

DETERMINACIÓN DE UN SECRETO COMÚN PARA EL INTERCAMBIO SEGURO DE INFORMACIÓN Y CLAVES CRIPTOGRÁFICAS DETERMINISTAS Y JERÁRQUICAS

CAMPO DE LA INVENCION

5

La presente divulgación se refiere a la determinación de un secreto común para dos nodos. En algunas aplicaciones, el secreto común se puede utilizar para la criptografía para permitir la comunicación segura entre dos nodos. La invención puede ser adecuada para su uso con, pero no limitado a, monederos digitales, tecnologías de cadena de bloques (por ejemplo, Bitcoin) y seguridad de dispositivos personales.

10

ANTECEDENTES DE LA INVENCION

La criptografía implica técnicas para la comunicación segura entre dos o más nodos. Un nodo puede incluir un dispositivo de comunicación móvil, una tableta, una computadora portátil, una computadora de escritorio, otras formas de dispositivos informáticos y dispositivos de comunicación, un dispositivo servidor en una red, un dispositivo cliente en una red, uno o más nodos en una red distribuida, etc. Los nodos pueden estar asociados con una persona física, un grupo de personas tal como los empleados de una empresa, un sistema tal como un sistema bancario, etc.

15

En algunos casos, los dos o más nodos pueden estar enlazados por una red de comunicaciones que no es segura. Por ejemplo, los dos nodos pueden estar enlazados por una red de comunicaciones donde un tercero puede ser capaz de escuchar furtivamente la comunicación entre los nodos. Por lo tanto, los mensajes enviados entre nodos se pueden enviar en forma encriptada y en donde, una vez recibidos, los destinatarios pueden descifrar los mensajes con clave(s) de descifrado correspondientes (u otros métodos de descifrado). De esta manera, la seguridad de tal comunicación puede depender en evitar que el tercero determine la clave de descifrado correspondiente.

20

25

Un método de criptografía incluye el uso de algoritmos de clave simétrica. Las claves son simétricas en el sentido de que se utiliza la misma clave simétrica tanto para la encriptación de un mensaje de texto sin formato como para la descifrado de texto cifrado. Una consideración del uso de algoritmos de clave simétrica es cómo transmitir la clave simétrica a ambos nodos de una manera segura para evitar que un espía adquiera la clave simétrica. Esto puede incluir, por ejemplo, la entrega de forma física de la clave simétrica a los nodos (autorizados) de modo que la clave simétrica nunca se transmita a través de una red de comunicaciones no segura. Sin embargo, la entrega física no siempre es una opción. Por lo tanto, un problema en sistemas

30

35

criptográficos de este tipo es el establecimiento de la clave simétrica (que se puede basar en un secreto común) entre los nodos a través de una red no segura. En los últimos tiempos, las situaciones pueden hacer que sea deseable que la transmisión de claves se realice usualmente de forma electrónica a través de sistemas de comunicaciones tal como el Internet. De esta manera, esta etapa de proporcionar un secreto compartido (por ejemplo, la clave simétrica) es una vulnerabilidad potencialmente catastrófica. Puesto que los algoritmos (y protocolos) de claves simétricas son simples y se utilizan de forma extendida, existe la necesidad de que dos nodos puedan determinar una clave secreta común de forma segura a través de una red no segura.

Otros métodos de criptografía existentes incluyen el uso de claves asimétricas. Estos se pueden utilizar en criptografía de claves públicas donde las claves asimétricas incluyen una clave privada y una clave pública correspondiente. La clave pública puede estar a disposición del público, mientras que la clave privada, como su nombre lo indica, se mantiene privada. Estas claves asimétricas se pueden utilizar para la encriptación de claves públicas y para la firma digital, entre otras cosas. Los protocolos existentes incluyen por ejemplo el Intercambio de Claves de Diffie-Hellman y el Protocolo de Tres Pasos que permiten la compartición segura de un secreto a través de redes no seguras. Sin embargo, estos métodos son caros de forma computacional en algunos casos, tales como cuando serán generados y compartidos de forma continua nuevos secretos.

Las jerarquías de claves asimétricas alternativas (tales como aquellas descritas en la Guía de Desarrolladores de Bitcoin) se basan en una semilla aleatoria y una estructura de índice que tiene como resultado una gestión de claves deficiente. Por el contrario, las modalidades de la presente invención pueden comprender el uso de "mensajes" significativos (M) para generar no solamente claves asimétricas sino también secretos deterministas jerárquicos compartidos que están asociados probablemente con datos específicos.

Cualquier discusión de documentos, actos, materiales, dispositivos, artículos o similares que se haya incluido en la presente especificación no se debe tomar como una admisión de que alguna o todas estas cuestiones forman parte de la base de la técnica anterior o que eran conocimientos generales comunes en el campo relevante para la presente divulgación tal como existía antes de la fecha de prioridad de cada reivindicación de esta solicitud.

A lo largo de esta especificación, la palabra "comprender", o variaciones tales como "comprende" o "que comprende", se entenderá que implica la inclusión de un elemento, entero o etapa establecido, o grupo de elementos, enteros o etapas, pero no la exclusión de cualquier otro elemento, entero o etapa, o grupo de elementos, enteros o etapas.

BREVE DESCRIPCIÓN DE LA INVENCION

De conformidad con un aspecto de la presente invención, se proporciona un método implementado por computadora de determinación de, en un primer nodo (C), un secreto común (CS) que es común con el primer nodo (C) y un segundo nodo (S), en donde el primer nodo (C) está asociado con un primer par de criptografía asimétrica que tiene una clave privada maestra de primer nodo (V_{1C}) y una clave pública maestra de primer nodo (P_{1C}), y el segundo nodo (S) está asociado con un segundo par de criptografía asimétrica que tiene una clave privada maestra de segundo nodo (V_{1S}) y una clave pública maestra de segundo nodo (P_{1S}), en donde el método comprende:

- determinar una segunda clave privada de primer nodo (V_{2C}) con base en por lo menos la clave privada maestra de primer nodo (V_{1C}) y una clave determinista (DK);
- determinar una segunda clave pública de segundo nodo (P_{2S}) con base en por lo menos la clave pública maestra de segundo nodo (P_{1S}) y la clave determinista (DK); y
- determinar el secreto común (CS) con base en la segunda clave privada de primer nodo (V_{2C}) y la segunda clave pública de segundo nodo (P_{2S}),

en donde el segundo nodo (S) tiene el mismo secreto común (CS) basado en una segunda clave pública de primer nodo (P_{2C}) y una segunda clave privada de segundo nodo (V_{2S}), en donde: la segunda clave pública de primer nodo (P_{2C}) se basa en por lo menos la clave pública maestra de primer nodo (P_{1C}) y la clave determinista (DK); y la segunda clave privada de segundo nodo (V_{2S}) se basa en por lo menos la clave privada maestra de segundo nodo (V_{1S}) y la clave determinista (DK).

Esto proporciona la ventaja de permitir que las segundas claves públicas se deriven independientemente en cada nodo, lo que aumenta de ese modo la seguridad, mientras que al mismo tiempo también permite a una máquina automatizar la generación de subclaves. También se proporciona la ventaja de tener entradas de transacción coincidentes que no se pueden rastrear, ya que la relación entre las claves públicas no puede ser determinada por terceros. De esta manera, esto permite que se logre un mayor nivel de anonimato, lo que mejora de ese modo la seguridad.

La clave determinista (DK) se puede basar en un mensaje (M). El método puede comprender adicionalmente: generar un primer mensaje firmado (SM1) con base en el mensaje (M) y la segunda clave privada de primer nodo (V_{2C}); y enviar, a través de la red de comunicaciones, el primer mensaje firmado (SM1) al segundo nodo (S), en donde el primer mensaje firmado (SM1) se puede validar con la segunda clave pública de primer nodo (P_{2C}) para autenticar el primer nodo (C).

El método también puede comprender: recibir, a través de la red de comunicaciones, un segundo mensaje firmado (SM2) procedente del segundo nodo (S); validar el segundo mensaje firmado (SM2) con la segunda clave pública de segundo nodo (P_{2S}); y autenticar el segundo nodo

(S) con base en el resultado de validar el segundo mensaje firmado (SM2), en donde el segundo mensaje firmado (SM2) se generó con base en el mensaje (M), o un segundo mensaje (M2), y la segunda clave privada de segundo nodo (V_{2S}).

El método puede comprender adicionalmente generar un mensaje (M); y enviar, a través de una red de comunicaciones, el mensaje (M) al segundo nodo (S). Alternativamente, el método puede comprender recibir el mensaje (M), a través de la red de comunicaciones, procedente del segundo nodo (S). En otra alternativa más, el método puede comprender recibir el mensaje (M), a través de la red de comunicaciones, procedente de otro nodo. En otra alternativa más, el método puede comprender recibir el mensaje (M) procedente de un almacén de datos, y/o una interfaz de entrada asociada con el primer nodo (C).

La clave pública maestra de primer nodo (P_{1C}) y la clave pública maestra de segundo nodo (P_{1S}) se pueden basar en una multiplicación de puntos de curva elíptica de respectivas clave privada maestra de primer nodo (V_{1C}) y clave privada maestra de segundo nodo (V_{1S}) y un generador (G).

El método puede comprender adicionalmente las etapas de: recibir, a través de la red de comunicaciones, la clave pública maestra de segundo nodo (P_{1S}); y almacenar, en un almacén de datos asociado con el primer nodo (C), la clave pública maestra de segundo nodo (P_{1S}).

El método puede comprender adicionalmente las etapas de: generar, en un primer nodo (C), la clave privada maestra de primer nodo (V_{1C}) y la clave pública maestra de primer nodo (P_{1C}); enviar, a través de la red de comunicaciones, la clave pública maestra de primer nodo (P_{1C}) al segundo nodo (S) y/u otro nodo; y almacenar, en un primer almacén de datos asociado con el primer nodo (C), la clave privada maestra de primer nodo (V_{1C}).

