(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 781 091**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/08 (2006.01)
H04L 9/14 (2006.01)
H04L 9/30 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.01.2017 PCT/US2017/012437**

(87) Fecha y número de publicación internacional: **27.07.2017 WO17127238**

(96) Fecha de presentación y número de la solicitud europea: **06.01.2017 E 17701221 (8)**

(97) Fecha y número de publicación de la concesión europea: **26.02.2020 EP 3381172**

(54) Título: **Método y sistema para aprovisionamiento y almacenamiento de clave criptográfica mediante criptografía de curva elíptica**

(30) Prioridad:

20.01.2016 US 201615001775

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.08.2020

(73) Titular/es:

MASTERCARD INTERNATIONAL INCORPORATED (100.0%)
2000 Purchase Street
Purchase, New York 10577, US

(72) Inventor/es:

DAVIS, STEVEN, CHARLES

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Método y sistema para aprovisionamiento y almacenamiento de clave criptográfica mediante criptografía de curva elíptica

Referencia cruzada a solicitudes relacionadas

Esta solicitud reivindica prioridad a, y el beneficio de, la fecha de presentación de la Solicitud de Patente de Estados Unidos N. º 15/001.775, presentada el 20 de enero de 2016.

Campo

La presente divulgación se refiere a la distribución de múltiples claves criptográficas usadas para acceder a datos, específicamente el uso de criptografía de curva elíptica para distribuir de manera segura una pluralidad de claves criptográficas usadas para derivar una clave única para acceso de datos que necesitan la negociación de propiedad de datos mediante receptores de clave criptográfica.

Antecedentes

En un mundo donde el número de dispositivos informáticos son miles de millones, se están transfiriendo constantemente datos. Los datos pueden transferirse de un dispositivo informático a otro; de un dispositivo informático a muchos otros dispositivos informáticos, o de muchos dispositivos informáticos a uno único. En muchos casos, la seguridad de una transferencia de datos puede ser tan importante como si se estuvieran transfiriendo los datos. Por ejemplo, si los datos se aseguran de manera apropiada, de manera que únicamente una parte pretendida puede visualizar los datos, los datos pueden hacerse públicamente disponibles para su acceso más fácil por la parte pretendida. Con un alto nivel de seguridad, los datos pueden estar seguros de cualquier entidad distinta de la parte pretendida a pesar de la accesibilidad pública. Como resultado, asegurar la seguridad de los datos que se están transfiriendo mediante canales públicos puede ser altamente importante.

Sin embargo, un perspectiva de este tipo puede ser extremadamente difícil en casos donde los datos se hacen disponibles para un grupo de entidades pretendidas. Por ejemplo, si una parte desea hacer datos públicamente disponibles accesibles para un grupo de cuatro personas diferentes, la parte puede encriptar los datos y proporcionar claves adecuadas para acceder a los datos a cada una de las cuatro personas diferentes. En un ejemplo de este tipo, un compromiso de cualquiera de las cuatro claves puede comprender que se transfieran los datos, que conduce a una situación significativamente menos segura. Para mantener el nivel más alto de seguridad, puede ser conveniente para la parte distribuir únicamente una clave única para acceder a los datos. Sin embargo, el grupo de cuatro personas puede no poder identificar qué persona va a recibir la clave única, o una identificación de este tipo puede llevar tiempo o ser inconveniente de otra manera para la parte.

Por lo tanto, existe una necesidad de una solución técnica para la transferencia de datos para la accesibilidad por una pluralidad de entidades mediante el uso de una clave de acceso única. Adicionalmente, existe una necesidad de una solución técnica mediante la cual la parte que transfiere puede proporcionar datos a cada una de la pluralidad de entidades para la negociación de propiedad por las entidades sin participación por la parte que transfiere. En un ejemplo de este tipo, los datos pueden transferirse de manera segura con una mínima probabilidad de estar comprometidos, y estando disponible el acceso únicamente para una única entidad, que puede seleccionarse entre la pluralidad de entidades sin requerir participación adicional por la parte que transfiere.

La técnica anterior incluye los documentos US 2015/310436 A1 y US 2015/213433 A1.

Sumario

La invención se define en las reivindicaciones independientes.

La presente divulgación proporciona una descripción de sistemas y métodos para distribuir múltiples claves criptográficas para usarse en el acceso de datos.

Un método para distribuir múltiples claves criptográficas usadas para acceder a datos incluye: recibir, por un dispositivo de recepción de un servidor de procesamiento, una señal de datos superpuesta con una solicitud de clave de acceso, en el que la solicitud de clave de acceso incluye al menos un número, n, mayor que 1, de claves solicitadas; generar, por un módulo de generación del servidor de procesamiento, n pares de claves que usan un algoritmo de generación de par de claves, en el que cada par de claves incluye una clave privada y una clave pública; derivar, por un módulo de derivación del servidor de procesamiento, una clave privada de acceso aplicando la clave privada incluida en cada uno de los n pares de claves a un algoritmo de derivación de clave; generar, por el módulo de generación del servidor de procesamiento, una clave pública de acceso que corresponde a la clave privada de acceso derivada usando el algoritmo de generación de par de claves; y transmitir electrónicamente, por un dispositivo de transmisión del servidor de procesamiento, una señal de datos superpuesta con una clave privada incluida en uno de los n pares de claves

para cada uno de los n pares de claves.

Un sistema para distribuir múltiples claves criptográficas usadas para acceder a datos incluye: un dispositivo de transmisión de un servidor de procesamiento; un dispositivo de recepción del servidor de procesamiento configurado para recibir una señal de datos superpuesta con una solicitud de clave de acceso, en el que la solicitud de clave de acceso incluye al menos un número, n, de claves solicitadas; un módulo de generación del servidor de procesamiento configurado para generar n pares de claves usando un algoritmo de generación de par de claves, en el que cada par de claves incluye una clave privada y una clave pública; y un módulo de derivación del servidor de procesamiento configurado para derivar una clave privada de acceso aplicando la clave privada incluida en cada uno de los n pares de claves a un algoritmo de derivación de clave. El módulo de generación del servidor de procesamiento está configurado adicionalmente para generar una clave pública de acceso que corresponde a la clave privada de acceso derivada usando el algoritmo de generación de par de claves. El dispositivo de transmisión del servidor de procesamiento está configurado para transmitir electrónicamente una señal de datos superpuesta con una clave privada incluida en uno de los n pares de claves para cada uno de los n pares de claves.

Breve descripción de las figuras de los dibujos

El alcance de la presente divulgación se entiende mejor a partir de la siguiente descripción detallada de realizaciones ilustrativas cuando se leen en conjunto con los dibujos adjuntos. En los dibujos se incluyen las siguientes figuras:

La Figura 1 es un diagrama de bloques que ilustra una arquitectura de sistema de alto nivel para la distribución de claves a múltiples entidades para la negociación de propiedad de recompensa de acuerdo con realizaciones ejemplares.

La Figura 2 es un diagrama de bloques que ilustra el servidor de procesamiento de la Figura 1 para la distribución de claves criptográficas a múltiples entidades para su uso en negociación de propiedad de recompensa de acuerdo con realizaciones ejemplares.

La Figura 3 es un diagrama de flujo que ilustra la generación de una clave de acceso por el servidor de procesamiento de la Figura 2 para asegurar datos para la negociación de propiedad por múltiples entidades de acuerdo con realizaciones ejemplares.

La Figura 4 es un diagrama de flujo que ilustra un flujo de proceso para la transferencia de una clave de acceso que usa criptografía de curva elíptica de acuerdo con realizaciones ejemplares.

La Figura 5 es un diagrama de flujo que ilustra un método ejemplar para distribuir múltiples claves criptográficas usadas para acceder a datos de acuerdo con realizaciones ejemplares.

La Figura 6 es un diagrama de bloques que ilustra una arquitectura de sistema informático de acuerdo con realizaciones ilustrativas.

Adicionalmente áreas de aplicabilidad de la presente divulgación serán evidentes a partir de la descripción detallada proporcionada en lo sucesivo. Debería entenderse que la descripción detallada de realizaciones ilustrativas se concibe para propósitos de ilustración únicamente y no se concibe, por lo tanto, para limitar necesariamente el alcance de la divulgación.

Descripción detallada

Glosario de términos

Cadena de bloques - un libro mayor de todas las transacciones de conformidad con una o más normas o convenciones asociadas con la cadena de bloques. Uno o más dispositivos informáticos pueden comprender una red de cadena de bloques, que puede estar configurada para procesar y registrar transacciones como parte de un bloque en la cadena de bloques. Una vez que se completa un bloque, el bloque se añade a la cadena de bloques y el registro de transacción se actualiza de esta manera. En muchos casos, la cadena de bloques puede ser un libro mayor de transacciones en orden cronológico, o puede presentarse en otro orden que puede ser adecuado para su uso por la red de cadena de bloques. En algunas configuraciones, una cadena de bloques puede ser un libro mayor de transacciones de moneda, donde las transacciones registradas en la cadena de bloques pueden incluir una dirección de destino y una cantidad de moneda, de manera que la cadena de bloques registra cuántas monedas son atribuibles a una dirección específica. En algunas de tales configuraciones, la cadena de bloques puede usar una moneda digital basada en cadena de bloques, que puede ser única para la cadena de bloques respectiva. En algunos casos, puede capturarse información adicional, tal como una dirección de origen, indicación de tiempo, etc. En algunas realizaciones, una cadena de bloques puede consistir también en datos adicionales, y en algunos casos arbitrarios, que se confirman y validan por la red de cadena de bloques a través de prueba de funcionamiento y/o cualesquiera toras técnicas de verificación adecuadas asociadas con los mismos. En algunos casos, tales datos pueden estar incluidos en la cadena de bloques como parte de las transacciones, tal como se incluyen en datos adicionales anexados a datos de transacción. En algunos casos, la inclusión de tales datos en una cadena de bloques puede constituir una transacción. En tales casos, una cadena de bloques puede no estar directamente asociada con una moneda digital, virtual, fiduciaria o de otro tipo específico. Una cadena de bloques puede ser privada, donde únicamente sistemas o dispositivos autorizados pueden acceder a la cadena de bloques, o puede ser pública, donde la cadena de bloques puede ser accesible por cualquier dispositivo o sistema. En cualquier caso, la capacidad para que los dispositivos o sistemas añadan transacciones a la cadena de

bloques puede estar limitada.

Sistema para distribución de clave criptográfica mediante criptografía de curva elíptica

La Figura 1 ilustra un sistema 100 para la transferencia de claves criptográficas que usa criptografía de curva elíptica para su uso en la transferencia segura de datos.

El sistema 100 puede incluir un servidor 102 de procesamiento. El servidor 102 de procesamiento, analizado en más detalle a continuación, puede estar configurado para generar múltiples claves de criptografía para su distribución usando criptografía de curva elíptica que se usa en la accesibilidad de datos por una pluralidad de dispositivos 104 informáticos. Esto se hace de tal manera que requiere procesamiento en un ordenador específicamente programado para llevar a cabo las funciones desveladas en el presente documento que no pueden realizarse en un ordenador de fin general, y no pueden hacerse de una manera realista a través de proceso mental o con lápiz y papel, para proporcionar de esta manera una solución técnica al negociar la propiedad de recompensa en la transferencia segura de datos. El servidor 102 de procesamiento puede recibir una solicitud de clave de acceso, que puede solicitar una pluralidad de claves para distribución a los dispositivos 104 informáticos para su uso en el acceso de datos. La solicitud de clave de acceso puede recibirse de un dispositivo externo, tal como otro dispositivo o sistema informático, tal como mediante una transmisión electrónica de un dispositivo o sistema de este tipo usando una red de comunicación adecuada (por ejemplo, una red de área local, red de área extensa, de radiofrecuencia, Bluetooth, comunicación de campo cercano, Internet, etc.), o puede recibirse mediante uno o más dispositivos de entrada interconectados con el servidor 102 de procesamiento, tal como puede accederse por un usuario del servidor 102 de procesamiento. La solicitud de clave de acceso puede especificar un número, n, de dispositivos 104 informáticos para los que se solicitan claves de acceso. En el ejemplo ilustrado en la Figura 1, la solicitud de clave de acceso puede ser para tres claves de acceso.

