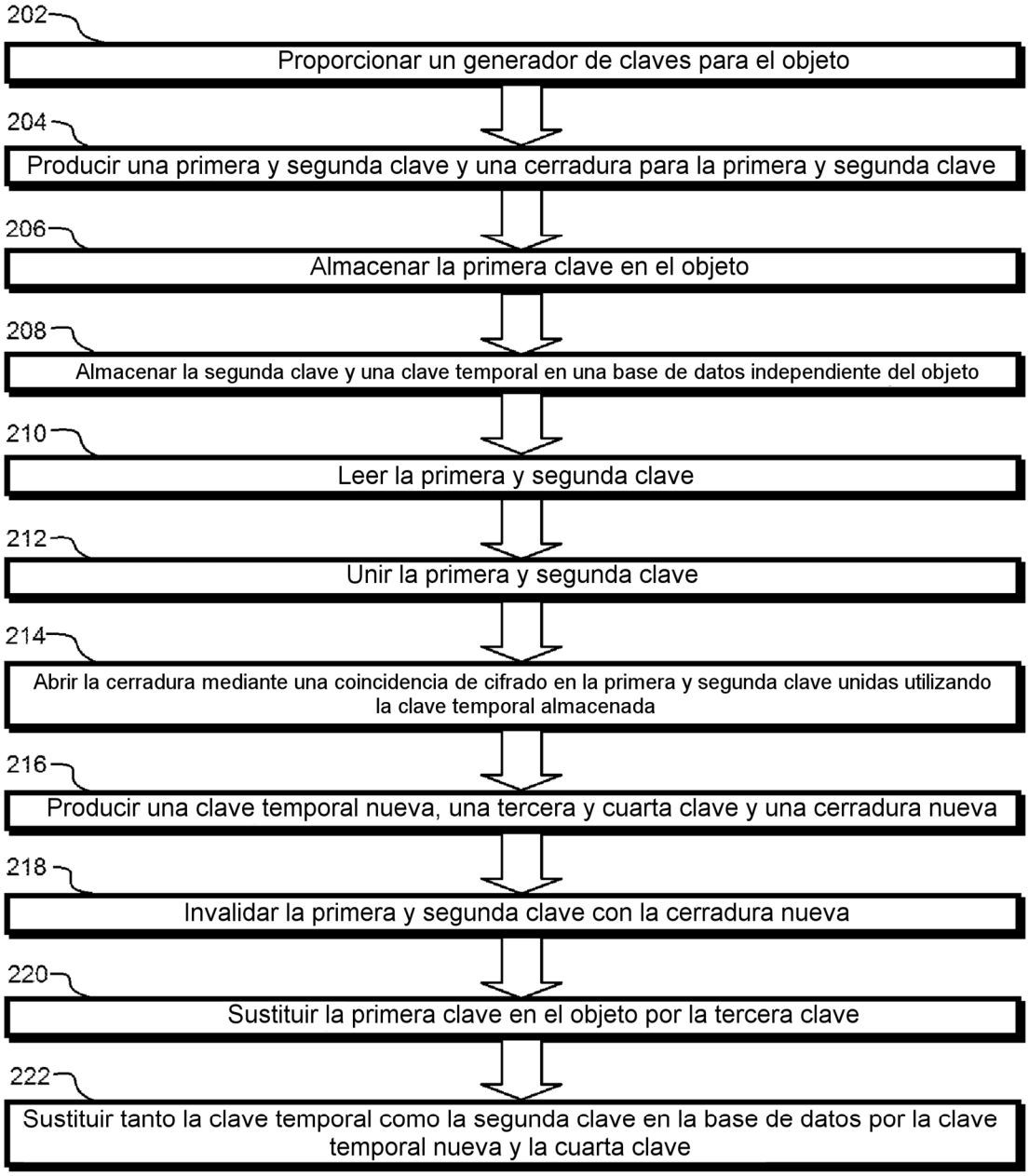
202
Proporcionar un generador de claves para el objeto
204
Producir una primera y segunda clave y una cerradura para la primera y segunda clave
206
Almacenar la primera clave en el objeto
208
Almacenar la segunda clave y una clave temporal en una base de datos independiente del objeto
210
Leer la primera y segunda clave
212
Unir la primera y segunda clave
214
Abrir la cerradura mediante una coincidencia de cifrado en la primera y segunda clave unidas utilizando la clave temporal almacenada
216
Producir una clave temporal nueva, una tercera y cuarta clave y una cerradura nueva
218
Invalidar la primera y segunda clave con la cerradura nueva
220
Sustituir la primera clave en el objeto por la tercera clave
222
Sustituir tanto la clave temporal como la segunda clave en la base de datos por la clave temporal nueva y la cuarta clave
200