El método también puede comprender: enviar, a través de la red de comunicaciones, al segundo nodo, un aviso indicativo de utilizar un sistema de criptografía de curva elíptica (ECC) común con un generador común (G) para el método de determinación de un secreto común (CS). La etapa de generar la clave privada maestra de primer nodo (V_{1C}) y la clave pública maestra de primer nodo (P_{1C}) puede comprender: generar la clave privada maestra de primer nodo (V_{1C}) con base en un número entero aleatorio en un intervalo permisible especificado en el sistema ECC común; y determinar la clave pública maestra de primer nodo (P_{1C}) con base en una multiplicación de puntos de curva elíptica de la clave privada maestra de primer nodo (V_{1C}) y el generador común (G) de conformidad con la siguiente fórmula:

$$P_{1C} = V_{1C} \times G$$

El método puede comprender adicionalmente: determinar la clave determinista (DK) con base en una determinación de un hash (función de resumen) del mensaje (M), en donde la

etapa de determinar una segunda clave privada de primer nodo (V_{2C}) se basa en una adición escalar de la clave privada maestra de primer nodo (V_{1C}) y la clave determinista (DK) de conformidad con la siguiente fórmula:

$$V_{2C} = V_{1C} + DK$$

5

La etapa de determinar una segunda clave pública de segundo nodo (P_{2S}) se puede basar en la clave pública maestra de segundo nodo (P_{1S}) con una adición de puntos de curva elíptica a la multiplicación de puntos de curva elíptica de la clave determinista (DK) y el generador común (G) de conformidad con la siguiente fórmula:

10

$$P_{2S} = P_{1S} + DK \times G.$$

La clave determinista (DK) se puede basar en la determinación de un hash (función de resumen) de una clave determinista previa.

El primer par de criptografía asimétrica y el segundo par de criptografía asimétrica se pueden basar en una función de respectivos primer par de criptografía asimétrica previo y segundo par de criptografía asimétrica previo.

De conformidad con otro aspecto de la presente invención, se proporciona un método de comunicación segura entre un primer nodo y un segundo nodo con algoritmo de clave simétrica, en donde el método comprende:

20

- determinar una clave simétrica con base en el secreto común determinado de conformidad con el método descrito anteriormente;

- encriptar un primer mensaje de comunicación, con la clave simétrica, en un primer mensaje de comunicación encriptado; y

- enviar, a través de una red de comunicaciones, el primer mensaje de comunicación encriptado desde el primer nodo (C) al segundo nodo (S).

El método puede comprender adicionalmente: recibir, a través de una red de comunicaciones, un segundo mensaje de comunicación encriptado procedente del segundo nodo (S); y desencriptar el segundo mensaje de comunicación encriptado, con la clave simétrica, en un segundo mensaje de comunicación.

30

De conformidad con un aspecto adicional de la presente invención, se proporciona un método para llevar a cabo una transacción en línea entre un primer nodo y un segundo nodo, en donde el método comprende: determinar una clave simétrica con base en el secreto común determinado de acuerdo con el método de conformidad con el método descrito anteriormente; encriptar un primer mensaje de transacción, con la clave simétrica, en un primer mensaje de transacción encriptado; enviar, a través de una red de comunicaciones, el primer mensaje de

35

transacción encriptado desde el primer nodo (C) al segundo nodo (S); recibir, a través de una red de comunicaciones, un segundo mensaje de transacción encriptado procedente del segundo nodo (S); y desencriptar el segundo mensaje de transacción encriptado, con la clave simétrica, en un segundo mensaje de transacción.

5 De conformidad con un aspecto adicional de la presente invención, se proporciona un dispositivo para la determinación de, en un primer nodo (C), un secreto común (CS) que es común con un segundo nodo (S), en donde el primer nodo (C) está asociado con un primer par de criptografía asimétrica que tiene una clave privada maestra de primer nodo (V_{1C}) y una clave pública maestra de primer nodo (P_{1C}), y el segundo nodo (S) está asociado con un segundo par de
10 criptografía asimétrica que tiene una clave privada maestra de segundo nodo (V_{1S}) y una clave pública maestra de segundo nodo (P_{1S}), en donde el dispositivo comprende un primer dispositivo de procesamiento para llevar a cabo el método tal como se definió anteriormente para determinar el secreto común.

De conformidad con un aspecto adicional de la presente invención, se proporciona
15 un dispositivo para la comunicación segura, o la realización de una transacción en línea segura entre un primer nodo y un segundo nodo, en donde el dispositivo incluye un primer dispositivo de procesamiento para: llevar a cabo el método de comunicación segura o de transacción en línea segura descrito anteriormente.

El dispositivo puede comprender un primer almacén de datos para almacenar una o
20 más de la clave privada maestra de primer nodo (V_{1C}). El primer almacén de datos también puede almacenar una o más de la clave pública maestra de primer nodo (P_{1C}), la clave pública maestra de segundo nodo (P_{1S}) y el mensaje (M).

El dispositivo puede comprender adicionalmente un módulo de comunicaciones para enviar y/o recibir, a través de una red de comunicaciones, uno o más del mensaje (M), la clave
25 pública maestra de primer nodo (P_{1C}), la clave pública maestra de segundo nodo (P_{1S}), el primer mensaje firmado (SM1), el segundo mensaje firmado (SM2), el aviso indicativo de utilizar un sistema de criptografía de curva elíptica (ECC) común con un generador común (G).

De conformidad con un aspecto adicional de la presente invención, se proporciona un sistema para determinar un secreto común entre un primer nodo (C) y un segundo nodo (S), en
30 donde:

el primer nodo (C) está asociado con un primer par de criptografía asimétrica que tiene una clave privada maestra de primer nodo (V_{1C}) y una clave pública maestra de primer nodo (P_{1C}); y

- el segundo nodo (S) está asociado con un segundo par de criptografía asimétrica
35 que tiene una clave privada maestra de segundo nodo (V_{1S}) y una clave pública maestra de segundo

nodo (P_{1S}), y el sistema comprende:

- un primer dispositivo de procesamiento, asociado con el primer nodo (C), configurado para:

- determinar una segunda clave privada de primer nodo (V_{2C}) con base en por lo menos la clave privada maestra de primer nodo (V_{1C}) y una clave determinista (DK);

- determinar una segunda clave pública de segundo nodo (P_{2S}) con base en por lo menos la clave pública maestra de segundo nodo (P_{1S}) y la clave determinista (DK); y

- determinar el secreto común (CS) con base en la segunda clave privada de primer nodo (V_{2C}) y la segunda clave pública de segundo nodo (P_{2S}); y

- un segundo dispositivo de procesamiento, asociado con el segundo nodo (S), configurado para:

- determinar una segunda clave pública de primer nodo (P_{2C}) con base en por lo menos la clave pública maestra de primer nodo (P_{1C}) y la clave determinista (DK); y

- determinar una segunda clave privada de segundo nodo (V_{2S}) con base en por lo menos la clave privada maestra de segundo nodo (V_{1S}) y la clave determinista (DK); y

- determinar el secreto común con base en la segunda clave pública de primer nodo (P_{2C}) y una segunda clave privada de segundo nodo (V_{2S}),

en donde el primer dispositivo de procesamiento y el segundo dispositivo de procesamiento determinan el mismo secreto común (CS).

En el sistema, la clave determinista (DK) se basa en un mensaje (M) y el primer dispositivo de procesamiento está configurado adicionalmente para: generar un primer mensaje firmado (SM1) con base en el mensaje (M) y la segunda clave privada de primer nodo (V_{2C}); y enviar, a través de la red de comunicaciones, el primer mensaje firmado (SM1) al segundo nodo (S). El segundo dispositivo de procesamiento puede estar configurado adicionalmente para: recibir el primer mensaje firmado (SM1); validar el primer mensaje firmado (SM1) con la segunda clave pública de primer nodo (P_{2C}); y autenticar el primer nodo (C) con base en un resultado del primer mensaje firmado (SM1) validado.

En el sistema, el segundo dispositivo de procesamiento puede estar configurado adicionalmente para: generar un segundo mensaje firmado (SM2) con base en el mensaje (M), o un segundo mensaje (M2), y la segunda clave privada de segundo nodo (V_{2S}); enviar el segundo mensaje firmado (SM2) al primer nodo (C), en donde el primer dispositivo de procesamiento está configurado adicionalmente para: recibir el segundo mensaje firmado (SM2); validar el segundo mensaje firmado (SM2) con la segunda clave pública de segundo nodo (P_{2S}); autenticar el segundo nodo (S) con base en un resultado del segundo mensaje firmado (SM2) validado.

En el sistema, el primer dispositivo de procesamiento puede estar configurado

adicionalmente para: generar el mensaje (M); y enviar el mensaje (M), en donde el segundo dispositivo de procesamiento está configurado para: recibir el mensaje (M). En una alternativa, el mensaje es generado por otro nodo, en donde el primer dispositivo de procesamiento está configurado para: recibir el mensaje (M), y en donde el segundo dispositivo de procesamiento está configurado para recibir el mensaje (M).

En otra alternativa más, el sistema comprende un almacén de datos de sistema e/o interfaz de entrada, en donde el primer dispositivo de procesamiento y el segundo dispositivo de procesamiento reciben el mensaje (M), o el segundo mensaje (M2) procedente del almacén de datos de sistema e/o interfaz de entrada.

El primer dispositivo de procesamiento puede recibir la clave pública maestra de segundo nodo (P_{1S}) procedente del almacén de datos de sistema y/o dispositivo de entrada, y el segundo dispositivo de procesamiento puede recibir la clave pública maestra de primer nodo (P_{1C}) procedente del almacén de datos de sistema y/o dispositivo de entrada.

La clave pública maestra de primer nodo (P_{1C}), la clave pública maestra de segundo nodo (P_{1S}) se pueden basar en una multiplicación de puntos de curva elíptica de respectivas clave privada maestra de primer nodo (V_{1C}) y clave privada maestra de segundo nodo (V_{1S}) y un generador (G).

El sistema puede comprender adicionalmente: un primer almacén de datos asociado con el primer nodo (C) para almacenar la clave privada maestra de primer nodo (V_{1C}); y un segundo almacén de datos asociado con el segundo nodo (S) para almacenar la clave privada maestra de segundo nodo (V_{1S}).

En el sistema, el primer dispositivo de procesamiento puede estar configurado para: generar la clave privada maestra de primer nodo (V_{1C}) y la clave pública maestra de primer nodo (P_{1C}); enviar la clave pública maestra de primer nodo (P_{1C}); y almacenar la clave privada maestra de primer nodo (V_{1C}) en el primer almacén de datos, en donde el segundo dispositivo procesador está configurado para: generar la clave privada maestra de segundo nodo (V_{1S}) y la clave pública maestra de segundo nodo (P_{1S}); enviar la clave pública maestra de segundo nodo (P_{1S}); y almacenar la clave privada maestra de segundo nodo (V_{1S}) en el segundo almacén de datos.

En el sistema, el primer almacén de datos puede recibir y almacenar la clave pública maestra de segundo nodo (P_{1S}); y el segundo almacén de datos puede recibir y almacenar la clave pública maestra de primer nodo (P_{1C}).