El servidor 102 de procesamiento puede generar a continuación el número solicitado, n, de pares de claves. Cada par de claves puede comprender una clave privada y una clave pública, en el presente documento denominado como un par de claves de "recompensa" que comprende una clave privada y clave pública de "recompensa". El servidor 102 de procesamiento puede usar un algoritmo de generación de par de claves adecuado en la generación del número solicitado de pares de claves. En una realización ejemplar, el algoritmo de generación de par de claves puede ser un esquema de acuerdo de clave de curva elíptica. En una realización adicional, puede usarse el protocolo de acuerdo de clave Diffie-Hellman de curva elíptica (ECDH) en la generación de cada uno de los n pares de claves, como puede apreciarse por un experto en la materia. En cualquier caso, el algoritmo de generación de par de claves puede ser uno adecuado para el uso de secretos compartidos, como se analiza en más detalle a continuación.

Una vez que se ha generado el número n de pares de claves de recompensa, el servidor 102 de procesamiento puede derivar una clave privada de acceso aplicando la clave privada de recompensa de cada uno de los n pares de claves de recompensa a un algoritmo de derivación de clave. En algunas realizaciones, el algoritmo de derivación de clave puede incluir el uso de una operación lógica XOR. En realizaciones ejemplares, el algoritmo de derivación de clave puede ser de manera que la varianza en la ordenación o secuenciación de las claves privadas de recompensa en la derivación de la clave privada de acceso puede dar como resultado la misma clave privada de acceso. En tales realizaciones, cualquier entidad en posesión de cada una de las claves privadas de recompensa, y con el conocimiento del algoritmo de derivación de clave usado, puede poder reproducir la clave privada de acceso independientemente de la ordenación o secuenciación de las claves privadas de recompensa.

El servidor 102 de procesamiento puede estar también configurado para generar una clave pública de acceso que corresponde al acceso derivado. La clave pública de acceso puede generarse mediante el uso de un algoritmo de generación de par de claves, que puede ser el mismo algoritmo de generación de par de claves usado para generar los pares de claves de recompensa. Por ejemplo, en una realización ejemplar, el servidor 102 de procesamiento puede usar el protocolo de acuerdo de clave de ECDH para generar la clave pública de acceso como parte de un par de claves con la clave privada de acceso derivada.

El servidor 102 de procesamiento puede usar la clave privada de acceso derivada para restringir el acceso a datos. Puede usarse cualquier método adecuado para la restricción de acceso a datos usando una clave privada. Por ejemplo, en un ejemplo, los datos pueden encriptarse usando la clave privada de acceso y un algoritmo de encriptación adecuado. En otro ejemplo, los datos a los que está restringido el acceso pueden ser una cantidad de moneda de cadena de bloques disponible mediante una red 106 de cadena de bloques. En un ejemplo de este tipo, la clave pública de acceso puede usarse para generar una dirección de destino para una cantidad de moneda de cadena de bloques, donde se usa la clave privada de acceso para firmar la dirección de destino y proporcionar acceso a la moneda de cadena de bloques asociada con la misma. El uso de pares de claves para transferir y acceder a la moneda de cadena de bloques usando una red 106 de cadena de bloques será evidente para los expertos en la materia.

Una vez que el servidor 102 de procesamiento ha restringido el acceso a datos deseados que usan la clave privada de acceso, el servidor 102 de procesamiento puede transmitir electrónicamente una clave privada de recompensa a cada uno de los dispositivos 104 informáticos de manera que cada dispositivo 104 informático recibe una clave privada de recompensa diferente. Por ejemplo, en el ejemplo ilustrado en la Figura 1, el servidor 102 de procesamiento puede

generar claves privadas de recompensa Ka, Kb, y Kc, que pueden transmitirse electrónicamente a los dispositivos informáticos, 104a, 104b, y 104c, respectivamente. En algunas realizaciones, las claves privadas de recompensa pueden superponerse en una señal de datos transmitida electrónicamente a los respectivos dispositivos 104 informáticos usando Internet u otra red de comunicación adecuada.

En una realización ejemplar, las claves privadas de recompensa pueden encriptarse antes de su transmisión usando un secreto compartido. En una realización de este tipo, el servidor 102 de procesamiento y cada uno de los dispositivos 104 informáticos puede generar pares de claves para su uso en la transferencia, encriptación y desencriptación de las claves privadas de recompensa mediante secretos compartidos. El servidor 102 de procesamiento y los dispositivos 104 informáticos puede cada uno generar un par de claves usando el mismo algoritmo de generación de par de claves, que puede ser el protocolo de acuerdo de clave de ECDH u otro algoritmo adecuado para su uso en conjunto con secretos compartidos. Usando el algoritmo de generación de par de claves, el servidor 102 de procesamiento puede generar un par de claves denominadas en el presente documento como un par de claves de "transferencia" que comprende una clave privada y clave pública de "transferencia". Cada dispositivo 104 informático puede generar un par de claves usando el algoritmo de generación de par de claves denominadas en el presente documento como un par de claves de "dispositivo" que comprende una clave privada y clave pública de "dispositivo". Cada dispositivo 104 informático puede transmitir electrónicamente su clave pública de dispositivo asociada al servidor 102 de procesamiento usando un método de comunicación adecuado. El servidor 102 de procesamiento puede transmitir también electrónicamente la clave pública de transferencia a cada uno de los dispositivos 104 informáticos. En algunos casos, la clave pública de transferencia puede transmitirse con (por ejemplo, en la misma transmisión o en una adjunta) la clave privada de recompensa encriptada.

Después de que el servidor 102 de procesamiento haya recibido la clave pública de dispositivo de un dispositivo 104 informático, el servidor 102 de procesamiento puede generar un secreto compartido. El secreto compartido puede generarse usando la clave privada de transferencia y la clave pública del dispositivo en conjunto con el algoritmo de generación de par de claves usado en la generación de cada una de las respectivas claves. El secreto compartido puede ser un secreto que es equivalente cuando se genera con la clave privada de un primer par de claves y la clave pública de un segundo par de claves o cuando se genera con la clave pública del primer par de claves y la clave privada del segundo par de claves. Por ejemplo, en el ejemplo ilustrado, el servidor 102 de procesamiento puede generar un secreto compartido para su uso al transportar la clave privada de recompensa Ka al dispositivo 104a informático usando la clave privada de transferencia generada por el servidor 102 de procesamiento y la clave pública de dispositivo recibido del dispositivo 104a informático. El dispositivo 104a informático puede generar un secreto compartido equivalente usando la clave pública de transferencia recibida del servidor 102 de procesamiento y la clave privada del dispositivo generada por el dispositivo 104a informático.

Una vez que el servidor 102 de procesamiento ha generado un secreto compartido asociado con un dispositivo 104 informático (por ejemplo, usando esa clave pública de dispositivo del dispositivo informático específico), el servidor 102 de procesamiento puede encriptar la clave privada de recompensa que se transporta a ese dispositivo 104 informático usando el secreto compartido asociado. Puede usarse cualquier algoritmo de encriptación adecuado, tal como el algoritmo de encriptación AES256. La clave privada de recompensa encriptada puede a continuación transmitirse electrónicamente al dispositivo 104 informático asociado usando cualquier método de comunicación adecuado. En algunos casos, el servidor 102 de procesamiento puede incluir la clave pública de transferencia en la comunicación electrónica usada para transportar una clave privada de recompensa encriptada.

Cada dispositivo 104 informático puede generar un secreto compartido para su uso al desencriptar la clave privada de recompensa encriptada recibida. El secreto compartido puede generarse usando la clave pública de transferencia transmitida electrónicamente por el servidor 102 de procesamiento y la clave privada del dispositivo generada del dispositivo informático. El secreto compartido puede generarse usando el algoritmo de generación de par de claves usado por el dispositivo 104 informático y el servidor 102 de procesamiento en la generación del correspondiente pares de claves. El dispositivo 104 informático puede usar el secreto compartido para desencriptar la clave privada de recompensa usando el algoritmo de encriptación apropiado usado por el servidor 102 de procesamiento. Por ejemplo, el dispositivo 104 informático puede usar el algoritmo AES256 en la desencriptación de la clave privada de recompensa usando el secreto compartido.

Una vez que cada dispositivo 104 informático ha recibido y desencriptado, si es aplicable, su respectiva clave privada de recompensa, los dispositivos 104 informáticos pueden negociar la posesión de cada una de las claves privadas de recompensa. En algunos casos, los usuarios asociados con los dispositivos 104 informáticos pueden negociar la posesión de las claves privadas de recompensa sin uso de los dispositivos 104 informáticos. Por ejemplo, en el ejemplo ilustrado tres usuarios de los dispositivos 104 informáticos pueden negociar fuera de línea para acordar que el usuario del dispositivo 104a informático recopilará cada una de las claves privadas de recompensa. En un ejemplo de este tipo, los dispositivos 104b y 104c informáticos pueden transmitir electrónicamente su clave privada de recompensa al dispositivo 104a informático usando un método de comunicación adecuado.

En algunas realizaciones, las claves privadas de recompensa pueden transferirse entre los dispositivos 104 informáticos usando secretos compartidos. En tales realizaciones, los dispositivos 104 informáticos pueden intercambiar sus claves públicas de dispositivo asociadas para su uso al generar secretos compartidos para la

encriptación de claves privadas de recompensa para su transferencia. Por ejemplo, el dispositivo 104b informático puede generar un secreto compartido para encriptar la clave privada de recompensa Kb usando la clave privada del dispositivo generada por el dispositivo 104b informático y la clave pública del dispositivo generada por el dispositivo 104a informático, y encriptar la clave privada de recompensa Kb con el secreto compartido. El dispositivo 104b informático puede transmitir electrónicamente la clave privada de recompensa encriptada Kb al dispositivo 104a informático usando un método de comunicación adecuado. El dispositivo 104a informático puede generar un secreto compartido usando la clave privada del dispositivo generada por el dispositivo 104a informático y la clave pública del dispositivo generada por el dispositivo 104b informático, y desencriptar la clave privada de recompensa Kb. Los dispositivos 104a y 104c informáticos pueden repetir el proceso para que el dispositivo 104a informático reciba y desencripte la clave privada de recompensa Kc.

Una vez que un dispositivo 104 informático tiene posesión de cada una de las claves privadas de recompensa, el dispositivo 104 informático puede derivar la clave privada de acceso usando el algoritmo de derivación de clave usado por el servidor 102 de procesamiento en la derivación de la misma. El dispositivo 104 informático puede usar la clave privada de acceso para acceder a los datos que se están transfiriendo. Por ejemplo, si los datos son moneda de cadena de bloques asociados con la red 106 de cadena de bloques, el dispositivo 104 informático puede usar la clave privada de acceso como una firma para acceder a la moneda de cadena de bloques transferida a la dirección de destino generada usando la clave pública de acceso.