Fig. 2

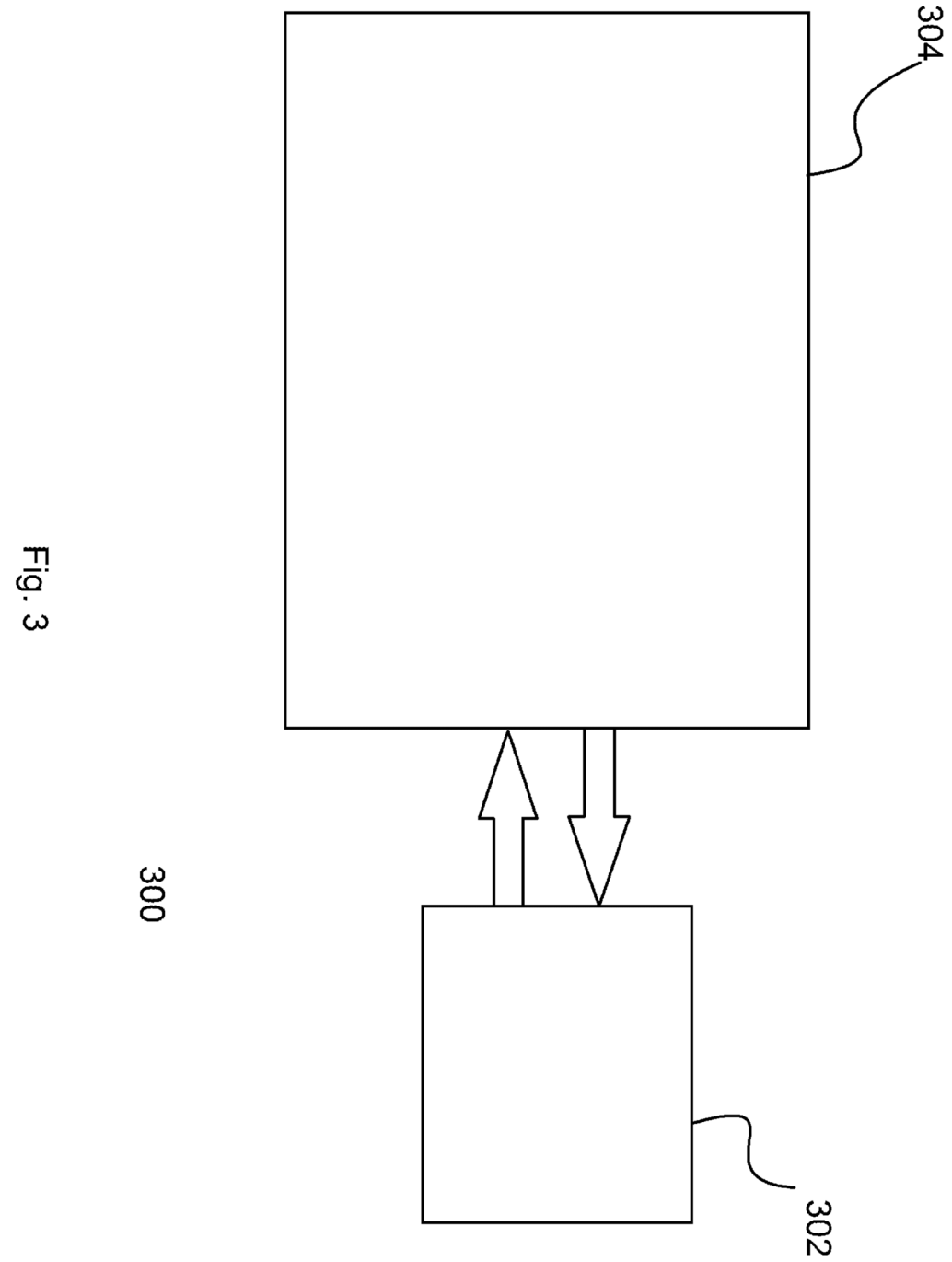