En el sistema, el primer dispositivo de procesamiento puede estar configurado adicionalmente para: generar la clave privada maestra de primer nodo (V_{1C}) con base en un número entero aleatorio en un intervalo permisible especificado en un sistema de criptografía de curva elíptica (ECC) común; y determinar la clave pública maestra de primer nodo (P_{1C}) con base en una

multiplicación de puntos de curva elíptica de la clave privada maestra de primer nodo (V_{1C}) y un generador común (G) de conformidad con la fórmula:

$$P_{1C} = V_{1C} \times G$$

5 El segundo dispositivo de procesamiento puede estar configurado adicionalmente para: generar la clave privada maestra de segundo nodo (V_{1S}) con base en un número entero aleatorio en el intervalo permisible especificado en el sistema ECC común; y determinar la clave pública maestra de segundo nodo (P_{1S}) con base en la multiplicación de puntos de curva elíptica de la clave privada maestra de segundo nodo (V_{1S}) y el generador común (G) de conformidad con la
10 fórmula:

$$P_{1S} = V_{1S} \times G.$$

En el sistema, el primer dispositivo de procesamiento puede estar configurado para: determinar la clave determinista (DK) con base en un hash (función de resumen) del mensaje (M), y
15 en donde: la segunda clave privada de primer nodo (V_{2C}) se basa en una adición escalar de la clave privada maestra de primer nodo (V_{1C}) y la clave determinista (DK) de conformidad con la fórmula:

$$V_{2C} = V_{1C} + DK$$

20 y la segunda clave pública de segundo nodo (P_{2S}) se basa en la clave pública maestra de segundo nodo (P_{1S}) con una adición de puntos de curva elíptica a la multiplicación de puntos de curva elíptica de la clave determinista (DK) y el generador común (G) de conformidad con la siguiente fórmula:

$$P_{2S} = P_{1S} + DK \times G$$

25 El segundo dispositivo de procesamiento puede estar configurado adicionalmente para: determinar la clave determinista (DK) con base en un hash (función de resumen) del mensaje (M), y en donde la segunda clave privada de segundo nodo (V_{2S}) se basa en una adición escalar de la clave privada maestra de segundo nodo (V_{1S}) y la clave determinista (DK) de conformidad con la
30 fórmula:

$$V_{2S} = V_{1S} + DK$$

y la segunda clave pública de primer nodo (P_{2C}) se basa en la clave pública maestra de primer nodo (P_{1C}) con una adición de puntos de curva elíptica a la multiplicación de puntos de curva elíptica de la
35 clave determinista (DK) y el generador común (G) de conformidad con la siguiente fórmula:

$$P_{2C} = P_{1C} + DK \times G$$

El sistema puede comprender adicionalmente: un primer módulo de comunicaciones asociado con el primer dispositivo de procesamiento para enviar y/o recibir, a través de una red de comunicaciones, uno o más del mensaje (M), la clave pública maestra de primer nodo (P_{1C}), la clave pública maestra de segundo nodo (P_{1S}), el primer mensaje firmado (SM1), el segundo mensaje firmado (SM2) y un aviso indicativo de utilizar un sistema de criptografía de curva elíptica (ECC) común con un generador común (G); y un segundo módulo de comunicaciones asociado con el segundo dispositivo de procesamiento para enviar y/o recibir, a través de una red de comunicaciones, uno o más del mensaje (M), la clave pública maestra de primer nodo (P_{1C}), la clave pública maestra de segundo nodo (P_{1S}), el primer mensaje firmado (SM1), el segundo mensaje firmado (SM2) y el aviso indicativo de utilizar un sistema de criptografía de curva elíptica (ECC) común con un generador común (G).

En el sistema, la clave determinista (DK) se puede basar en la determinación de un hash (función de resumen) de una clave determinista previa.

En el sistema, el primer par de criptografía asimétrica y el segundo par de criptografía asimétrica se pueden basar en una función de respectivos primer par de criptografía asimétrica previo y segundo par de criptografía asimétrica previo.

De conformidad con un aspecto adicional de la presente invención, se proporciona un sistema para la comunicación segura entre un primer nodo y un segundo nodo con algoritmo de clave simétrica, en donde el sistema comprende: un sistema descrito anteriormente para determinar un secreto común con el primer dispositivo de procesamiento y el segundo dispositivo de procesamiento, en donde el primer dispositivo de procesamiento está configurado adicionalmente para: determinar una clave simétrica con base en el secreto común; encriptar un primer mensaje de comunicación, con la clave simétrica, en un primer mensaje de comunicación encriptado; y enviar el primer mensaje de comunicación encriptado. El segundo dispositivo de procesamiento está configurado adicionalmente para: determinar la misma clave simétrica con base en el secreto común; recibir el primer mensaje de comunicación encriptado; y desencriptar el primer mensaje de comunicación encriptado, con la clave simétrica, en el primer mensaje de comunicación.

En el sistema para la comunicación segura, el segundo dispositivo de procesamiento puede estar configurado adicionalmente para: encriptar un segundo mensaje de comunicación, con la clave simétrica, en el segundo mensaje de comunicación encriptado; y enviar el segundo mensaje de comunicación encriptado. El primer dispositivo de procesamiento puede estar configurado adicionalmente para: recibir el segundo mensaje de comunicación encriptado; desencriptar el segundo mensaje de comunicación encriptado, con la clave simétrica, en el segundo mensaje de

comunicación.

En el sistema descrito anteriormente, el primero y el segundo mensajes de comunicación pueden ser mensajes de transacción entre el primer nodo y el segundo nodo para una transacción en línea entre el primer nodo y el segundo nodo.

- 5 De conformidad con un aspecto adicional de la presente invención, se proporciona un programa de computadora que comprende instrucciones legibles por máquina para hacer que un dispositivo de procesamiento implemente cualquiera de los métodos descritos anteriormente.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

10

Los ejemplos de la presente divulgación se describirán con referencia a:

La Figura 1 es un diagrama esquemático de un sistema de ejemplo para determinar un secreto común para un primer nodo y un segundo nodo.

- 15 La Figura 2 es un diagrama de flujo de métodos implementados por computadora para la determinación de un secreto común;

la Figura 3 es un diagrama de flujo de métodos implementados por computadora para registrar el primero y el segundo nodos;

la Figura 4 es otro diagrama de flujo de métodos implementados por computadora para la determinación de un secreto común;

- 20 la Figura 5 es un diagrama de flujo de métodos implementados por computadora de comunicación segura entre el primer nodo y el segundo nodo;

la Figura 6 es un diagrama esquemático de un sistema de ejemplo para el alquiler de recursos electrónicos.

- 25 la Figura 7 es un diagrama esquemático de un sistema de ejemplo que aplica los métodos al reemplazo de contraseña;

la Figura 8 es un diagrama de flujo de métodos implementados por computadora para autenticar el primer nodo y el segundo nodo;

la Figura 9 es un ejemplo de una estructura de árbol de diferentes claves para diferentes fines;

- 30 la Figura 10 es un ejemplo de una estructura de árbol que utiliza el método de generación de clave maestra; y

la Figura 11 ilustra un esquema de un dispositivo de procesamiento de ejemplo.

DESCRIPCIÓN DETALLADA DE LA INVENCION

Panorama general

Ahora se describirán un método, un dispositivo y un sistema para determinar un secreto común (CS) en un primer nodo (C) que es el mismo secreto común en un segundo nodo (S). La Figura 1 ilustra un sistema 1 que incluye un primer nodo 3 que está en comunicación, a través de una red de comunicaciones 5, con un segundo nodo 7. El primer nodo 3 tiene un primer dispositivo de procesamiento asociado 23 y el segundo nodo 5 tiene un segundo dispositivo de procesamiento asociado 27. El primero y el segundo nodos 3, 7 pueden incluir un dispositivo electrónico, tal como una computadora, una tableta, un dispositivo de comunicación móvil, un servidor de computadora, etc. En uno de los ejemplos, el primer nodo 3 puede ser un dispositivo cliente y el segundo nodo 7 un servidor.

El primer nodo 3 está asociado con un primer par de criptografía asimétrica que tiene una clave privada maestra de primer nodo (V_{1C}) y una clave pública maestra de primer nodo (P_{1C}). El segundo nodo (7) está asociado con un segundo par de criptografía asimétrica que tiene una clave privada maestra de segundo nodo (V_{1S}) y una clave pública maestra de segundo nodo (P_{1S}). El primero y el segundo pares de criptografía asimétrica para los respectivos primero y segundo nodos 3, 7 se pueden generar durante el registro. Los métodos de registro 100, 200 llevados a cabo por el primero y el segundo nodo 3, 7 se describirán con más detalle a continuación con referencia a la Figura 3. La clave pública para cada nodo se puede compartir públicamente, tal como a través de la red de comunicaciones.

Para determinar el secreto común (CS) tanto en el primer nodo 3 como en el segundo nodo 7, los nodos 3, 7 llevan a cabo las etapas de los respectivos métodos 300, 400 sin comunicar claves privadas a través de la red de comunicaciones 5.

El método 300 llevado a cabo por el primer nodo 3 incluye determinar 330 una segunda clave privada de primer nodo (V_{2C}) con base en por lo menos la clave privada maestra de primer nodo (V_{1C}) y una clave determinista (DK). La clave determinista se puede basar en un mensaje (M) que es compartido entre el primero y el segundo nodos, que puede incluir la compartición del mensaje a través de la red de comunicaciones 5 tal como se describe con más detalle a continuación. El método 300 también incluye determinar 370 una segunda clave pública de segundo nodo (P_{2S}) con base en por lo menos la clave pública maestra de segundo nodo (P_{1S}) y la clave determinista (DK). El método 300 incluye determinar 380 el secreto común (CS) con base en la segunda clave privada de primer nodo (V_{2C}) y la segunda clave pública de segundo nodo (P_{2S}).

Es importante destacar que el mismo secreto común (CS) también se puede determinar en el segundo nodo 7 mediante el método 400. El método 400 determina 430 una

segunda clave pública de primer nodo (P_{2C}) con base en la clave pública maestra de primer nodo (P_{1C}) y la clave determinista (DK). El método 400 incluye adicionalmente determinar 470 una segunda clave privada de segundo nodo (V_{2S}) con base en la clave privada maestra de segundo nodo (V_{1S}) y la clave determinista (DK). El método 400 incluye determinar 480 el secreto común (CS) con base en la segunda clave privada de segundo nodo (V_{2S}) y la segunda clave pública de primer nodo (P_{2C}).