Los métodos y sistemas analizados en el presente documento pueden posibilitar la transferencia de datos que son accesibles usando una clave única privada que debe derivarse mediante una pluralidad de claves distribuidas a múltiples entidades. Usando claves distribuidas a múltiples entidades, los datos pueden permanecer asegurados hasta que se realice la negociación por las múltiples entidades, sin participación requerida por la parte que transfiere. Además, puesto que la clave de acceso se deriva usando las claves distribuidas a cada entidad, los datos pueden tener un nivel significativamente superior de seguridad que el uso de una clave única, que puede proporcionar mayor protección para los datos, particularmente en instancias cuando los datos pueden estar públicamente disponibles, pero no accesibles, tal como en una red 106 de cadena de bloques. El uso de criptografía de curva elíptica puede proporcionar incluso mayor protección, ya que incluso las claves privadas de recompensa pueden tener un nivel mejorado de protección en su transferencia. Como tal, los métodos y sistemas analizados en el presente documento pueden proporcionar mayor protección tanto en la transferencia de datos como en la transferencia de claves usadas en el acceso de los datos transferidos.

El uso de los métodos y sistemas analizados en el presente documento puede ser también beneficioso en el almacenamiento de una clave criptográfica usada para acceder a datos seguros. Por ejemplo, una entidad puede tener datos para almacenarse de manera segura, y puede usar los métodos analizados en el presente documento para generar una clave única privada para encriptar los datos, donde las claves privadas de recompensa usadas para derivar la clave privada única se distribuyen a una pluralidad de diferentes sistemas informáticos y la clave privada única se descarta. En tales casos, si un almacén de clave criptográfica para uno de los sistemas informáticos está comprometido, los datos pueden aún ser seguros ya que la entidad que obtiene el acceso a la clave privada de recompensa no podrá derivar la clave privada única usada para encriptar los datos. La clave privada comprometida puede proporcionarse a los otros sistemas informáticos, y la clave privada única derivarse a partir de la misma y el proceso repetirse para generar un nuevo conjunto de claves privadas de recompensa. En un ejemplo de este tipo, los datos pueden permanecer seguros en cualquier momento que cualquier almacén de clave criptográfica esté comprometido. Como tal, los métodos analizados en el presente documento pueden ser beneficiosos para proporcionar almacenamiento de clave criptográfica distribuido seguro.

Servidor de procesamiento

La Figura 2 ilustra una realización del servidor 102 de procesamiento del sistema 100. Será evidente para los expertos en la materia que la realización del servidor 102 de procesamiento ilustrada en la Figura 2 se proporciona como ilustración únicamente y puede no ser exhaustiva a todas las posibles configuraciones del servidor 102 de procesamiento adecuadas para realizar las funciones como se analiza en el presente documento. Por ejemplo, el sistema 600 informático ilustrado en la Figura 6 y analizado en más detalle a continuación puede ser una configuración adecuada del servidor 102 de procesamiento.

El servidor 102 de procesamiento puede incluir un dispositivo 202 de recepción. El dispositivo 202 de recepción puede estar configurado para recibir datos a través de una o más redes mediante uno o más protocolos de red. En algunos casos, el dispositivo 202 de recepción puede también estar configurado para recibir datos de dispositivos 104 informáticos, redes 106 de cadena de bloques, y otras entidades mediante redes de comunicación adecuadas, tal como redes de área local, redes de área extensa, redes de radiofrecuencia, Internet. En algunas realizaciones, el dispositivo 202 de recepción puede estar comprendido de múltiples dispositivos, tales como diferentes dispositivos de recepción para recibir datos a través de diferentes redes, tal como un primer dispositivo de recepción para recibir datos a través de comunicación de campo cercano y un segundo dispositivo de recepción para recibir datos a través de Internet. El dispositivo 202 de recepción puede recibir señales de datos que se transmiten electrónicamente, donde los datos pueden superponerse en la señal de datos y decodificarse, analizarse, leerse u obtenerse de otra manera mediante la recepción de la señal de datos por el dispositivo 202 de recepción. En algunos casos, el dispositivo 202

de recepción puede incluir un módulo de análisis para analizar la señal de datos recibida para obtener los datos superpuestos en la misma. Por ejemplo, el dispositivo 202 de recepción puede incluir un programa analizador configurado para recibir y transformar la señal de datos recibida en entrada usable para las funciones realizadas por el dispositivo de procesamiento para llevar a cabo los métodos y sistemas analizados en el presente documento.

El dispositivo 202 de recepción puede estar configurado para recibir señales de datos transmitidas electrónicamente por los dispositivos 104 informáticos para su uso al realizar las funciones analizadas en el presente documento. Las señales de datos transmitidas electrónicamente por los dispositivos 104 informáticos pueden superponerse con claves públicas de dispositivo, tal como para su uso al generar secretos compartidos. El dispositivo 202 de recepción puede recibir también señales de datos de dispositivos y sistemas adicionales, tal como de la red 106 de cadena de bloques y/o nodos asociados con la misma para su uso en la transferencia de datos (por ejemplo, moneda de cadena de bloques) mediante la red 106 de cadena de bloques, y tal como un dispositivo informático externo que envía una solicitud de clave de acceso. En algunos casos, el dispositivo 202 de recepción puede recibir una señal de datos superpuesta con una solicitud de clave de acceso para *n* claves privadas de recompensa para acceder a datos de un dispositivo 104 informático para recibir una de las claves privadas de recompensa.

El servidor 102 de procesamiento puede incluir también un módulo 204 de comunicación. El módulo 204 de comunicación puede estar configurado para transmitir datos entre módulos, motores, bases de datos, memorias, y otros componentes del servidor 102 de procesamiento para su uso al realizar las funciones analizadas en el presente documento. El módulo 204 de comunicación puede estar comprendido de uno o más tipos de comunicación y utilizar diversos métodos de comunicación para comunicaciones en un dispositivo informático. Por ejemplo, el módulo 204 de comunicación puede estar comprendido de un bus, conectores de patilla de contacto, alambres, etc. En algunas realizaciones, el módulo 204 de comunicación puede estar configurado también para comunicarse entre componentes internos del servidor 102 de procesamiento y componentes externos del servidor 102 de procesamiento, tal como bases de datos conectadas externamente, dispositivos de visualización, dispositivos de entrada, etc. El servidor 102 de procesamiento puede incluir también un dispositivo de procesamiento. El dispositivo de procesamiento puede estar configurado para realizar las funciones del servidor 102 de procesamiento analizadas en el presente documento como será evidente para los expertos en la materia. En algunas realizaciones, el dispositivo de procesamiento puede incluir y/o estar comprendido de una pluralidad de motores y/o módulos especialmente configurados para realizar una o más funciones del dispositivo de procesamiento, tal como un módulo 218 de consulta, módulo 206 de generación, módulo 208 de derivación, módulo 210 de encriptación, módulo 212 de desencriptación, etc. Como se usa en el presente documento, el término "módulo" puede ser software o hardware particularmente programado para recibir una entrada, realizar uno o más procesos usando la entrada, y proporcionar una salida. La entrada, la salida y los procesos realizados por diversos módulos serán evidentes para un experto en la materia basándose en la presente divulgación.

El servidor 102 de procesamiento puede incluir un módulo 218 de consulta. El módulo 218 de consulta puede estar configurado para ejecutar consultas en bases de datos para identificar información. El módulo 218 de consulta puede recibir uno o más valores de datos o cadenas de consulta, y puede ejecutar una consulta basándose en los mismos en una base de datos indicada, tal como una memoria 216, para identificar información almacenada en la misma. El módulo 218 de consulta puede a continuación emitir la información identificada a un motor o módulo apropiado del servidor 102 de procesamiento según sea necesario. El módulo 218 de consulta puede ejecutar, por ejemplo, una consulta en la memoria 216 para identificar una o más claves recibidas de un dispositivo 104 informático o generadas por el servidor 102 de procesamiento para su uso en los métodos analizados en el presente documento.

El servidor 102 de procesamiento puede incluir un módulo 206 de generación. El módulo 206 de generación puede estar configurado para generar pares de claves y secretos compartidos. El módulo 206 de generación puede recibir una solicitud como entrada, que puede solicitar la generación de un par de claves o secreto compartido y puede incluir información para su uso en conjunto con las mismas. El módulo 206 de generación puede realizar las funciones solicitadas y puede emitir los datos solicitados para su uso por otro módulo o motor del servidor 102 de procesamiento. Por ejemplo, el módulo 206 de generación puede estar configurado para generar pares de claves, tal como pares de claves de recompensa, usando un algoritmo de generación de par de claves según se incluye o se indica de otra manera (por ejemplo, y se identifica en la memoria 216 mediante el módulo 218 de consulta) en la solicitud. El módulo 206 de generación puede estar configurado también para generar un secreto compartido usando una clave pública y clave privada de dos pares de claves diferentes, que pueden utilizar el mismo algoritmo de generación de par de claves. En algunos casos, el módulo 206 de generación puede estar configurado también para generar una clave pública que corresponde a una clave privada usando el algoritmo de generación de par de claves. En una realización ejemplar, el protocolo de acuerdo de clave de ECDH puede usarse por el módulo 206 de generación.

El servidor 102 de procesamiento puede incluir adicionalmente un módulo 208 de derivación. El módulo 208 de derivación puede estar configurado para derivar claves públicas y/o privadas. El módulo 208 de derivación puede recibir una o más claves así como un algoritmo de derivación de clave o indicación de la misma como entrada, puede derivar una clave o claves solicitadas, y puede emitir la clave o claves solicitadas para su uso por otro módulo o motor del servidor 102 de procesamiento. Por ejemplo, el módulo 208 de derivación puede recibir una pluralidad de claves privadas de recompensa generadas por el módulo 306 de generación y puede derivar una clave privada de acceso correspondiente basándose en la misma usando un algoritmo de derivación de clave adecuado. En algunas realizaciones, el módulo 208 de derivación puede usar un algoritmo de manera que una ordenación o secuenciación

de las claves privadas de recompensa puede ser intrascendente en que una varianza al orden de uso de las claves privadas de recompensa en la derivación puede dar como resultado la misma clave privada de acceso. En una realización de este tipo, el algoritmo de derivación de clave puede incluir el uso de una operación lógica XOR.

El servidor 102 de procesamiento puede incluir también un módulo 210 de encriptación. El módulo 210 de encriptación puede estar configurado para encriptar datos usando algoritmos de encriptación adecuados, tal como el algoritmo AES256. El módulo 210 de encriptación puede recibir datos a encriptarse y una clave para su uso de la misma como entrada, puede encriptar los datos usando un algoritmo adecuado, y puede emitir los datos encriptados a otro módulo o motor del servidor 102 de procesamiento para uso de los mismos. En algunos casos, el módulo 210 de encriptación puede recibir el algoritmo de encriptación o indicación del mismo como entrada. En otras instancias, el módulo 210 de encriptación puede identificar el algoritmo de encriptación a usarse. El módulo 210 de encriptación puede encriptar, por ejemplo, una clave privada de recompensa usando un secreto compartido generado en asociación de la misma.

El servidor 102 de procesamiento puede incluir también un módulo 212 de desencriptación. El módulo 212 de desencriptación puede estar configurado para desencriptar datos usando algoritmos de encriptación adecuados, tal como el algoritmo AES256. El módulo 212 de desencriptación puede recibir datos a desencriptarse y una clave para su uso de la misma como entrada, puede desencriptar los datos usando un algoritmo adecuado, y puede emitir los datos desencriptados a otro módulo o motor del servidor 102 de procesamiento para uso de los mismos. La entrada proporcionada al módulo 212 de desencriptación puede incluir el algoritmo de encriptación a usar, o puede incluir una indicación del mismo, tal como una indicación para su uso al identificar un algoritmo de encriptación almacenado en la memoria 216 mediante un módulo 218 de consulta. El módulo 212 de desencriptación puede desencriptar, por ejemplo, claves proporcionadas por los dispositivos 104 informáticos usando secretos compartidos asociados.