Fig. 3

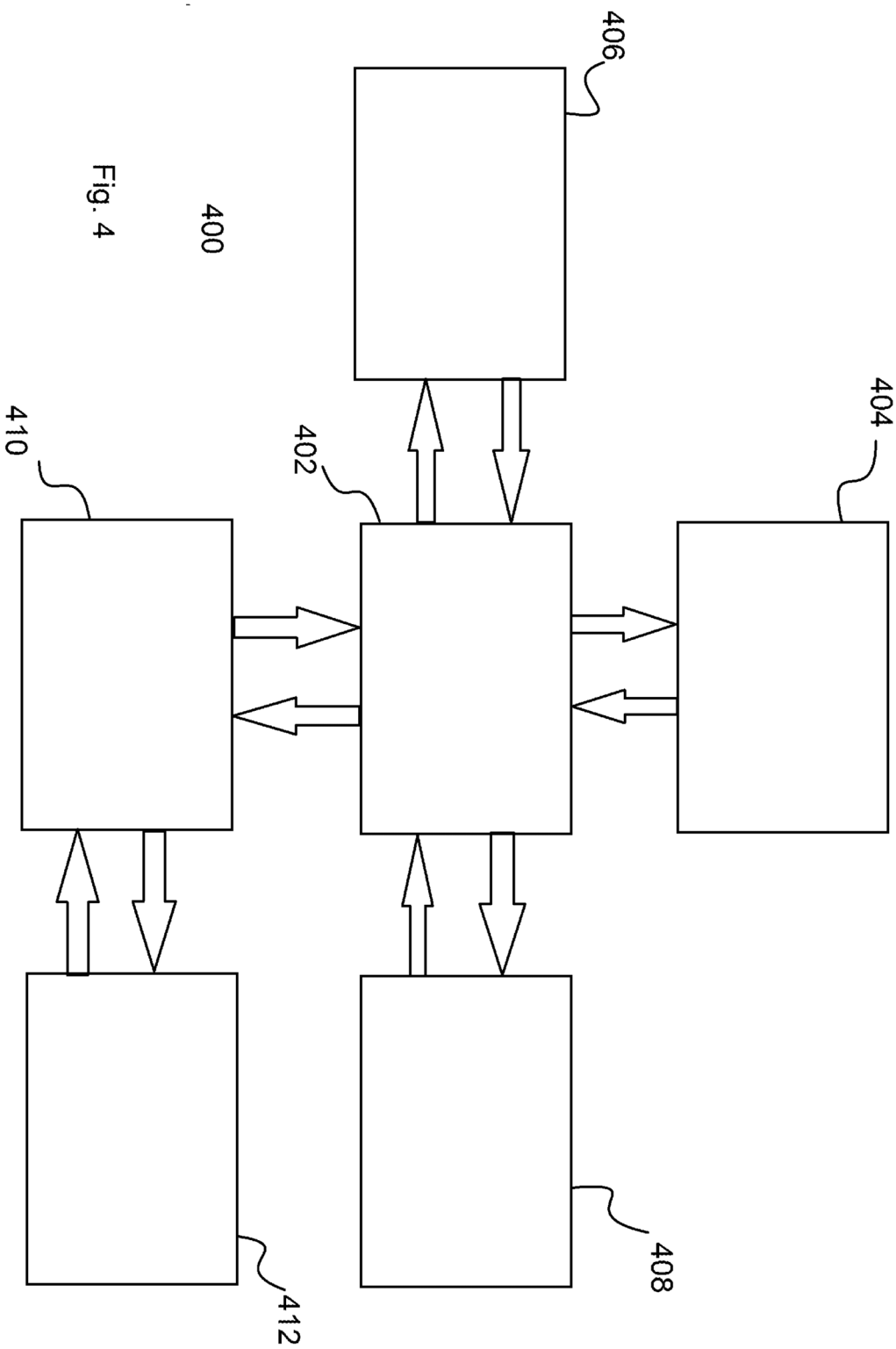

Fig. 4