La red de comunicaciones 5 puede incluir una red de área local, una red de área amplia, redes celulares, red de radiocomunicación, el Internet, etc. Estas redes, donde los datos se pueden transmitir por medio de medios de comunicaciones tales como un cable eléctrico, fibra óptica o de manera inalámbrica, pueden ser susceptibles de ser escuchadas furtivamente, tal como por un espía 11. El método 300, 400 puede permitir que tanto el primer nodo 3 como el segundo nodo 7 determinen independientemente un secreto común sin transmitir el secreto común a través de la red de comunicaciones 5. De esta manera, una ventaja es que el secreto común (CS) se puede determinar de forma segura mediante cada nodo sin tener que transmitir una clave privada a través de una red de comunicaciones 5 potencialmente no segura. A su vez, el secreto común se puede utilizar como una clave secreta (o como la base de una clave secreta) para la comunicación encriptada entre el primero y el segundo nodos 3, 7 a través de la red de comunicaciones 5.

Los métodos 300, 400 pueden incluir etapas adicionales. El método 300 puede incluir, en el primer nodo 3, generar un mensaje firmado (SM1) con base en el mensaje (M) y la segunda clave privada de primer nodo (V_{2C}). El método 300 incluye adicionalmente enviar 360 el primer mensaje firmado (SM1), a través de la red de comunicaciones, al segundo nodo 7. A su vez, el segundo nodo 7 puede llevar a cabo las etapas de recibir 440 el primer mensaje firmado (SM1). El método 400 también incluye la etapa de validar 450 el primer mensaje firmado (SM1) con la segunda clave pública de primer nodo (P_{2C}) y autenticar 460 el primer nodo 3 con base en el resultado de validar el primer mensaje firmado (SM1). De forma ventajosa, esto permite que el segundo nodo 7 autentique que el primer nodo pretendido (donde se generó el primer mensaje firmado) es el primer nodo 3. Esto se basa en la suposición de que solamente el primer nodo 3 tiene acceso a la clave privada maestra de primer nodo (V_{1C}) y, por lo tanto, solamente el primer nodo 3 puede determinar la segunda clave privada de primer nodo (V_{2C}) para generar el primer mensaje firmado (SM1). Se debe apreciar que, de forma similar, un segundo mensaje firmado (SM2) se puede generar en el segundo nodo 7 y se puede enviar al primer nodo 3 de tal manera que el primer nodo 3 puede autenticar el segundo nodo 7, tal como en un escenario de red entre pares (peer-to-peer).

La compartición del mensaje (M) entre el primero y el segundo nodos se puede lograr de varias formas. En uno de los ejemplos, el mensaje se puede generar en el primer nodo 3,

el cual a continuación se envía, a través de la red de comunicaciones 5, al segundo nodo 7. De forma alternativa, el mensaje se puede generar en el segundo nodo 7 y a continuación se puede enviar, a través de la red de comunicaciones 5, al segundo nodo 7. En otro ejemplo más, el mensaje se puede generar en un tercer nodo 9 y el mensaje se puede enviar tanto al primero como al segundo nodos 3, 7. En otra alternativa más, un usuario puede ingresar el mensaje a través de una interfaz de usuario 15 para que sea recibido por el primero y el segundo nodos 3, 7. En otro ejemplo más, el mensaje (M) se puede recuperar de un almacén de datos 19 y se puede enviar al primero y al segundo nodos 3, 7. En algunos ejemplos, el mensaje (M) puede ser público y, por lo tanto, se puede transmitir a través de una red no segura 5.

En ejemplos adicionales, uno o más mensajes (M) se pueden almacenar en un almacén de datos 13, 17, 19, donde el mensaje puede estar asociado con una sesión, una transacción, etc., entre el primer nodo 3 y el segundo nodo 7. De esta manera, los mensajes (M) se pueden recuperar y utilizar para recrear, en los respectivos primero y segundo nodos 3, 7, el secreto común (CS) asociado con esa sesión, o transacción. De forma ventajosa, un registro para permitir la recreación del secreto común (CS) se puede mantener sin que el registro tenga que almacenarse de forma privada o transmitirse de forma segura. Esto puede ser ventajoso si se llevan a cabo numerosas transacciones en el primero y el segundo nodos 3, 7 y no sería práctico almacenar todos los mensajes (M) en los propios nodos.

20 Método de registro 100, 200

Se describirá un ejemplo de un método de registro 100, 200 con referencia a la Figura 3, donde el método 100 es llevado a cabo por el primer nodo 3 y el método 200 es llevado a cabo por el segundo nodo 7. Esto incluye establecer el primero y el segundo pares de criptografía asimétrica para los respectivos primero y segundo nodos 3, 7.

Los pares de criptografía asimétrica incluyen claves privadas y públicas asociadas, tales como aquellas utilizadas en la encriptación de claves públicas. En este ejemplo, los pares de criptografía asimétrica se generan utilizando Criptografía de Curva Elíptica (ECC) y las propiedades de operaciones de curva elíptica.

Los estándares para la ECC pueden incluir estándares conocidos tales como aquellos descritos por el Grupo de Estándares para la Criptografía Eficiente (www.sceq.org). La criptografía de curva elíptica también se describe en los documentos US 5,600,725, US 5,761,305, US 5,889,865, US 5,896,455, US 5,933,504, US 6,122,736, US 6,141,420, US 6,618,483, US 6,704,870, US 6,785,813, US 6,078,667, US 6,792,530.

En el método 100, 200, esto incluye el establecimiento del primero y el segundo nodos 110, 210 en un sistema ECC común y el uso de un generador común (G). En uno de los

ejemplos, el sistema ECC común se puede basar en secp256K1, que es un sistema ECC utilizado por Bitcoin. El generador común (G) se puede seleccionar, generar de forma aleatoria o asignar.

Pasando ahora al primer nodo 3, el método 100 incluye establecer 110 en el sistema ECC común y el generador común (G). Esto puede incluir recibir el sistema ECC común y el generador común procedentes del segundo nodo 7, o un tercer nodo 9. De forma alternativa, una interfaz de usuario 15 puede estar asociada con el primer nodo 3, por lo que un usuario puede proporcionar selectivamente el sistema ECC común y/o el generador común (G). En otra alternativa más, uno o ambos del sistema ECC común y/o el generador común (G) se pueden seleccionar de forma aleatoria mediante el primer nodo 3. El primer nodo 3 puede enviar, a través de la red de comunicaciones 5, un aviso indicativo de utilizar el sistema ECC común con un generador común (G) al segundo nodo 7. A su vez, el segundo nodo 7 se puede establecer 210 al enviar un aviso indicativo de un acuse de recibo para utilizar el sistema ECC común y el generador común (G).

El método 100 también incluye el primer nodo 3 que genera 120 un primer par de criptografía asimétrica que incluye la clave privada maestra de primer nodo (V_{1C}) y la clave pública maestra de primer nodo (P_{1C}). Esto incluye generar la clave privada maestra de primer nodo (V_{1C}) con base, por lo menos en parte, en un número entero aleatorio en un intervalo permisible especificado en el sistema ECC común. Esto también incluye determinar la clave pública maestra de primer nodo (P_{1C}) con base en una multiplicación de puntos de curva elíptica de la clave privada maestra de primer nodo (V_{1C}) y el generador común de conformidad con la fórmula:

20

$$P_{1C} = V_{1C} \times G \quad (\text{Ecuación 1})$$

De esta manera, el primer par de criptografía asimétrica incluye:

V_{1C} : La clave privada maestra de primer nodo que el primer nodo mantiene en secreto.

P_{1C} : La clave pública maestra de primer nodo que se da a conocer públicamente.

El primer nodo 3 puede almacenar la clave privada maestra de primer nodo (V_{1C}) y la clave pública maestra de primer nodo (P_{1C}) en un primer almacén de datos 13 asociado con el primer nodo 3. Por seguridad, la clave privada maestra de primer nodo (V_{1C}) se puede almacenar en una porción segura del primer almacén de datos 13 para asegurar que la clave permanezca privada.

El método 100 incluye adicionalmente enviar 130 la clave pública maestra de primer nodo (P_{1C}), a través de la red de comunicaciones 5, al segundo nodo 7. El segundo nodo 7 puede, en la recepción 220 de la clave pública maestra de primer nodo (P_{1C}), almacenar 230 la clave pública maestra de primer nodo (P_{1C}) en un segundo almacén de datos 17 asociado con el segundo nodo 7.

De forma similar al primer nodo 3, el método 200 del segundo nodo 7 incluye

generar 240 un segundo par de criptografía asimétrica que incluye la clave privada maestra de segundo nodo (V_{1S}) y la clave pública maestra de segundo nodo (P_{1S}). La clave privada maestra de segundo nodo (V_{1S}) también es un número entero aleatorio dentro del intervalo permisible. A su vez, la clave pública maestra de segundo nodo (P_{1S}) se determina mediante la siguiente fórmula:

5

$$P_{1S} = V_{1S} \times G \quad (\text{Ecuación 2})$$

De esta manera, el segundo par de criptografía asimétrica incluye:

10 V_{1S} : La clave privada maestra de segundo nodo que el segundo nodo mantiene en secreto.

P_{1S} : La clave pública maestra de segundo nodo que se da a conocer públicamente.

El segundo nodo 7 puede almacenar el segundo par de criptografía asimétrica en el segundo almacén de datos 17. El método 200 incluye adicionalmente enviar 250 la clave pública maestra de segundo nodo (P_{1S}) al primer nodo 3. A su vez, el primer nodo 3 puede recibir 140 y 15 almacena 150 la clave pública maestra de segundo nodo (P_{1S}).

Se debe apreciar que en algunas alternativas, las respectivas claves maestras públicas se pueden recibir y almacenar en un tercer almacén de datos 19 asociado con el tercer nodo 9 (tal como un tercero de confianza). Esto puede incluir a un tercero que actúa como un directorio público, tal como una autoridad de certificación. De esta manera, en algunos ejemplos, la 20 clave pública maestra de primer nodo (P_{1C}) se puede solicitar y recibir mediante el segundo nodo 7 solamente cuando se requiere la determinación del secreto común (CS)(y viceversa).

Solamente se puede necesitar que las etapas de registro tengan lugar una vez como una configuración inicial. Después de eso, las claves maestras se pueden reutilizar en un asunto seguro para generar secreto(s) comunes que dependen, entre otros, de la clave determinista (DK).

25

Iniciación de la sesión y determinación del secreto común mediante el primer nodo 3

Un ejemplo de la determinación de un secreto común (CS) se describirá ahora con referencia a la Figura 4. El secreto común (CS) se puede utilizar para una sesión, un tiempo, una transacción u otro fin en particular entre el primer nodo 3 y el segundo nodo 7 y puede no ser 30 deseable, o seguro, utilizar el mismo secreto común (CS). De esta manera, el secreto común (CS) se puede cambiar entre diferentes sesiones, tiempo, transacciones, etc.