En algunas realizaciones, el servidor 102 de procesamiento puede incluir módulos o motores adicionales para su uso al realizar las funciones analizadas en el presente documento. Por ejemplo, el servidor 102 de procesamiento puede incluir módulos adicionales para su uso en conjunto con una red 106 de cadena de bloques, tal como para iniciar y enviar transacciones de cadena de bloques y para firmar direcciones y solicitudes de transacción para transferir moneda de cadena de bloques usando la red 106 de cadena de bloques. En algunos casos, los módulos del servidor 102 de procesamiento ilustrados en la Figura 2 y analizados en el presente documento pueden estar configurados para realizar funciones adicionales en asociación de los mismos. Por ejemplo, el módulo 206 de generación puede estar configurado para generar una dirección de destino de cadena de bloques usando la clave pública de acceso.

El servidor 102 de procesamiento puede incluir también un dispositivo 214 de transmisión. El dispositivo 214 de transmisión puede estar configurado para transmitir datos a través de una o más redes mediante uno o más protocolos de red. En algunos casos, el dispositivo 214 de transmisión puede estar configurado para transmitir datos a dispositivos 104 informáticos, redes 106 de cadena de bloques, y otras entidades mediante redes de comunicación adecuadas, tales como redes de área local, redes de área extensa, redes de radiofrecuencia, Internet. En algunas realizaciones, el dispositivo 214 de transmisión puede estar comprendido de múltiples dispositivos, tal como diferentes dispositivos de transmisión para transmitir datos a través de diferentes redes, tal como un primer dispositivo de transmisión para transmitir datos a través de comunicación de campo cercano y un segundo dispositivo de transmisión para transmitir datos a través de Internet. El dispositivo 214 de transmisión puede transmitir electrónicamente señales de datos que tienen datos superpuestos que pueden analizarse por un dispositivo informático de recepción. En algunos casos, el dispositivo 214 de transmisión puede incluir uno o más módulos para superponer, codificar, o formatear de otra manera datos en señales de datos adecuadas para su transmisión.

El dispositivo 214 de transmisión puede estar configurado para transmitir electrónicamente señales de datos a dispositivos 104 informáticos que están superpuestos con claves públicas y/o privadas, que pueden encriptarse, en algunos casos, usando secretos compartidos. Por ejemplo, el dispositivo 214 de transmisión puede estar configurado para transmitir señales de datos superpuestas con claves privadas de recompensa encriptadas a dispositivos 104 informáticos, que pueden también estar superpuestos con una clave pública de transferencia para su uso por los dispositivos 104 informáticos al generar un secreto compartido. El dispositivo 214 de transmisión puede estar también configurado para transmitir señales de datos a redes 106 de cadena de bloques para su uso al transferir moneda de cadena de bloques.

El servidor 102 de procesamiento puede incluir también la memoria 216. La memoria 216 puede estar configurada para almacenar datos para su uso por el servidor 102 de procesamiento al realizar las funciones analizadas en el presente documento. La memoria 216 puede estar configurada para almacenar datos usando métodos y esquemas de formateo de datos adecuados y puede ser cualquier tipo adecuado de memoria, tal como memoria de sólo lectura, memoria de acceso aleatorio, etc. La memoria 216 puede incluir, por ejemplo, claves y algoritmos de encriptación, protocolos y normas de comunicación, normas y protocolos de formateo de datos, código de programa para módulos y programas de aplicación del dispositivo de procesamiento, y otros datos que pueden ser adecuados para su uso por el servidor 102 de procesamiento en la realización de las funciones desveladas en el presente documento como será evidente para los expertos en la materia. La memoria 216 puede estar configurada para almacenar el algoritmo de generación de par de claves, algoritmos de derivación de clave y algoritmos de encriptación para su uso al realizar las funciones del servidor 102 de procesamiento analizadas en el presente documento.

Derivación de una clave privada de acceso

La Figura 3 ilustra un proceso 300 para la derivación de una clave privada de acceso para su uso al acceder a datos mediante múltiples claves criptográficas generadas para su distribución a una pluralidad de dispositivos 104 informáticos.

En la etapa 302, el módulo 206 de generación del servidor 102 de procesamiento puede generar una pluralidad de pares 304 de claves de recompensa usando un algoritmo de generación de par de claves adecuado, que puede ser un esquema de acuerdo de clave de curva elíptica, tal como el protocolo de acuerdo de clave de ECDH. El número de pares 304 de claves de recompensa generados por el módulo 206 de generación puede estar basado en una solicitud de clave de acceso según se recibe por el dispositivo 202 de recepción del servidor 102 de procesamiento o uno o más dispositivos de entrada interconectados con el servidor 102 de procesamiento.

En el ejemplo ilustrado en la Figura 3, el módulo 206 de generación puede generar tres pares 304 de claves de recompensa, ilustrados en la Figura 3 como el par de claves 1 304a, par de claves 2 304b, y par de claves 3 304c. Cada par 304 de claves de recompensa puede comprender una clave privada de recompensa y una correspondiente clave pública de recompensa. En la etapa 306, el módulo 208 de derivación del servidor 102 de procesamiento puede usar una operación lógica XOR con la clave privada de recompensa de cada uno de los pares 304 de claves de recompensa para derivar una clave 308 privada de acceso. Usando la operación lógica XOR, el orden de operaciones para derivar la clave 308 privada de recompensa puede ser intrascendente en cuanto a la clave privada de acceso derivada. Por ejemplo, en el proceso 300 ilustrado en la Figura 3, los pares de claves 304 pueden incluir tres claves privadas de recompensa R1, R2, y R3. La clave 308 privada de recompensa derivada usando una operación 306 lógica XOR de todas las tres claves mediante XOR(R1, XOR(R2, R3)) puede ser equivalente a las claves 308 privadas de acceso derivadas mediante las operaciones XOR(R2, XOR(R1, R3)) y XOR (R3, XOR(R1, R2)).

La clave 308 privada de acceso resultando puede usarse a continuación por el servidor 102 de procesamiento en la restricción de acceso a datos. Por ejemplo, la clave 308 privada de recompensa puede usarse para encriptar datos, o puede usarse para firmar una dirección de destino para recibir moneda de cadena de bloques asociada con una red 106 de cadena de bloques. Las claves privadas de recompensa incluidas en cada par 304 de claves de recompensa pueden distribuirse entre los dispositivos 104 informáticos como un medio para proporcionar acceso a los datos restringidos. Para almacenamiento de clave criptográfica distribuido, una entidad puede usar la clave 308 privada de recompensa para encriptar o restringir de otra manera el acceso a datos, puede descartar la clave 308 privada de recompensa, y puede distribuir a continuación la clave privada de recompensa en cada par 304 de claves de recompensa a un dispositivo 104 informático, que puede ser parte de la entidad (por ejemplo, un subsidiario o sistema informático controlado) o puede ser una entidad confiable asociada. En tales casos, si el almacenamiento de clave para cualquier dispositivo 104 informático está comprometido, los datos permanecen seguros.

Proceso para transferir claves mediante criptografía de curva elíptica para acceso de datos

La Figura 4 ilustra un proceso para la distribución de claves privadas mediante criptografía de curva elíptica, tal como para la distribución de claves privadas de recompensa generadas usando el proceso 300 ilustrado en la Figura 3 usado en la derivación de una clave privada de acceso usada para acceder a datos.

En la etapa 402, el servidor 102 de procesamiento puede generar una pluralidad de pares de claves de recompensa y derivar de los mismos una clave privada de acceso, tal como usando el proceso 300 ilustrado en la Figura 3 y analizado anteriormente. En la etapa 404, el servidor 102 de procesamiento y un dispositivo 104 informático pueden intercambiar claves públicas para su uso al generar secretos compartidos. El dispositivo 104 informático puede generar un par de claves de dispositivo usando un algoritmo de generación de par de claves, tal como el protocolo de acuerdo de clave de ECDH, que puede comprender un dispositivo clave privada y un dispositivo clave pública. El módulo 206 de generación del servidor 102 de procesamiento puede generar un par de claves de transferencia usando el mismo algoritmo de generación de par de claves, dando como resultado una clave privada de transferencia y una clave pública de transferencia. El intercambio de claves públicas puede incluir la comunicación electrónica del dispositivo clave pública del dispositivo 104 informático al servidor 102 de procesamiento y de la clave pública de transferencia del servidor 102 de procesamiento (por ejemplo, mediante el dispositivo 214 de transmisión) al dispositivo 104 informático.

En la etapa 406, el módulo 206 de generación del servidor 102 de procesamiento puede generar un secreto compartido. El secreto compartido puede generarse usando el mismo algoritmo de generación de par de claves, tal como el protocolo de acuerdo de clave de ECDH, usando la clave privada de transferencia generada por el módulo 206 de generación y la clave pública del dispositivo recibida del dispositivo 104 informático. En la etapa 406, el dispositivo 104 informático puede generar un secreto compartido equivalente usando el mismo algoritmo de generación de par de claves usando la clave privada del dispositivo generada previamente por el dispositivo 104 informático y la clave pública de transferencia recibida del servidor 104 de procesamiento.

En la etapa 410, el módulo 210 de encriptación del servidor 104 de procesamiento puede encriptar la clave privada de recompensa generada en la etapa 402 y usada en la derivación de la clave privada de acceso mediante un algoritmo de encriptación adecuado usando el secreto compartido. El algoritmo de encriptación puede ser, por ejemplo, el

algoritmo AES256. En la etapa 412, el dispositivo 214 de transmisión del servidor 102 de procesamiento puede transmitir electrónicamente una señal de datos superpuesta con la clave privada de recompensa encriptada al dispositivo 104 informático usando una red de comunicación y protocolo adecuados.

En la etapa 414, el dispositivo 104 informático puede recibir la señal de datos y puede analizar la clave privada de recompensa encriptada partir de la misma. En la etapa 416, el dispositivo 104 informático puede desencriptar la clave privada de recompensa. La clave privada de recompensa puede desencriptarse usando el mismo algoritmo de encriptación usado por el servidor 102 de procesamiento usando el secreto compartido. La clave privada de recompensa desencriptada puede a continuación usarse al derivar la clave privada de acceso cuando se combina con otras claves privadas de recompensa (por ejemplo, recibidas de otros dispositivos 104 informáticos) usando el algoritmo de derivación de clave apropiado.

Método ejemplar para distribuir múltiples claves criptográficas usadas para acceder a datos

La Figura 5 ilustra un método 500 para distribuir múltiples claves criptográficas a una pluralidad de dispositivos informáticos que pueden usarse para derivar una clave de acceso para acceder a datos.

En la etapa 502, una señal de datos superpuesta con una solicitud de clave de acceso puede recibirse por un dispositivo de recepción (por ejemplo, el dispositivo 202 de recepción) de un servidor de procesamiento (por ejemplo, el servidor 102 de procesamiento), en el que la solicitud de clave de acceso incluye al menos un número, n, mayor que 1, de claves solicitadas. En la etapa 504, pueden mapearse *n* pares de claves por un módulo de generación (por ejemplo, el módulo 206 de generación) del servidor de procesamiento usando un algoritmo de generación de par de claves, en el que cada par de claves incluye una clave privada y una clave pública.