Generación de un mensaje (M) 310

En este ejemplo, el método 300 llevado a cabo por el primer nodo 3 incluye generar 35 310 un mensaje (M). El mensaje (M) puede ser aleatorio, pseudoaleatorio o definido por el usuario.

En uno de los ejemplos, el mensaje (M) se basa en tiempo Unix y un nonce (y valor arbitrario). Por ejemplo, el mensaje (M) se puede proporcionar como:

$$\text{Mensaje (M)} = \text{Tiempo Unix} + \text{nonce} \quad (\text{Ecuación 3})$$

5

En algunos ejemplos, el mensaje (M) es arbitrario. Sin embargo, se debe apreciar que el mensaje (M) puede tener valores selectivos (tales como Tiempo Unix, etc.) que pueden ser útiles en algunas aplicaciones.

El método 300 incluye enviar 315 el mensaje (M), a través de la red de comunicaciones 3, al segundo nodo 7. El mensaje (M) se puede enviar a través de una red no segura ya que el mensaje (M) no incluye información sobre las claves privadas.

10

Determinación de una clave determinista 320

El método 300 incluye adicionalmente la etapa de determinar 320 una clave determinista (DK) con base en el mensaje (M). En este ejemplo, esto incluye determinar un hash (función de resumen) criptográfico del mensaje. Un ejemplo de un algoritmo hash (función de resumen) criptográfico incluye SHA-256 para crear una clave determinista (DK) de 256 bits. Es decir:

15

$$DK = \text{SHA-256}(M) \quad (\text{Ecuación 4})$$

20

Se apreciará que se pueden utilizar otros algoritmos hash (función de resumen). Esto puede incluir otros algoritmos hash (función de resumen) en la familia de Algoritmo de Hash Seguro (SHA). Algunos ejemplos en particular incluyen casos en el subconjunto SHA-3, que incluyen SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256. Otros algoritmos hash (función de resumen) pueden incluir aquellos en la familia RACE Integrity Primitives Evaluation Message Digest (RIPEMD). Un ejemplo en particular puede incluir RIPEMD-160. Otras funciones hash (funciones de resumen) pueden incluir familias basadas en la función hash Zémor-Tillich y funciones hash basadas en knapsack (mochila).

25

Determinación de una segunda clave privada de primer nodo 330

El método 300 a continuación incluye la etapa 330 de determinar 330 la segunda clave privada de primer nodo (V_{2c}) con base en la clave privada maestra de segundo nodo (V_{1c}) y la clave determinista (DK). Esto se puede basar en una adición escalar de la clave privada maestra de primer nodo (V_{1c}) y la clave determinista (DK) de conformidad con la siguiente fórmula:

30

35

$$V_{2C} = V_{1C} + DK \quad (\text{Ecuación 5})$$

De esta manera, la segunda clave privada de primer nodo (V_{2C}) no es un valor aleatorio, sino que más bien se deriva de forma determinista a partir de la clave privada maestra de primer nodo. La clave pública correspondiente en el par criptográfico, es decir, la segunda clave pública de primer nodo (P_{2C}), tiene la siguiente relación:

$$P_{2C} = V_{2C} \times G \quad (\text{Ecuación 6})$$

La sustitución de V_{2C} de la Ecuación 5 en la Ecuación 6 proporciona:

$$P_{2C} = (V_{1C} + DK) \times G \quad (\text{Ecuación 7})$$

Donde el operador '+' se refiere a la adición escalar y el operador 'x' se refiere a la multiplicación de puntos de curva elíptica. Obsérvese que el álgebra de la criptografía de curva elíptica es distributiva, la Ecuación 7 se puede expresar como:

$$P_{2C} = V_{1C} \times G + DK \times G \quad (\text{Ecuación 8})$$

Finalmente, la Ecuación 1 se puede sustituir en la Ecuación 7 para proporcionar:

$$P_{2C} = P_{1C} + DK \times G \quad (\text{Ecuación 9.1})$$

$$P_{2C} = P_{1C} + \text{SHA-256}(M) \times G \quad (\text{Ecuación 9.2})$$

En las Ecuaciones 8 a 9.2, el operador '+' se refiere a la adición de puntos de curva elíptica. De esta manera, la correspondiente segunda clave pública de primer nodo (P_{2C}) se puede derivar dado el conocimiento de la clave pública maestra de primer nodo (P_{1C}) y el mensaje (M). El segundo nodo 7 puede tener tal conocimiento para determinar de forma independiente la segunda clave pública de primer nodo (P_{2C}) tal como se discutirá con más detalle a continuación con respecto al método 400.

Generación de un primer mensaje firmado (SM1) con base en el mensaje y la segunda clave privada de primer nodo 350

El método 300 incluye adicionalmente generar 350 un primer mensaje firmado (SM1) con base en el mensaje (M) y la segunda clave privada de primer nodo (V_{2C}) determinada. La

generación de un mensaje firmado incluye aplicar un algoritmo de firma digital para firmar digitalmente el mensaje (M). En uno de los ejemplos, esto incluye aplicar la segunda clave privada de primer nodo (V_{2C}) al mensaje en un Algoritmo de Firma Digital para Curvas Elípticas (ECDSA) para obtener el primer mensaje firmado (SM1).

5 Los ejemplos de ECDSA incluyen aquellos basados en sistemas ECC con secp256k1, secp256r1, secp384r1, se3cp521r1.

El primer mensaje firmado (SM1) se puede verificar con la correspondiente segunda clave pública de primer nodo (P_{2C}) en el segundo nodo 7. Esta verificación del primer mensaje firmado (SM1) puede ser utilizada por el segundo nodo 7 para autenticar el primer nodo 3, lo cual se
10 discutirá en el método 400 a continuación.

Determinación de una segunda clave pública de segundo nodo 370'

El primer nodo 3 a continuación puede determinar 370 una segunda clave pública de segundo nodo (P_{2S}). Tal como se discutió anteriormente, la segunda clave pública de segundo nodo
15 (P_{2S}) se puede basar por lo menos en la clave pública maestra de segundo nodo (P_{1S}) y la clave determinista (DK). En este ejemplo, puesto que la clave pública se determina 370' como la clave privada con una multiplicación de puntos de curva elíptica con el generador (G), la segunda clave pública de segundo nodo (P_{2S}) se puede expresar, de manera similar a la Ecuación 6, como:

$$20 \quad P_{2S} = V_{2S} \times G \quad (\text{Ecuación 10.1})$$

$$P_{2S} = P_{1S} + DK \times G \quad (\text{Ecuación 10.2})$$

La demostración matemática para la Ecuación 10.2 es la misma que aquella descrita anteriormente para derivar la Ecuación 9.1 para la segunda clave pública de primer nodo (P_{2C}). Se
25 debe apreciar que el primer nodo 3 puede determinar 370 la segunda clave pública de segundo nodo independientemente del segundo nodo 7.

Determinación del secreto común 380 en el primer nodo 3

El primer nodo 3 a continuación puede determinar 380 el secreto común (CS) con
30 base en la segunda clave privada de primer nodo (V_{2C}) determinada y la segunda clave pública de segundo nodo (P_{2S}) determinada. El secreto común (CS) se puede determinar mediante el primer nodo 3 mediante la siguiente fórmula:

$$35 \quad S = V_{2C} \times P_{2S} \quad (\text{Ecuación 11})$$

Método 400 llevado a cabo en el segundo nodo 7

Ahora será descrito el correspondiente método 400 llevado a cabo en el segundo nodo 7. Se debe apreciar que algunas de estas etapas son similares a aquellas discutidas anteriormente que fueron llevadas a cabo por el primer nodo 3.

5 El método 400 incluye recibir 410 el mensaje (M), a través de la red de comunicaciones 5, procedente del primer nodo 3. Esto puede incluir el mensaje (M) enviado por el primer nodo 3 en la etapa 315. El segundo nodo 7 a continuación determina 420 una clave determinista (DK) con base en el mensaje (M). La etapa de determinar 420 la clave determinista (DK) por el segundo nodo 7 es similar a la etapa 320 llevada a cabo por el primer nodo descrito
10 anteriormente. En este ejemplo, el segundo nodo 7 lleva a cabo esta etapa de determinación 420 independiente del primer nodo 3.

La siguiente etapa incluye determinar 430 una segunda clave pública de primer nodo (P_{2C}) con base en la clave pública maestra de primer nodo (P_{1C}) y la clave determinista (DK). En este ejemplo, puesto que la clave pública se determina 430' como la clave privada con una
15 multiplicación de puntos de curva elíptica con el generador (G), la segunda clave pública de primer nodo (P_{2C}) se puede expresar, de manera similar a la Ecuación 9, como:

$$P_{2C} = V_{2C} \times G \quad (\text{Ecuación 12.1})$$

$$P_{2C} = P_{1C} + DK \times G \quad (\text{Ecuación 12.2})$$

20

La demostración matemática para las Ecuaciones 12.1 y 12.2 es la misma que aquella discutida anteriormente para las Ecuaciones 10.1 y 10.2.

El segundo nodo 7 que autentica el primer nodo 3

25 El método 400 puede incluir etapas llevadas a cabo por el segundo nodo 7 para autenticar que el supuesto primer nodo 3 es el primer nodo 3. Tal como se discutió previamente, esto incluye recibir 440 el primer mensaje firmado (SM1) procedente del primer nodo 3. El segundo nodo 7 a continuación puede validar 450 la firma en el primer mensaje firmado (SM1) con la segunda clave pública de primer nodo (P_{2C}) que se determinó en la etapa 430.

30 La verificación de la firma digital se puede realizar de acuerdo con un Algoritmo de Firma Digital para Curvas Elípticas (ECDSA) tal como se discutió anteriormente. Es importante destacar que el primer mensaje firmado (SM1) que se firmó con la segunda clave privada de primer nodo (V_{2C}) solo se debe verificar correctamente con la correspondiente segunda clave pública de primer nodo (P_{2C}), ya que V_{2C} y P_{2C} forman un par criptográfico. Puesto que estas claves son
35 deterministas en la clave privada maestra de primer nodo (V_{1C}) y la clave pública maestra de primer

nodo (P_{1C}) que se generaron en el registro del primer nodo 3, la verificación del primer mensaje firmado (SM_1) se puede utilizar como una base de autenticar que un supuesto primer nodo que envía el primer mensaje firmado (SM_1) es el mismo primer nodo 3 durante el registro. De esta manera, el segundo nodo 7 puede llevar a cabo adicionalmente la etapa de autenticar (460) el primer nodo 3 con base en el resultado de validar (450) el primer mensaje firmado.

La autenticación anterior puede ser adecuada para escenarios donde uno de los dos nodos es un nodo de confianza y solamente uno de los nodos necesita ser autenticado. Por ejemplo, el primer nodo 3 puede ser un cliente y el segundo nodo 7 puede ser un servidor de confianza del cliente. De esta manera, el servidor (segundo nodo 7) puede necesitar autenticar las credenciales del cliente (primer nodo 3) con el fin de permitir el acceso del cliente al sistema de servidor. Puede que no sea necesario que el servidor autentique las credenciales del servidor al cliente. Sin embargo, en algunos escenarios, puede ser deseable que ambos nodos se autenticquen entre sí, tal como en un escenario de red entre pares (peer-to-peer) que se describirá en otro ejemplo a continuación.

15

El segundo nodo 7 que determina el secreto común

El método 400 puede incluir adicionalmente la determinación 470 por parte del segundo nodo 7 de una segunda clave privada de segundo nodo (V_{2S}) con base en la clave privada maestra de segundo nodo (V_{1S}) y la clave determinista (DK). De forma similar a la etapa 330 llevada a cabo por el primer nodo, la segunda clave privada de segundo nodo (V_{2S}) se puede basar en una adición escalar de la clave privada maestra de segundo nodo (V_{1S}) y la clave determinista (DK) de conformidad con las siguientes fórmulas:

20

$$V_{2S} = V_{1S} + DK \quad (\text{Ecuación 13.1})$$

25

$$V_{2S} = V_{1S} + \text{SHA-256}(M) \quad (\text{Ecuación 13.2})$$

El segundo nodo 7 a continuación puede, independientemente del primer nodo 3, determinar 480 el secreto común (CS) con base en la segunda clave privada de segundo nodo (V_{2S}) y la segunda clave pública de primer nodo (P_{2C}) con base en la siguiente fórmula:

30

$$S = V_{2S} \times P_{2C} \quad (\text{Ecuación 14})$$

Demostración del secreto común (CS) determinado por el primer nodo 3 y el segundo nodo 7

35

El secreto común (CS) determinado por el primer nodo 3 es el mismo que el secreto

común (CS) determinado en el segundo nodo 7. Ahora se describirá la demostración matemática de que la Ecuación 11 y la Ecuación 14 proporcionan el mismo secreto común (CS).

Volviendo al secreto común (CS) determinado por el primer nodo 3, la Ecuación 10.1 se puede sustituir en la Ecuación 11 de la siguiente manera:

5

$$S = V_{2C} \times P_{2S} \quad (\text{Ecuación 11})$$

$$S = V_{2C} \times (V_{2S} \times G)$$

$$S = (V_{2C} \times V_{2S}) \times G \quad (\text{Ecuación 15})$$

10

Volviendo al secreto común (CS) determinado por el segundo nodo 7, la Ecuación 12.1 se puede sustituir en la Ecuación 14 de la siguiente manera:

$$S = V_{2S} \times P_{2C} \quad (\text{Ecuación 14})$$

$$S = V_{2S} \times (V_{2C} \times G)$$

15

$$S = (V_{2S} \times V_{2C}) \times G \quad (\text{Ecuación 16})$$

Puesto que el álgebra de ECC es conmutativa, la Ecuación 15 y la Ecuación 16 son equivalentes, ya que:

20

$$S = (V_{2C} \times V_{2S}) \times G = (V_{2S} \times V_{2C}) \times G \quad (\text{Ecuación 17})$$

El secreto común (CS) y la clave secreta

El secreto común (CS) se puede utilizar como una clave secreta, o como la base de una clave secreta en un algoritmo de clave simétrica para la comunicación segura entre el primer nodo 3 y el segundo nodo 7.

25

El secreto común (CS) puede tener la forma de un punto de curva elíptica (x_s, y_s). Este se puede convertir a un formato de clave estándar utilizando operaciones estándar públicamente conocidas acordadas por los nodos 3, 7. Por ejemplo, el valor x_s puede ser un número entero de 256 bits que se podría utilizar como una clave para la encriptación AES₂₅₆. También se podría convertir en un número entero de 160 bits utilizando RIPEMD160 para cualquier aplicación que requiera esta clave de longitud.

30

El secreto común (CS) se puede determinar según sea necesario. Es importante destacar que el primer nodo 3 no necesita almacenar el secreto común (CS), ya que este se puede volver a determinar con base en el mensaje (M). En algunos ejemplos, el/los mensaje(s) (M) utilizado(s) se puede(n) almacenar en el almacén de datos 13, 17, 19 (u otro almacén de datos) sin

35

el mismo nivel de seguridad que el requerido para las claves privadas maestras. En algunos ejemplos, el mensaje (M) puede estar a disposición del público.

5 Sin embargo, dependiendo de algunas aplicaciones, el secreto común (CS) se podría almacenar en el primer almacén de datos (X) asociado con el primer nodo, siempre que el secreto común (CS) se mantenga tan seguro como la clave privada maestra de primer nodo (V_{1C}).

Además, el sistema divulgado puede permitir la determinación de múltiples secretos comunes que pueden corresponder a múltiples claves secretas seguras con base en un único par de criptografía de claves maestras. Una ventaja de esto se puede ilustrar mediante el siguiente ejemplo.

10 En situaciones donde hay múltiples sesiones, cada una asociada con múltiples secretos comunes (CS) respectivos, puede ser deseable tener un registro asociado con esas múltiples sesiones para que los secretos comunes (CS) respectivos se puedan volver a determinar para el futuro. En sistemas conocidos, esto puede haber requerido que se almacenen múltiples claves secretas en un almacén de datos seguro, lo cual puede ser costoso o inconveniente de mantener. Por el contrario, el presente sistema tiene las claves privadas maestras mantenidas
15 seguras en los respectivos primero y segundo nodos, mientras que las otras claves deterministas, o mensaje (M), se pueden almacenar ya sea de forma segura o insegura. A pesar de que las claves deterministas (DK) o el mensaje (M) se almacenan de forma insegura, los múltiples secretos comunes (CS) se mantienen seguros ya que las claves privadas maestras necesarias para determinar los secretos comunes siguen siendo seguras.

20 El método también se puede utilizar para generar "claves de sesión" para enlaces de comunicación temporales, tal como para transmitir de forma segura contraseñas de inicio de sesión.

Aplicaciones de ejemplo

25 Los métodos, el dispositivo y el sistema de la presente divulgación pueden tener una serie de aplicaciones que incluyen, pero no se limitan a, aquellas que se describen a continuación.

Encriptación de mensajes

La presente divulgación se puede utilizar para facilitar la comunicación segura, en particular el envío y la recepción de mensajes de comunicación, entre el primer nodo 3 y el segundo
30 nodo 7 a través de una red de comunicaciones potencialmente no segura 5. Esto se puede lograr mediante el uso del secreto común (CS) como la base para una clave simétrica. Este método de determinación de un secreto común (CS) y uso de la clave simétrica para la encriptación y desencriptación de los mensajes de comunicación puede ser más eficiente desde el punto de vista de la computación en comparación con los métodos de encriptación de claves públicas conocidos.

35 Los métodos 500, 600 de comunicación segura entre el primer nodo 3 y el segundo

nodo 7 se describirán ahora con referencia a la Figura 5. El primer nodo 3 determina 510 una clave simétrica con base en el secreto común (CS) determinado en el método anterior. Esto puede incluir la conversión del secreto común (CS) a un formato de clave estándar. De forma similar, el segundo nodo 7 también puede determinar 610 la clave simétrica con base en el secreto común (CS).

5 Para enviar un primer mensaje de comunicación de forma segura desde el primer nodo 3, a través de la red de comunicaciones, al segundo nodo, el primer mensaje de comunicación se tiene que encriptar. De esta manera, la clave simétrica es utilizada por el primer nodo para la encriptación 520 de un primer mensaje de comunicación para formar un primer mensaje de comunicación encriptado, que a continuación se envía 530, a través de la red de comunicaciones 5, al segundo nodo 7. El segundo nodo 7, a su vez, recibe 620 el primer mensaje de comunicación encriptado 620 y descripta 630 el primer mensaje de comunicación encriptado, con la clave simétrica, en el primer mensaje de comunicación.

10 De forma similar, el segundo nodo 7 puede encriptar 640 un segundo mensaje de comunicación, con la clave simétrica, en un segundo mensaje de comunicación encriptado, que a continuación se envía 650 al primer nodo 3. El primer nodo 3 a continuación puede recibir 540 el segundo mensaje de comunicación encriptado, y descriptarlo 550 en el segundo mensaje de comunicación.

Monedero de criptomonedas

20 En otro ejemplo, el método se puede utilizar para la generación y la gestión de secretos comunes (CS) tales como claves secretas para transacciones de criptomonedas. Las claves de criptomonedas, tales como aquellas que se utilizan en las transacciones de Bitcoin, normalmente están asociadas a fondos y activos que se pueden intercambiar por valor.

Alquiler de recursos electrónicos

25 Un ejemplo de uso del método y el sistema para facilitar el alquiler de recursos electrónicos se describirá con referencia a la Figura 6. Esto ilustra un sistema 701 donde el primer nodo 3 está asociado a un cliente 703 y el segundo nodo 7 está asociado a un recurso electrónico, tal como una instalación de supercomputadora 707. De esta manera, el cliente 504 puede desear utilizar la instalación de supercomputadora 707 ubicada de forma remota para procesar grandes cantidades de datos confidenciales.

30 La instalación de supercomputadora 707 puede alquilar el tiempo de CPU de supercomputadora sobre una base de por tiempo y/o por ciclo de CPU. El cliente 703 puede registrarse con la instalación de supercomputadora al depositar su clave pública, tal como al enviar 130, a través de una red de comunicaciones 5, la clave pública maestra de primer nodo (P_{1C}) al

segundo nodo 7.

La instalación de supercomputadora 707 a continuación puede proporcionar software al cliente 703 para llevar a cabo procesos en segundo plano tales como establecer conexiones seguras que utilizan encriptación AES y para facilitar las etapas en el método 300 descrito anteriormente.

Cuando se lleva a cabo el método 300, el primer nodo 3 puede enviar a 360 un primer mensaje firmado (SM1) el cual, en parte, se basa en un mensaje (M) que incluye el Tiempo Unix concatenado con un nonce (valor arbitrario).

El segundo nodo 7 puede recibir 440 el primer mensaje firmado (SM1). El segundo nodo 7 puede llevar a cabo adicionalmente una etapa de determinar si el Tiempo Unix en el mensaje (M) está dentro de un valor permitido para el Tiempo Unix. Por ejemplo, el valor permitido para el Tiempo de Unix se puede establecer de conformidad con los Términos y Condiciones establecidos entre el cliente 703 y la instalación de supercomputadora 707. Por ejemplo, se puede requerir que el Tiempo Unix (del mensaje) esté dentro de un período establecido (por ejemplo, 300 segundos) de cuando la instalación de la supercomputadora recibe 440 el primer mensaje firmado (SM1). Si el Tiempo Unix en el mensaje (M) está fuera del tiempo permitido, no se aceptará el intercambio de datos confidenciales.