En la etapa 506, una clave privada de acceso puede derivarse por un módulo de derivación (por ejemplo, el módulo 208 de derivación) del servidor de procesamiento aplicando la clave privada incluida en cada uno de los n pares de claves a un algoritmo de derivación de clave. En la etapa 508, una clave pública de acceso que corresponde a la clave privada de acceso derivada puede generarse por el módulo de generación del servidor de procesamiento usando el algoritmo de generación de par de claves. En la etapa 510, una señal de datos superpuesta con una clave privada incluida en uno de los n pares de claves puede transmitirse electrónicamente por un dispositivo de transmisión (por ejemplo, el dispositivo 214 de transmisión) del servidor de procesamiento para cada uno de los *n* pares de claves.

En una realización, el método 500 puede incluir también: almacenar, en una memoria (por ejemplo, la memoria 216) del servidor de procesamiento, un par de claves de transferencia que incluye una clave pública de transferencia y una clave privada de transferencia; recibir, por el dispositivo de recepción del servidor de procesamiento, una señal de datos superpuesta con una clave pública compartida de cada uno de los n dispositivos informáticos (por ejemplo, los dispositivos 104 informáticos); generar, por el módulo de generación del servidor de procesamiento, n secretos compartidos, en el que cada secreto compartido se genera usando una clave pública compartida de las n claves públicas compartidas y la clave privada de transferencia y el algoritmo de generación de par de claves; y encriptar, por un módulo de encriptación (por ejemplo, el módulo 210 de encriptación) del servidor de procesamiento, la clave privada incluida en cada uno de los *n* pares de claves con uno de los *n* secretos compartidos usando un algoritmo de encriptación, en el que la clave privada incluida superpuesta en la señal de datos transmitida electrónicamente es la respectiva clave privada encriptada. En una realización adicional, el método 500 puede incluir adicionalmente transmitir electrónicamente, por el dispositivo de transmisión del servidor de procesamiento, una señal de datos superpuesta con la clave pública de transferencia a los *n* dispositivos informáticos.

En una realización incluso más adicional, la señal de datos superpuesta con la clave pública de transferencia puede transmitirse electrónicamente a los n dispositivos informáticos antes de recibir la señal de datos superpuesta con la clave pública compartida. En otra realización adicional más, cada señal de datos superpuesta con la clave pública de transferencia puede ser una misma señal de datos que cada señal de datos superpuesta con una clave privada encriptada. En otra realización adicional más, la señal de datos transmitida puede transmitirse electrónicamente a un nodo en una red de cadena de bloques (por ejemplo, la red 106 de cadena de bloques) y cuando se incluye la clave privada encriptada en una solicitud de transacción que incluye adicionalmente una dirección de destino que corresponde a la respectiva clave pública compartida.

En algunas realizaciones, el algoritmo de generación de par de claves puede ser un esquema de acuerdo de clave de curva elíptica. En realizaciones adicionales, el esquema de acuerdo de clave de curva elíptica puede ser el protocolo de acuerdo de clave de la curva implícita elíptica Diffie-Hellman. En una realización, el algoritmo de derivación de clave puede incluir el uso de una operación lógica XOR. En algunas realizaciones, el método 500 puede incluir adicionalmente transmitir electrónicamente transmitiendo, por el dispositivo de transmisión del servidor de procesamiento, una señal de datos superpuesta con una solicitud de transacción a un nodo en una red de cadena de bloques, en el que la solicitud de transacción incluye al menos una dirección de destino firmada usando la clave privada de acceso derivada.

Arquitectura de sistema informático

La Figura 6 ilustra un sistema 600 informático en el que pueden implementarse realizaciones de la presente divulgación, o porciones de la misma, como código legible por ordenador. Por ejemplo, el servidor 102 de procesamiento de la Figura 1 puede implementarse en el sistema 600 informático usando hardware, software, firmware, medio legible por ordenador no transitorio que tiene instrucciones almacenadas en el mismo, o una combinación del mismo y puede implementarse en uno o más sistemas informáticos u otros sistemas de procesamiento. Hardware, software o cualquier combinación de los mismos puede incorporar módulos y componentes usados para implementar los métodos de las Figuras 3-5.

Si se usa lógica programable, tal lógica puede ejecutarse en una plataforma de procesamiento comercialmente disponible o un dispositivo de fin especial. Un experto en la materia puede apreciar que realizaciones de la materia objeto divulgada pueden practicarse con diversas configuraciones de sistema informático, incluyendo sistemas multiprocesador, miniordenadores, ordenadores centrales, ordenadores enlazados o agrupados con funciones distribuidas, así como ordenadores ubicuos o en miniatura que pueden embeberse en prácticamente cualquier dispositivo. Por ejemplo, pueden usarse al menos un dispositivo de procesador y una memoria para implementar las realizaciones anteriormente descritas.

Una unidad o dispositivo de procesador como se analiza en este documento puede ser un único procesador, una pluralidad de procesadores o combinaciones de los mismos. Dispositivos de procesador pueden tener uno o más "núcleos" de procesador. Los términos "medio de programa informático", "medio legible por ordenador no transitorio" y "medio usable por ordenador" como se analizan en este documento se usan para referirse generalmente a medios tangibles tal como una unidad 618 de almacenamiento extraíble, una unidad 622 de almacenamiento extraíble y un disco duro instalado en unidad 612 de disco duro.

Diversas realizaciones de la presente divulgación se describen en términos de este sistema 600 informático de ejemplo. Después de leer esta descripción, será evidente para un experto en la materia cómo implementar la presente divulgación usando otros sistemas informáticos y/o arquitecturas informáticas. Aunque operaciones pueden describirse como un proceso secuencial, algunas de las operaciones pueden de hecho realizarse en paralelo, simultáneamente y/o en un entorno distribuido, y con código de programa almacenado local o remotamente para acceso por máquina de un único o múltiples procesadores. Además, en algunas realizaciones el orden de operaciones puede reorganizarse.

El dispositivo 604 de procesador puede ser un dispositivo procesador de fin especial o de fin general específicamente configurado para realizar las funciones analizadas en el presente documento. El dispositivo 604 procesador puede estar conectado a una infraestructura 606 de comunicaciones, tal como un bus, cola de mensajes, red, esquema de paso de mensaje de múltiples núcleos, etc. La red puede ser cualquier red adecuada para realizar las funciones como se desvela en el presente documento y puede incluir una red de área local (LAN), una red de área extensa (WAN), una red inalámbrica (por ejemplo, WiFi), una red de comunicación móvil, una red satelital, Internet, de fibra óptica, cable coaxial, infrarrojos, radiofrecuencia (RF), o cualquier combinación de las mismas. Otros tipos y configuraciones de red adecuados serán evidentes para un experto en la materia. El sistema 600 informático también puede incluir una memoria 608 principal (por ejemplo, memoria de acceso aleatorio, memoria de sólo lectura, etc.), y también puede incluir una memoria 610 secundaria. La memoria 610 secundaria puede incluir la unidad 612 de disco duro y una unidad 614 de disco de almacenamiento extraíble, tal como una unidad de disco flexible, una unidad de cinta magnética, una unidad de disco óptico, una memoria flash, etc.

La unidad 614 de disco de almacenamiento extraíble puede leer de y/o escribir en la unidad 618 de almacenamiento extraíble de una manera bien conocida. La unidad 618 de almacenamiento extraíble puede incluir un medio de almacenamiento extraíble que puede leerse por y escribirse por la unidad 614 de disco de almacenamiento extraíble. Por ejemplo, si la unidad 614 de almacenamiento extraíble es una unidad de disco flexible o puerto de bus serie universal, la unidad 618 de almacenamiento extraíble puede ser un disco flexible o dispositivo flash portátil, respectivamente. En una realización, la unidad 618 de almacenamiento extraíble puede ser medio de grabación legible por ordenador no transitorio.

En algunas realizaciones, la memoria 610 secundaria puede incluir medios alternativos para permitir que programas informáticos u otras instrucciones se carguen en el sistema 600 informático, por ejemplo, la unidad 622 de almacenamiento extraíble y una interfaz 620. Ejemplos de tales medios pueden incluir un cartucho de programa e interfaz de cartucho (por ejemplo, como se encuentran en sistemas de video juegos), un chip de memoria extraíble (por ejemplo, EEPROM, PROM, etc.) y conexión asociada, y otras unidades 622 de almacenamiento extraíbles e interfaces 620 como será evidente para los expertos en la materia.

Los datos almacenados en el sistema 600 informático (por ejemplo, en la memoria 608 principal y/o la memoria 610 secundaria) pueden almacenarse en cualquier tipo de medio legible por ordenador adecuado, tal como almacenamiento óptico (por ejemplo, un disco compacto, disco versátil digital, Disco Blu-ray, etc.) o almacenamiento de cinta magnética (por ejemplo, una unidad de disco duro). Los datos pueden estar configurados en cualquier tipo de configuración de base de datos adecuada, tal como una base de datos relacional, una base de datos de lenguaje de consulta estructurada (SQL), una base de datos distribuida, una base de datos de objetos, etc. Serán evidentes para los expertos en la materia configuraciones adecuadas y tipos de almacenamiento.

El sistema 600 informático también puede incluir una interfaz 624 de comunicaciones. La interfaz 624 de comunicaciones puede configurarse para permitir que software y datos se transfieran entre el sistema 600 informático y dispositivos externos. Interfaces 624 de comunicaciones ejemplares pueden incluir un módem, una interfaz de red (por ejemplo, una tarjeta de Ethernet), un puerto de comunicaciones, una ranura y tarjeta PCMCIA, etc. El software y datos transferidos mediante la interfaz 624 de comunicaciones pueden estar en forma de señales, que pueden ser electrónicas, electromagnéticas, ópticas u otras señales como será evidente para los expertos en la materia. Las señales pueden viajar a través de una ruta 626 de comunicaciones, que puede configurarse para transportar las señales y puede implementarse usando alambre, cable, fibra óptica, una línea telefónica, un enlace de teléfono celular, un enlace de frecuencia de radio, etc.

El sistema 600 informático puede incluir adicionalmente una interfaz 602 de visualización. La interfaz 602 de visualización puede estar configurada para permitir que se transfieran datos entre el sistema 600 informático y la pantalla 630 externa. Interfaces 602 de visualización ejemplares pueden incluir la interfaz multimedia de alta definición (HDMI), interfaz visual digital (DVI), conjunto de gráficos de vídeo (VGA), etc. La pantalla 630 puede ser cualquier tipo adecuado de pantalla para visualizar datos transmitidos mediante la interfaz 602 de pantalla del sistema 600 informático, que incluyen una pantalla de tubo de rayos catódicos (CRT), pantalla de cristal líquido (LCD), pantalla de diodo de emisión de luz (LED), pantalla táctil capacitiva, pantalla de transistor de película delgada (TFT), etc.

Medio de programa informático y medio usable por ordenador pueden referirse a memorias, tal como la memoria 608 principal y memoria 610 secundaria, que pueden ser semiconductores de memoria (por ejemplo, DRAM, etc.). Estos productos de programa informático pueden ser medios para proporcionar software al sistema 600 informático. Los programas informáticos (por ejemplo, lógica de control de ordenador) pueden almacenarse en la memoria 608 principal y/o la memoria 610 secundaria. También pueden recibirse programas informáticos a través de la interfaz 624 de comunicaciones. Tales programas informáticos, cuando se ejecutan, pueden posibilitar que el sistema 600 informático implemente los presentes métodos como se analizan en el presente documento. En particular, los programas informáticos, cuando se ejecutan, pueden posibilitar que el dispositivo 604 de procesador implemente los métodos ilustrados por las Figuras 3-5, como se analiza en este documento. En consecuencia, tales programas informáticos pueden representar controladores del sistema 600 informático. Cuando la presente divulgación se implementa usando software, el software puede almacenarse en un producto de programa informático y cargarse en el sistema 600 informático usando la unidad 614 de disco de almacenamiento extraíble, interfaz 620 y unidad 612 de disco duro o interfaz 624 de comunicaciones.

El dispositivo 604 procesador puede comprender uno o más módulos o motores configurados para realizar las funciones del sistema 600 informático. Cada uno de los módulos o motores puede implementarse usando hardware y, en algunos casos, puede utilizarse también software, tal como correspondiendo a código de programa y/o programas almacenados en la memoria 608 principal o memoria 610 secundaria. En tales casos, el código de programa puede compilarse por el dispositivo 604 procesador (por ejemplo, por un módulo o motor de compilación) antes de la ejecución por el hardware del sistema 600 informático. Por ejemplo, el código de programa puede ser código fuente escrito en un lenguaje de programación que se traduce en un lenguaje de nivel inferior, tal como lenguaje ensamblador o código máquina, para su ejecución por el dispositivo 604 procesador y/o cualesquiera componentes de hardware adicionales del sistema 600 informático. El proceso de compilación puede incluir el uso de análisis léxico, preprocesamiento, análisis, análisis semántico, traducción de sintaxis dirigida, generación de código, optimización de código y cualesquiera otras técnicas que pueden ser adecuadas para la traducción de código de programa en un lenguaje de nivel inferior adecuado para controlar el sistema 600 informático para realizar las funciones desveladas en el presente documento. Será evidente para los expertos en la materia que tales procesos dan como resultado que el sistema 600 informático sea un sistema 600 informático especialmente configurado programado de manera inequívoca para realizar las funciones anteriormente analizadas.

Las técnicas consistentes con la presente divulgación proporcionan, entre otras características, sistemas y métodos para distribuir múltiples claves criptográficas usadas para acceder a datos. Aunque se han descrito anteriormente diversas realizaciones ilustrativas del sistema y método divulgados, debería entenderse que se han presentado para fines de ejemplo únicamente, no como limitaciones. No es exhaustivo y no limita la divulgación a la forma precisa divulgada. Son posibles modificaciones y variaciones a la luz de las enseñanzas anteriores o pueden obtenerse a partir de la puesta en práctica de la divulgación, sin alejarse del alcance o ámbito.

REIVINDICACIONES

1. Un método para distribuir múltiples claves criptográficas usadas para acceder a datos, que comprende:

recibir (502), por un dispositivo de recepción de un servidor de procesamiento, una señal de datos que comprende una solicitud de clave de acceso, en el que la solicitud de clave de acceso incluye al menos un número, n, mayor que 1, de claves solicitadas;
generar (504), por un módulo de generación del servidor de procesamiento, n pares de claves usando un algoritmo de generación de par de claves, en el que cada par de claves incluye una clave privada y una clave pública;
derivar (506), por un módulo de derivación del servidor de procesamiento, una clave privada de acceso aplicando la clave privada incluida en cada uno de los n pares de claves a un algoritmo de derivación de clave, en el que la clave privada de acceso se usa para restringir el acceso a datos;
generar (508), por el módulo de generación del servidor de procesamiento, una clave pública de acceso que corresponde a la clave privada de acceso derivada usando el algoritmo de generación de par de claves; y
transmitir (510) electrónicamente, por un dispositivo de transmisión del servidor de procesamiento, una señal de datos que comprende una clave privada incluida en uno de los *n* pares de claves para cada uno de los *n* pares de claves a cada uno de los n dispositivos informáticos de manera que cada uno de los n dispositivos informáticos recibe una clave privada diferente, comprendiendo el método adicionalmente:

almacenar, en una memoria del servidor de procesamiento, un par de claves de transferencia que incluye una clave pública de transferencia y una clave privada de transferencia;
recibir, por el dispositivo de recepción del servidor de procesamiento, una señal de datos que comprende una clave pública compartida de cada uno de los *n* dispositivos informáticos;
generar, por el módulo de generación del servidor de procesamiento, *n* secretos compartidos, en el que cada secreto compartido se genera usando una clave pública compartida de las *n* claves públicas compartidas y la clave privada de transferencia y el algoritmo de generación de par de claves; y
encriptar, por un módulo de encriptación del servidor de procesamiento, la clave privada incluida en cada uno de los *n* pares de claves con uno de los *n* secretos compartidos usando un algoritmo de encriptación, en el que la clave privada comprendida por la señal de datos transmitida electrónicamente es la respectiva clave privada encriptada.

2. El método de la reivindicación 1, que comprende adicionalmente:
transmitir electrónicamente, por el dispositivo de transmisión del servidor de procesamiento, una señal de datos que comprende la clave pública de transferencia a los *n* dispositivos informáticos.

3. El método de la reivindicación 2, en el que la señal de datos que comprende la clave pública de transferencia se transmite electrónicamente a los *n* dispositivos informáticos antes de recibir la señal de datos que comprende la clave pública compartida.

4. El método de la reivindicación 2, en el que cada señal de datos que comprende la clave pública de transferencia es una misma señal de datos que cada señal de datos que comprende una clave privada encriptada.

5. El método de la reivindicación 1, en el que la señal de datos transmitida se transmite electrónicamente a un nodo en una red de cadena de bloques y cuando la clave privada encriptada está incluida en una solicitud de transacción que incluye adicionalmente una dirección de destino que corresponde a la respectiva clave pública compartida.

6. El método de la reivindicación 1, en el que el algoritmo de derivación de clave incluye el uso de una operación lógica XOR.

7. El método de la reivindicación 1, que comprende adicionalmente:
transmitir electrónicamente, por el dispositivo de transmisión del servidor de procesamiento, una señal de datos que comprende una solicitud de transacción a un nodo en una red de cadena de bloques, en el que la solicitud de transacción incluye al menos una dirección de destino firmada usando la clave privada de acceso derivada.

8. Un sistema para distribuir múltiples claves criptográficas usadas para acceder a datos, que comprende:

un dispositivo (214) de transmisión de un servidor de procesamiento;
un dispositivo (202) de recepción del servidor de procesamiento configurado para recibir una señal de datos que comprende una solicitud de clave de acceso, en el que la solicitud de clave de acceso incluye al menos un número, *n*, de claves solicitadas;
un módulo (206) de generación del servidor de procesamiento configurado para generar *n* pares de claves usando un algoritmo de generación de par de claves, en el que cada par de claves incluye una clave privada y una clave pública; y
un módulo (208) de derivación del servidor de procesamiento configurado para derivar una clave privada de acceso aplicando la clave privada incluida en cada uno de los *n* pares de claves a un algoritmo de derivación de clave, en el que se usa la clave privada de acceso para restringir el acceso a datos, en el que

el módulo de generación del servidor de procesamiento está configurado adicionalmente para generar una clave pública de acceso que corresponde a la clave privada de acceso derivada usando el algoritmo de generación de par de claves, y
el dispositivo de transmisión del servidor de procesamiento está configurado para transmitir electrónicamente una señal de datos que comprende una clave privada incluida en uno de los *n* pares de claves para cada uno de los *n* pares de claves a cada uno de n dispositivos informáticos de manera que cada uno de los n dispositivos informáticos recibe una clave privada diferente, comprendiendo adicionalmente el sistema:

un módulo (210) de encriptación del servidor de procesamiento; y
una memoria (216) del servidor de procesamiento configurada para almacenar un par de claves de transferencia que incluye una clave pública de transferencia y una clave privada de transferencia, en el que
el dispositivo de recepción del servidor de procesamiento está configurado adicionalmente para recibir una señal de datos que comprende una clave pública compartida de cada uno de los n dispositivos informáticos,
el módulo de generación del servidor de procesamiento está configurado adicionalmente para generar n secretos compartidos, en el que cada secreto compartido se genera usando una clave pública compartida de las *n* claves públicas compartidas y la clave privada de transferencia y el algoritmo de generación de par de claves,
el módulo de encriptación del servidor de procesamiento está configurado para encriptar la clave privada incluida en cada uno de los *n* pares de claves con uno de los *n* secretos compartidos usando un algoritmo de encriptación, y
la clave privada comprendida por la señal de datos transmitida electrónicamente es la respectiva clave privada encriptada.

9. El sistema de la reivindicación 8, en el que el dispositivo de transmisión del servidor de procesamiento está configurado adicionalmente para transmitir electrónicamente una señal de datos que comprende la clave pública de transferencia a los *n* dispositivos informáticos.

10. El sistema de la reivindicación 9, en el que la señal de datos que comprende la clave pública de transferencia se transmite electrónicamente a los *n* dispositivos informáticos antes de recibir la señal de datos que comprende la clave pública compartida.

11. El sistema de la reivindicación 9, en el que cada señal de datos que comprende la clave pública de transferencia es una misma señal de datos que cada señal de datos que comprende una clave privada encriptada.

12. El sistema de la reivindicación 8, en el que la señal de datos transmitida se transmite electrónicamente a un nodo en una red de cadena de bloques y cuando la clave privada encriptada está incluida en una solicitud de transacción que incluye adicionalmente una dirección de destino que corresponde a la respectiva clave pública compartida.

13. El sistema de la reivindicación 8, en el que el algoritmo de derivación de clave incluye el uso de una operación lógica XOR.

14. El sistema de la reivindicación 8, en el que el dispositivo de transmisión del servidor de procesamiento está configurado adicionalmente para transmitir electrónicamente una señal de datos que comprende una solicitud de transacción a un nodo en una red de cadena de bloques, en el que la solicitud de transacción incluye al menos una dirección de destino firmada usando la clave privada de acceso derivada.