Las etapas anteriores pueden asegurar que la clave de sesión resultante, que se basa en el secreto común determinado (CS) en las etapas 380, 480, nunca se pueda reproducir en un momento posterior y que sea única para la sesión que se estableció. A continuación, se puede utilizar un protocolo para establecer una clave de sesión simétrica, tal como una clave de encriptación/desencriptación AES, durante el período de la sesión. La clave de sesión se utiliza para todas las comunicaciones entre el primer nodo 3 y el segundo nodo 7 durante el período de la sesión. Esto permite al cliente encriptar código y/o grandes cantidades de datos, enviarlos a la instalación de supercomputadora 707 para su procesamiento, y recibir resultados encriptados de nuevo procedentes de la instalación de supercomputadora 707.

Reemplazo, suplemento o alternativa de contraseña

El sistema y el método también se pueden utilizar como un reemplazo, suplemento o alternativa de de contraseña. Haciendo referencia a la Figura 7, se proporciona un sistema que incluye un primer nodo 3 asociado a un usuario y una pluralidad de nodos adicionales 7', 7'', 7'''. La pluralidad de nodos adicionales se puede asociar cada uno a respectivas instituciones que participan en el mismo protocolo. Por ejemplo, las instituciones pueden incluir bancos, proveedores de servicios, servicios gubernamentales, compañías de seguros, proveedores de telecomunicaciones, minoristas, etc.

El usuario 803 puede desear comunicarse con estas instituciones, de manera segura, para acceder a los servicios. En los sistemas conocidos, esto puede requerir que el usuario tenga múltiples contraseñas para iniciar sesión en cada una de las respectivas instituciones. No es deseable utilizar la misma contraseña para iniciar sesión en varias instituciones por razones de seguridad.

En este ejemplo, el usuario y las múltiples instituciones se establecen con usar el mismo protocolo. Esto puede incluir el establecimiento en el sistema ECC (tal como aquellos basados en secp256k1, secp256r1, secp384r1, secp521r1) y un generador (G). El usuario a continuación puede registrar y compartir la clave pública maestra de primer nodo (P_{1C}) con la pluralidad de instituciones y nodos adicionales asociados $7'$, $7''$, $7'''$. Los nodos adicionales $7'$, $7''$, $7'''$ pueden llevar a cabo cada uno etapas del método similar al segundo nodo 7 tal como se describió anteriormente.

Cada vez que el usuario 803 desea iniciar sesión en uno de los sitios web de una institución participante, no necesita utilizar una contraseña. En cambio, el protocolo reemplaza la necesidad de contraseñas para cada institución. Todo lo que se requiere en el primer nodo 3 es la Clave Pública de la Institución, que siempre está disponible, y el registro del usuario en las instituciones (que incluye el registro de la clave pública maestra de primer nodo (P_{1C}) con la institución). Puesto que el registro por parte del usuario con una institución es una práctica normal para utilizar servicios basados en la web, esto no es una carga para el usuario 803. Una vez que se ha completado el registro, se puede determinar, utilizar y volver a utilizar un secreto común (CS) en lugar de una contraseña. Por ejemplo, al comienzo de cada sesión, el primer nodo 3 puede generar 310 un mensaje (M) que se envía al nodo adicional $7'$, $7''$, $7'''$ implicado en la sesión. El mensaje (M) se utiliza para determinar 320, 420 una correspondiente clave determinista que a continuación es utilizada tanto por el primer nodo 3 como por el nodo adicional $7'$, $7''$, $7'''$ para determinar el secreto común (CS) tal como se describió en los métodos anteriores. De forma alternativa, el mensaje (M) se puede generar o recibir procedente del nodo adicional $7'$, $7''$, $7'''$. En otra alternativa más, el mensaje (M) puede ser un mensaje predeterminado que se almacena en un almacén de datos 13, 17, 19 accesible por el primer nodo 3 y/o el nodo adicional $7'$, $7''$, $7'''$.

Esta técnica elimina una importante carga de seguridad de las instituciones. En particular, ya no es necesario que guarden un archivo de contraseña (registro secreto de contraseñas o hash (función de resumen) de contraseñas) ya que el secreto común se puede volver a calcular a partir de información no secreta. Más bien, la institución solamente necesita mantener segura su propia clave privada maestra. Además, el usuario no necesita memorizar o almacenar de forma segura muchas contraseñas (una para cada institución), siempre y cuando puedan mantener segura su clave privada maestra de primer nodo (V_{1C}).

Variaciones

Algunas variaciones se describirán ahora con los siguientes ejemplos.

Autenticación de red entre pares (peer-to-peer)

- 5 En un escenario de red entre pares (peer-to-peer), el primer nodo 3 y el segundo nodo 7 pueden necesitar autenticar las credenciales entre sí. Un ejemplo de esto se describirá ahora con referencia a la Figura 8. En este ejemplo, las etapas del método 300, 400 para autenticar el primer nodo 3 con base en el primer mensaje firmado (SM1) validado son similares a las discutidas anteriormente.
- 10 Sin embargo, el método 400 llevado a cabo por el segundo nodo 7 incluye adicionalmente generar 462 un segundo mensaje firmado (SM2) con base en el mensaje (M) y la segunda clave privada de segundo nodo (V_{2s}). En algunas alternativas, el segundo mensaje firmado (SM2) se puede basar en un segundo mensaje (M2) y la segunda clave privada de segundo nodo (V_{2s}), donde el segundo mensaje (M2) se comparte con el primer nodo 3. El método 400 incluye
- 15 adicionalmente enviar 464 el segundo mensaje firmado (SM1), a través de la red de comunicaciones 5, al primer nodo 3.

- En el primer nodo 3, el método 300 incluye recibir el segundo mensaje firmado (SM2) procedente del segundo nodo 7. El método incluye validar 374 la firma en el segundo mensaje firmado (SM2) con la segunda clave pública de segundo nodo (P_{2s}) que se determinó en la
- 20 etapa 370. El método 300 a continuación puede incluir autenticar 376 el segundo nodo 7 con base en el resultado de validar el segundo mensaje firmado (SM2). Esto tiene como resultado que el primero y el segundo nodos 3, 7 se autentiquen entre sí.

Jerarquía de claves deterministas

- 25 En uno de los ejemplos, se puede determinar una serie de claves deterministas sucesivas, donde cada clave sucesiva se puede determinar con base en la clave determinista precedente.

- Por ejemplo, en lugar de repetir las etapas 310 a 370 y 410 a 470 para generar claves de propósito único sucesivas, por acuerdo previo entre los nodos, ambas partes pueden volver
- 30 a revisar de forma repetida la clave determinista (DK) utilizada anteriormente para establecer una jerarquía de claves deterministas. En efecto, la clave determinista, con base en el hash (función de resumen) de un mensaje (M), puede ser un mensaje de siguiente generación (M') para la siguiente generación de clave determinista (DK'). Hacer esto permite calcular generaciones sucesivas de secretos compartidos sin la necesidad de más transmisiones de establecimiento de protocolo, en
- 35 particular la transmisión de múltiples mensajes para cada generación de secretos comunes. El

secreto común de siguiente generación (CS') se puede calcular de la siguiente manera.

En primer lugar, tanto el primer nodo 3 como el segundo nodo 7 determinan independientemente la siguiente generación de la clave determinista (DK'). Esto es similar a las etapas 320 y 420, pero se adaptó con las siguientes fórmulas:

5

$$M' = \text{SHA-256}(M) \quad (\text{Ecuación 18})$$

$$DK' = \text{SHA-256}(M') \quad (\text{Ecuación 19.1})$$

$$DK' = \text{SHA-256}(\text{SHA-256}(M)) \quad (\text{Ecuación 19.2})$$

10

El primer nodo 3 a continuación puede determinar la siguiente generación de la segunda clave pública de segundo nodo (P_{2S}') y la segunda clave privada de primer nodo (V_{2C}') similar a las etapas 370 y 330 descritas anteriormente, pero adaptadas con las siguientes fórmulas:

$$P_{2S}' = P_{1S} + DK' \times G \quad (\text{Ecuación 20.1})$$

15

$$V_{2C}' = V_{1C} + DK' \quad (\text{Ecuación 20.2})$$

El segundo nodo 7 a continuación puede determinar la siguiente generación de la segunda clave pública de primer nodo (P_{2C}') y la segunda clave privada de segundo nodo (V_{2S}') similar a las etapas 430 y 470 descritas anteriormente, pero adaptadas con las siguientes fórmulas:

20

$$P_{2C}' = P_{1C} + DK' \times G \quad (\text{Ecuación 21.1})$$

$$V_{2S}' = V_{1S} + DK' \quad (\text{Ecuación 21.2})$$

25

El primer nodo 3 y el segundo nodo 7 a continuación pueden determinar cada uno el secreto común de siguiente generación (CS').

En particular, el primer nodo 3 determina el secreto común de siguiente generación (CS') con la fórmula:

$$CS' = V_{2C}' \times P_{2S}' \quad (\text{Ecuación 22})$$

30

El segundo nodo 7 determina el secreto común de siguiente generación (CS') con la fórmula:

$$CS' = V_{2S}' \times P_{2C}' \quad (\text{Ecuación 23})$$

35

Las generaciones posteriores (CS'', CS''', etc.) se pueden calcular de la misma manera para crear una jerarquía de cadena. Esta técnica requiere que tanto el primer nodo 3 como el segundo nodo 7 sigan el Mensaje original (M) o la clave determinista calculada originalmente (DK), y con qué nodo se relaciona. Puesto que esta información es públicamente conocida, no existen problemas de seguridad con respecto a la retención de esta información. Por consiguiente, esta información se puede mantener en 'tablas fragmentadas' ('tablas hash') (que vinculan valores hash con claves públicas) y se puede distribuir libremente a través de la red 5 (por ejemplo, utilizando Torrent). Además, si algún secreto común individual (CS) en la jerarquía se ve comprometido, esto no afecta la seguridad de ningún otro secreto común en la jerarquía, siempre que las claves privadas V_{1C} , V_{1S} permanezcan seguras.

Estructura de árbol de claves

Además de una jerarquía de cadena (lineal) tal como se describió anteriormente, se puede crear una jerarquía en la forma de estructura de árbol.