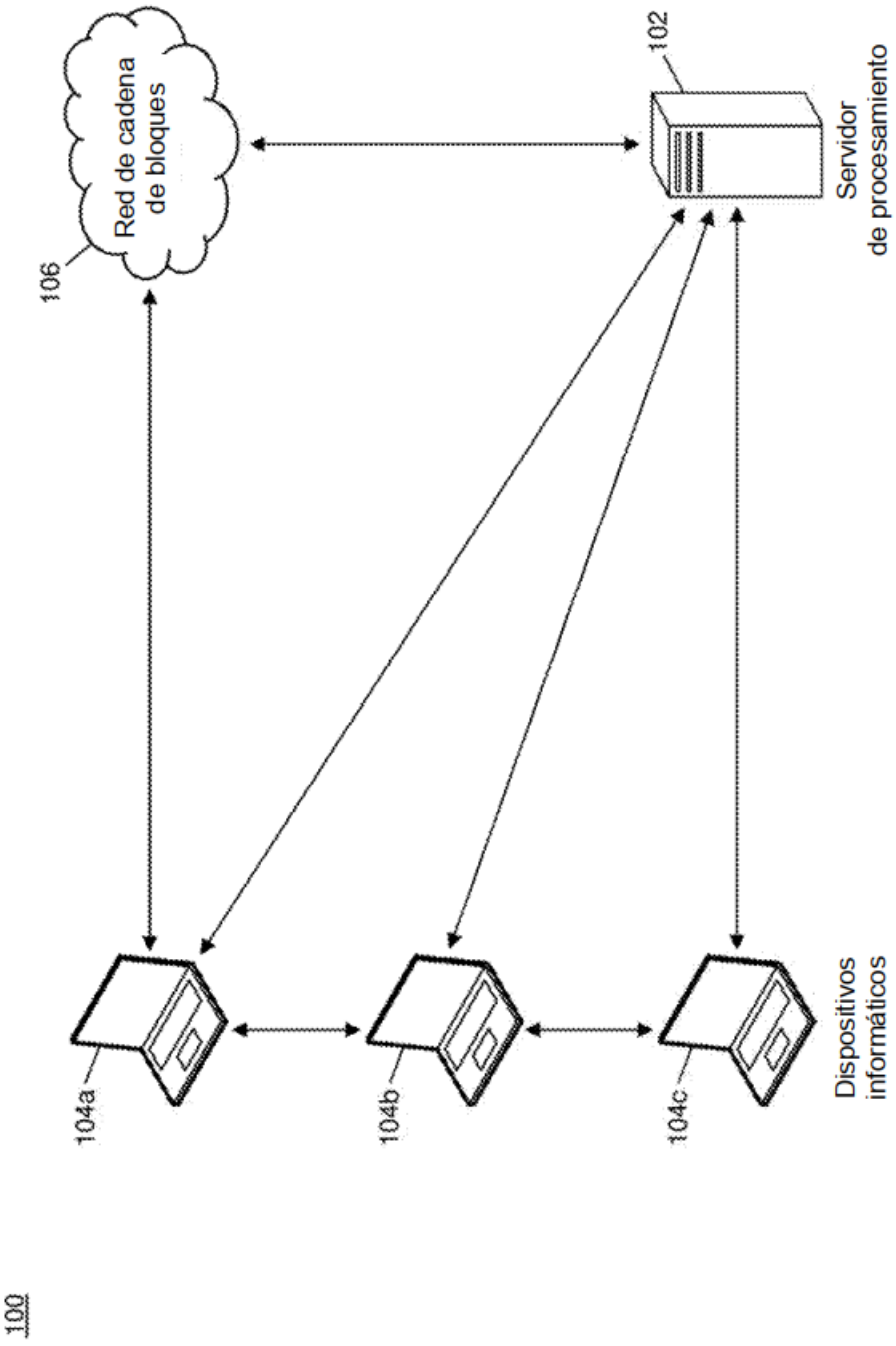
Red de cadena de bloques
106
102
Servidor de procesamiento
104a
104b
104c
Dispositivos informáticos
100

FIG. 1

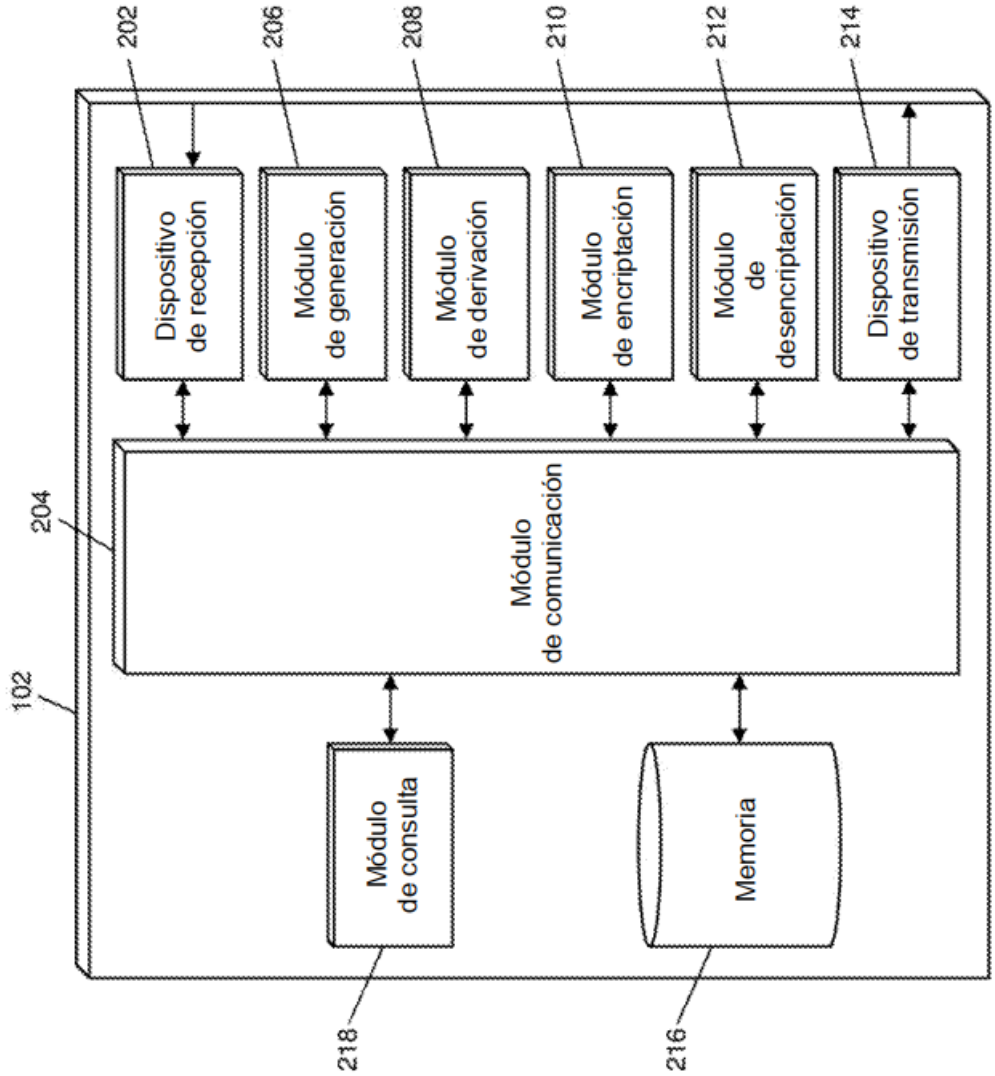
202
206
208
210
212
214
Dispositivo de recepción
Módulo de generación
Módulo de derivación
Módulo de encriptación
Módulo de desencriptación
Dispositivo de transmisión
204
Módulo de comunicación
102
Módulo de consulta
Memoria
218
216

FIG. 2

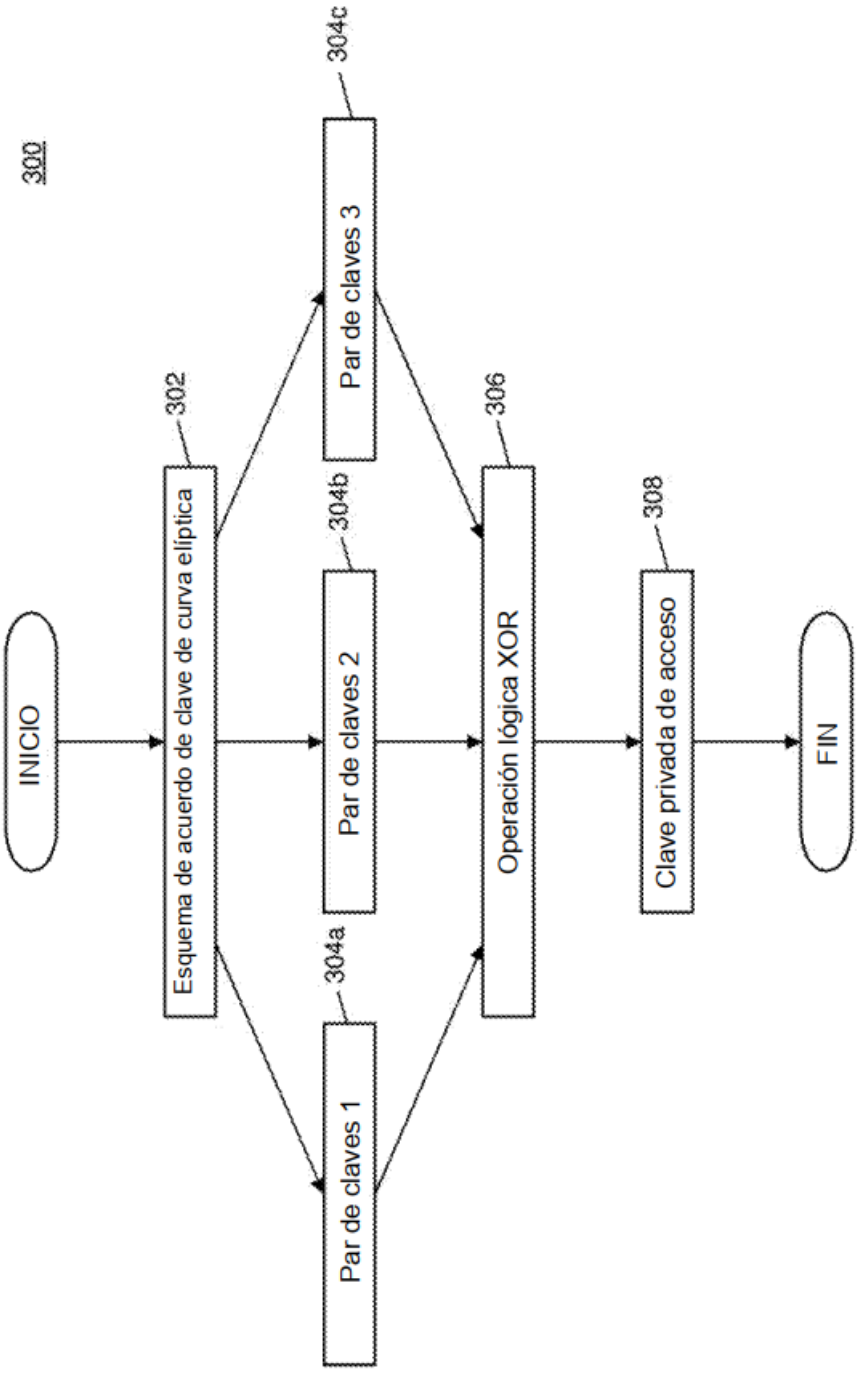
300
INICIO
302
Esquema de acuerdo de clave de curva elíptica
304a
Par de claves 1
304b
Par de claves 2
304c
Par de claves 3
306
Operación lógica XOR
308
Clave privada de acceso
FIN

FIG. 3

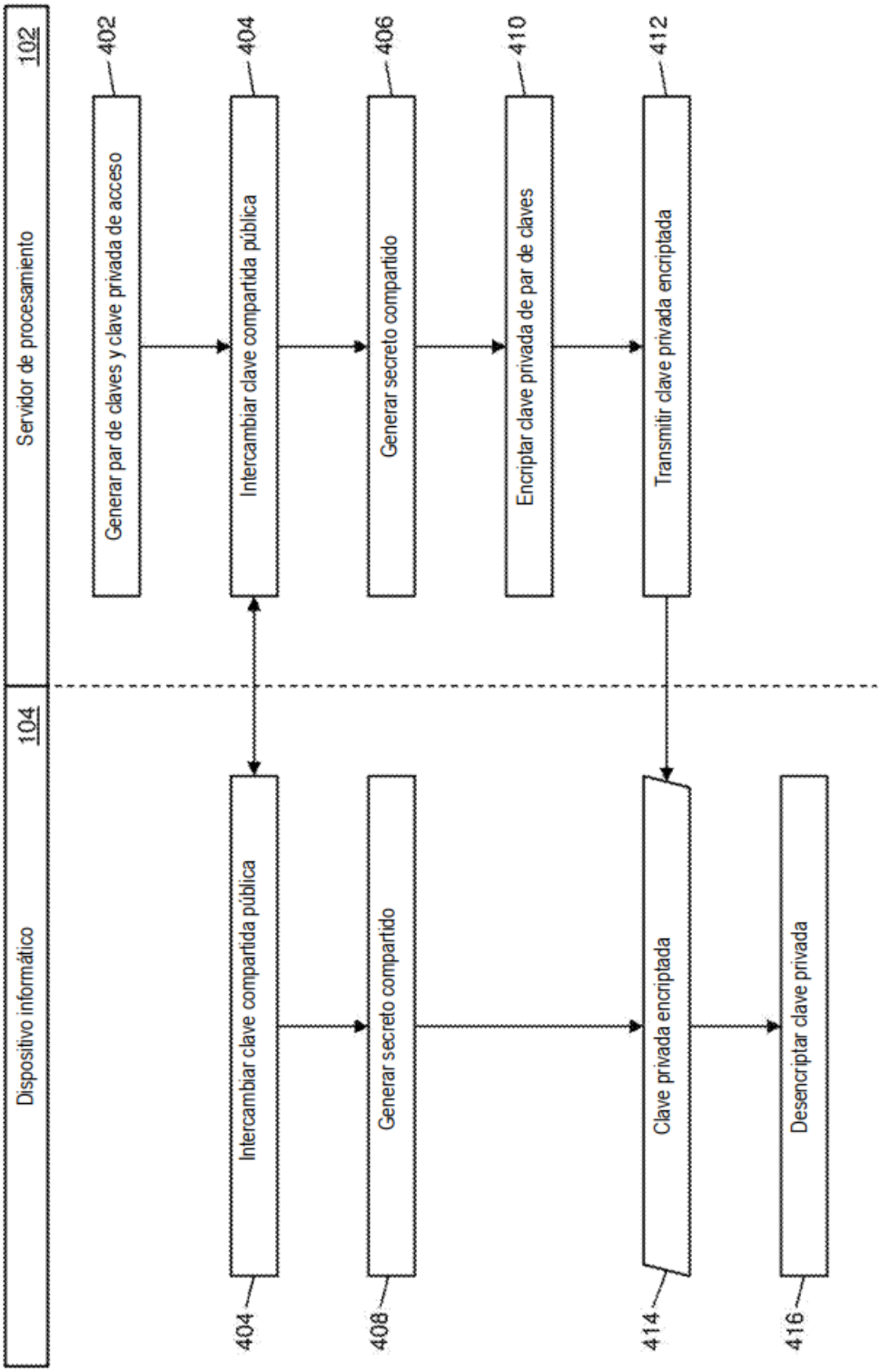
Servidor de procesamiento
102
Dispositivo informático
104
402
Generar par de claves y clave privada de acceso
404
Intercambiar clave compartida pública
406
Generar secreto compartido
410
Encriptar clave privada de par de claves
412
Transmitir clave privada encriptada
404
Intercambiar clave compartida pública
408
Generar secreto compartido
414
Clave privada encriptada
416
Desencriptar clave privada

FIG. 4

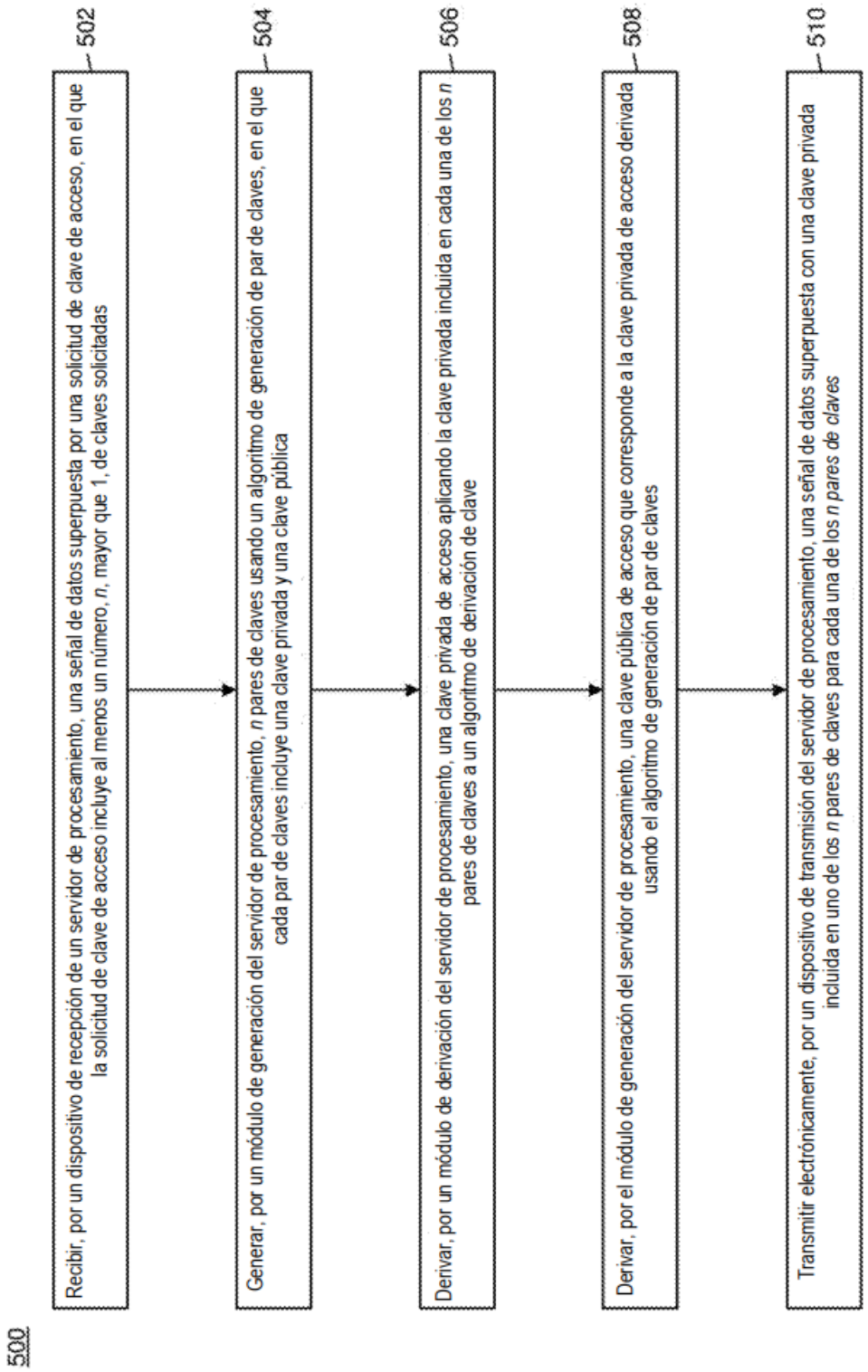
500
502
Recibir, por un dispositivo de recepción de un servidor de procesamiento, una señal de datos superpuesta por una solicitud de clave de acceso, en el que la solicitud de clave de acceso incluye al menos un número, n, mayor que 1, de claves solicitadas
504
Generar, por un módulo de generación del servidor de procesamiento, n pares de claves usando un algoritmo de generación de par de claves, en el que cada par de claves incluye una clave privada y una clave pública
506
Derivar, por un módulo de derivación del servidor de procesamiento, una clave privada de acceso aplicando la clave privada incluida en cada una de los n pares de claves a un algoritmo de derivación de clave
508
Derivar, por el módulo de generación del servidor de procesamiento, una clave pública de acceso que corresponde a la clave privada de acceso derivada usando el algoritmo de generación de par de claves
510
Transmitir electrónicamente, por un dispositivo de transmisión del servidor de procesamiento, una señal de datos superpuesta con una clave privada incluida en uno de los n pares de claves para cada una de los n pares de claves

FIG. 5

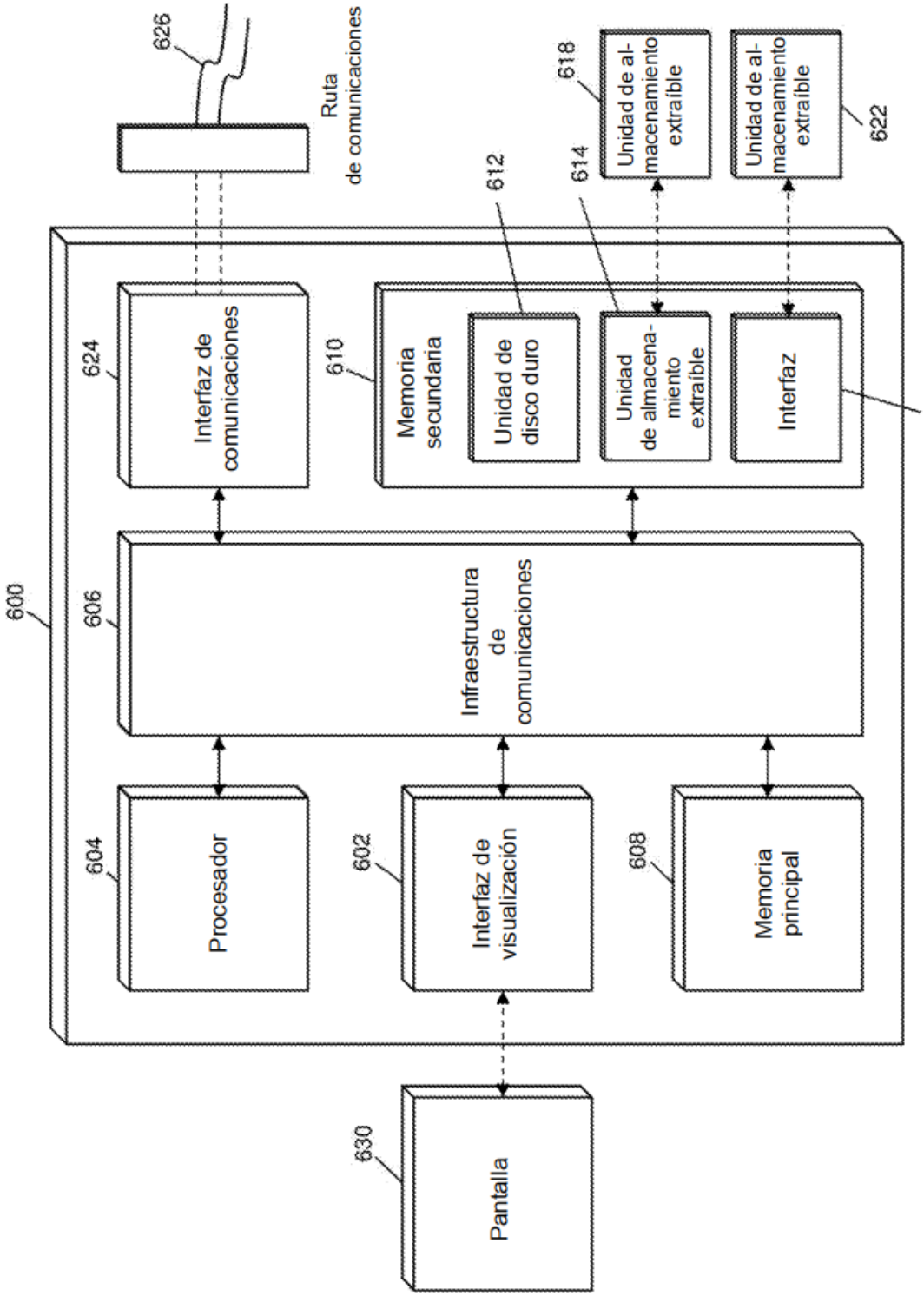
626
Ruta de comunicaciones
618
Unidad de almacenamiento extraíble
622
612
614
Unidad de almacenamiento extraíble
624
Interfaz de comunicaciones
610
Memoria secundaria
Unidad de disco duro
Unidad de almacenamiento extraíble
Interfaz
620
600
606
Infraestructura de comunicaciones
604
Procesador
602
Interfaz de visualización
608
Memoria principal
630
Pantalla

FIG. 6