Con una estructura de árbol, se puede determinar una variedad de claves para diferentes fines, tales como claves de autenticación, claves de encriptación, claves de firma, claves de pago, etc. por lo que todas estas claves están vinculadas a una única clave maestra mantenida de forma segura. Esto se ilustra mejor en la Figura 9 que muestra una estructura de árbol 901 con una variedad de claves diferentes. Cada una de estas se puede utilizar para crear un secreto compartido con otra parte.

La ramificación de árboles se puede lograr de varias maneras, tres de las cuales se describen a continuación.

(i) Generación de claves maestras

En la jerarquía de cadena, cada nuevo 'enlace' (par de claves Pública/Privada) se crea al agregar un Mensaje revisado por repetición multiplicado a la clave maestra original. Por ejemplo, (que muestra solamente la clave privada del primer nodo 3 por claridad):

$$V_{2C} = V_{1C} + \text{SHA-256}(M) \quad (\text{Ecuación 24})$$

$$V_{2C'} = V_{1C} + \text{SHA-256}(\text{SHA-256}(M)) \quad (\text{Ecuación 25})$$

$$V_{2C''} = V_{1C} + \text{SHA-256}(\text{SHA-256}(\text{SHA-256}(M))) \quad (\text{Ecuación 26})$$

y así sucesivamente.

Para crear una ramificación, cualquier clave se puede utilizar como una clave secundaria. Por ejemplo, V_{2C} se puede utilizar como una subclave maestra (V_{3C}) al agregar el hash

(función de resumen) a ella como se hace para la clave maestra normal:

$$V_{3C} = V_{2C}' + \text{SHA-256}(M) \quad (\text{Ecuación 27})$$

5 La subclave maestra (V_{3C}) puede tener una clave de siguiente generación (V_{3C}'), por ejemplo:

$$V_{3C}' = V_{2C}' + \text{SHA-256}(\text{SHA-256}(M)) \quad (\text{Ecuación 28})$$

10 Esto proporciona una estructura de árbol 903 utilizando el método de generación de claves maestras tal como se muestra en la Figura 10.

(ii) Asociación Lógica

15 En este método todos los nodos en el árbol (pares de claves pública/privada) se generan como una cadena (o de cualquier otra manera) y las relaciones lógicas entre los nodos en el árbol se mantienen mediante una tabla en la cual cada nodo en el árbol simplemente se asocia a su nodo padre en el árbol utilizando un puntero. De esta manera, el puntero se puede utilizar para determinar los pares de claves pública/privada relevantes para determinar la clave secreta común (CS) para la sesión.

20

(iii) Mensaje de Multiplicidad

Se pueden generar nuevos pares de claves privada/pública mediante la introducción de un mensaje nuevo en cualquier punto de la cadena o árbol. El mensaje en sí puede ser arbitrario o puede portar algún significado o función (por ejemplo, podría estar relacionado con un número de cuenta bancaria "real", etc.). Puede ser deseable que tales mensajes nuevos para formar los nuevos pares de claves privada/pública sean retenidos de forma segura.

25

Dispositivo de procesamiento

30 Tal como se indicó anteriormente, el primero y el segundo nodos 3, 7 pueden ser un dispositivo electrónico, tal como una computadora, una tableta, un dispositivo de comunicación móvil, un servidor de computadora, etc. El dispositivo electrónico puede incluir un dispositivo de procesamiento 23, 27, un almacén de datos 13, 17 y una interfaz de usuario 15.

La Figura 11 ilustra un ejemplo de un dispositivo de procesamiento 23, 27. El dispositivo de procesamiento 23, 27 se puede utilizar en el primer nodo 3, el segundo nodo 7 u otros nodos 9. El dispositivo de procesamiento 23, 27 incluye un procesador 1510, una memoria 1520 y

35

un dispositivo de interfaz 1540 que se comunican entre sí a través de un bus 1530. La memoria 1520 almacena instrucciones y datos para implementar el método 100, 200, 300, 400 descrito anteriormente, y el procesador 1510 lleva a cabo las instrucciones procedentes de la memoria 1520 para implementar el método 100, 200, 300, 400. El dispositivo de interfaz 1540 puede incluir un

5 módulo de comunicaciones que facilita la comunicación con la red de comunicaciones 5 y, en algunos ejemplos, con la interfaz de usuario 15 y periféricos tales como el almacén de datos 13, 17, 19. Se debe observar que aunque el dispositivo de procesamiento 1501 puede ser independiente de elementos de red, el dispositivo de procesamiento 501 también puede ser parte de otro elemento de red. Además, algunas funciones llevadas a cabo por el dispositivo de procesamiento 1501 se pueden

10 distribuir entre múltiples elementos de red. Por ejemplo, el primer nodo 3 puede tener múltiples dispositivos de procesamiento 23 para llevar a cabo el método 100, 300 en una red de área local segura asociada al primer nodo 3.

Cuando esta divulgación describe que un usuario, un emisor, un comerciante, un proveedor u otra entidad lleva a cabo una acción en particular (que incluye firma, emisión,

15 determinación, cálculo, envío, recepción, creación, etc.), esta redacción se utiliza para mayor claridad de presentación. Se debe entender que estas acciones son llevadas a cabo por los dispositivos informáticos operados por estas entidades.

La firma puede comprender la ejecución de una función criptográfica. La función criptográfica tiene una entrada para un texto claro y una entrada para una clave, tal como una clave

20 privada. Un procesador puede ejecutar la función para calcular un número o cadena que se puede utilizar como una firma. La firma a continuación se proporciona junto con el texto claro para proporcionar un texto firmado. La firma cambia completamente si el texto del mensaje o la clave cambia en un solo bit. Si bien el cálculo de la firma requiere poco poder computacional, la recreación de un mensaje que tiene una firma determinada es prácticamente imposible. De esta

25 forma, el texto claro solo se puede modificar y estar acompañada por una firma válida si la clave privada está disponible. Además, otras entidades pueden verificar fácilmente la firma utilizando la clave pública disponible públicamente.

En la mayoría de las circunstancias, la encriptación y la desencriptación comprende un procesador que ejecuta una función criptográfica para calcular una cadena de salida que

30 representa el mensaje encriptado o un mensaje de texto claro, respectivamente.

Claves, tokens (componentes léxicos), metadatos, transacciones, ofertas, contratos, firmas, scripts, metadatos, invitaciones y similares se refieren a datos representados como números, texto o cadenas almacenados en la memoria de datos, tales como variables en código de programa de tipo "cadena" o "Int" u otros tipos o archivos de texto.

35 Un ejemplo del ledger (libro mayor) de red entre pares (peer-to-peer) es la

Blockchain (cadena de bloques) de bitcoin. La transferencia de fondos o el pago de tarifas en la moneda de bitcoins comprende la creación de una transacción en la Blockchain (cadena de bloques) de bitcoin con los fondos u las tarifas generados a partir de la transacción. Un ejemplo de una transacción de bitcoin incluye un hash (función de resumen) de transacción de entrada, un importe de transacción, uno o más destinos, una clave pública de un beneficiario o beneficiarios y una firma creada al utilizar la transacción de entrada como el mensaje de entrada y una clave privada de un pagador para calcular la firma. La transacción se puede verificar al comprobar que el hash (función de resumen) de transacción de entrada existe en una copia de la Blockchain (cadena de bloques) de bitcoin y que la firma es correcta utilizando la clave pública. Para garantizar que el mismo hash (función de resumen) de transacción de entrada no se ha utilizado en otro lugar todavía, la transacción se transmite a una red de nodos informáticos ('mineros'). Un minero acepta y registra la transacción en la Blockchain (cadena de bloques) solo si el hash (función de resumen) de transacción de entrada todavía no está conectado y las firmas son válidas. Un minero rechaza la transacción si el hash (función de resumen) de transacción de entrada ya está vinculado a una transacción diferente.

La asignación de criptomonedas para un token (componente léxico) comprende crear una transacción con las criptomonedas asignadas y el token (componente léxico) representado en un campo de metadatos en la transacción.

Cuando dos elementos están asociados, esto significa que hay una conexión lógica entre estos elementos. En una base de datos, por ejemplo, los identificadores para los dos elementos se pueden almacenar en los mismos registros para hacer que los dos elementos se asocien entre sí. En una transacción, los identificadores para los dos elementos se pueden incluir en la cadena de transacción para hacer que los dos elementos se asocien entre sí.

El uso del protocolo de bitcoin, el canjeo de un script (archivo de órdenes) y/o el desbloqueo de un token (componente léxico) comprende calcular una cadena de firma del script (archivo de órdenes) y/o transacción utilizando la clave privada. El script (archivo de órdenes) puede requerir más de una firma derivada de claves privadas diferentes u otras condiciones. El resultado de esta transacción a continuación se proporciona a un minero.

La autorización de otra entidad puede comprender calcular una cadena de firma de una transacción utilizando una clave privada y proporcionar la cadena de firma a la entidad para permitir que la entidad utilice la firma para verificar la transacción.

Un usuario que tiene una cuenta con otra entidad puede comprender la entidad que almacena información sobre el usuario, tal como la dirección de correo electrónico, el nombre y las claves potencialmente públicas. Por ejemplo, la entidad puede mantener una base de datos, tal como SQL, OrientDB, MongoDB u otras. En algunos ejemplos, la entidad también puede almacenar

una o más de las claves privadas del usuario.

- El experto apreciará que la presente invención proporciona numerosos beneficios y ventajas técnicas sobre la técnica anterior. Por ejemplo, el protocolo BIP32 (por ejemplo, tal como se describe en la guía de desarrolladores de Bitcoin) utiliza una semilla aleatoria para generar las subclaves. Esto da lugar a la necesidad de mantener una base de datos de índices. De acuerdo con la presente invención, sin embargo, se utiliza un mensaje significativo M para generar las subclaves (y por lo tanto también los secretos subcompartidos). De forma ventajosa, esto evita la necesidad de una base de datos de índices, y de esta manera proporciona una técnica de seguridad más simple que es más eficiente en términos de los recursos informáticos necesarios para ejecutarla.
- Adicionalmente, permite la asociación de información significativa con las subclaves. Por ejemplo, las subclaves reutilizables se pueden utilizar para representar cuentas bancarias o códigos de clientes específicos, etc. Alternativamente, las subclaves únicas se pueden generar con base en el hash (función de resumen) de una factura o archivo de película en específico (u otros datos), etc.

- Los expertos en la técnica apreciarán que se pueden realizar numerosas variaciones y/o modificaciones en las modalidades descritas anteriormente, sin apartarse del amplio alcance general de la presente divulgación tal como se define en las reivindicaciones adjuntas. Por lo tanto, las presentes modalidades se deben considerar, en todos los aspectos, como ilustrativas y no como restrictivas.