(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 819 862**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/60 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.02.2017 PCT/EP2017/053466**

(87) Fecha y número de publicación internacional: **24.08.2017 WO17140759**

(96) Fecha de presentación y número de la solicitud europea: **16.02.2017 E 17705856 (7)**

(97) Fecha y número de publicación de la concesión europea: **15.07.2020 EP 3398319**

(54) Título: **Métodos y sistemas para cifrar comunicaciones utilizando un elemento seguro**

(30) Prioridad:

17.02.2016 US 201662296188 P
10.05.2016 US 201615151224

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.04.2021

(73) Titular/es:

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

(72) Inventor/es:

BENOIT, BERNARD;
FOURNIER, JEAN-CLAUDE;
PERRINE, JÉRÔME y
GAUTERON, LAURENT

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Métodos y sistemas para cifrar comunicaciones utilizando un elemento seguro

Referencia cruzada a solicitudes relacionadas

Esta solicitud reivindica la prioridad de la Solicitud de Patente de EE. UU. No. 15/151.224, presentada el 10 de mayo de 2016 y titulada “Methods and Systems for Encrypting Communications Using a Secure Element” y la Solicitud de Patente Provisional de EE. UU. No. 62/296.188, presentada el 17 de febrero de 2016 y titulada “Methods and Systems for Encrypting Communications Using a Secure Element”.

Antecedentes

Las personas se comunican de forma inalámbrica y sobre la marcha. Entre los dispositivos que lo hacen posible se encuentran los que a veces se denominan dispositivos móviles personales. Ejemplos de dispositivos móviles personales incluyen teléfonos celulares, teléfonos inteligentes, intercomunicadores portátiles y puntos de acceso portátiles, entre otros. Un dispositivo móvil personal podría ser de mano (como puede ser el caso de un intercomunicador portátil), montado en la carrocería o conectado a un vehículo (como el techo de un automóvil), por ejemplo.

Dada la facilidad relativa con la que las señales de radio pueden ser interceptadas, la comunicación con (o entre) los dispositivos móviles personales a menudo se cifran para evitar la interceptación de la comunicación por parte de terceros (ver, por ejemplo, US 2003/0031320 A1). En términos generales, el cifrado es el proceso de convertir la voz audible u otros datos en datos ininteligibles, mientras que el descifrado es el proceso de convertir los datos ininteligibles de nuevo al original (por ejemplo, voz audible). Los respectivos algoritmos utilizados para el cifrado y el descifrado a menudo se denominan en conjunto cifrado. Ejemplos de cifrados comunes incluyen Advanced Encryption Standard (AES), Blowfish, Data Encryption Standard (DES), Triple DES y RC4, entre muchos otros.

Descripción general de realizaciones descritas

Se describen en el presente documento métodos y sistemas para disposición de comunicación de sesiones en nombre de los puntos finales criptográficas.

Al menos una forma de realización toma la forma de un método que incluye las etapas de (i) realización de un procedimiento de intercambio de claves con un punto terminal a través del dispositivo de comunicación por voz para obtener una clave de semilla simétrica para una sesión de voz segura con el punto terminal; (ii) generar claves de sesión simétricas primera y segunda para la sesión de voz segura en base a la clave semilla simétrica obtenida; (iii) recibir paquetes de voz de salida desde el dispositivo de comunicación por voz en relación con la sesión de voz segura, donde cada paquete de voz de salida incluye una cabecera de paquete de voz de salida y una carga útil de paquete de voz de salida sin cifrar; (iv) utilizar un primer algoritmo de cifrado simétrico para generar las respectivas cargas útiles de paquetes de voz de salida cifrados una vez en función de la primera clave de sesión simétrica, todos o parte de las respectivas cabeceras del paquete de voz de salida y las respectivas cargas útiles de paquetes de voz de salida no cifrados; (v) utilizar un segundo algoritmo de cifrado simétrico para generar respectivas cargas útiles de paquetes de voz de salida cifrados dos veces en base a la segunda clave de sesión simétrica y las respectivas cargas útiles de paquetes de voz de salida cifradas una vez; y (vi) enviar las respectivas cargas útiles de paquetes de voz de salida cifrados dos veces al dispositivo de comunicación por voz para ensamblar con las respectivas cabeceras de paquetes de voz de salida para su transmisión al punto terminal en relación con la sesión de voz segura.

Además, se debe apreciar expresamente que, mientras que dos etapas de cifrado se describen en los ejemplos de esta descripción, cualquier número de etapas de cifrado (por ejemplo, tres, cinco, diez, etc.) podría ser utilizado en otras diversas realizaciones, según lo consideren adecuado los expertos en la técnica para una implementación determinada. En algunos casos, se pueden combinar dos o tres capas de cifrado privado (es decir, cifrado que utiliza un algoritmo de cifrado no publicado) con dos o tres capas de cifrado público (es decir, cifrado que utiliza un algoritmo de cifrado publicado). Y, ciertamente, también se podrían enumerar aquí muchas otras posibilidades. Además, el lenguaje utilizado en este documento con respecto a las claves “primera” y “segunda” para los algoritmos de cifrado “primero” y “segundo” contempla implementaciones que utilizan solo esas etapas de cifrado “primera” y “segunda”, y también contempla una o más etapas de cifrado. siendo implementado después de la denominada “primera” etapa de cifrado y antes de la denominada “segunda” (es decir, última) etapa de cifrado.

En algunas realizaciones, el elemento seguro es un componente en una placa de circuito impreso (PCB) del dispositivo de comunicación por voz. En algunas realizaciones, el elemento seguro que está acoplado comunicativamente con el dispositivo de comunicación por voz incluye el elemento seguro que está acoplado comunicativamente con el dispositivo de comunicación por voz a través de una conexión de interfaz periférica en serie (SPI).

En algunas realizaciones, el elemento seguro está acoplado en comunicación con el dispositivo de comunicación por voz incluye el elemento seguro está acoplado en comunicación con el dispositivo de comunicación por voz a través de una interfaz micro SD.

En algunas realizaciones, el elemento seguro está acoplado en comunicación con el dispositivo de comunicación por voz incluye el elemento seguro que está acoplado en comunicación con el dispositivo de comunicación por voz a través de una interfaz de módulo de identidad segura (SIM).

En algunas realizaciones, el dispositivo de comunicación por voz incluye un teléfono inteligente.

En algunas realizaciones, el dispositivo de comunicación por voz incluye unos auriculares.

En algunas realizaciones, el procedimiento de intercambio de claves incluye un procedimiento de intercambio de claves de Diffie-Hellman. En algunas realizaciones, el procedimiento de intercambio de claves Diffie-Hellman incluye un procedimiento de intercambio de claves Diffie-Hellman de curva elíptica.

En algunas realizaciones, el método además incluye realizar un procedimiento de autenticación mutua de usuario final con el punto terminal a través del dispositivo de comunicación por voz para la sesión de voz segura. En algunas realizaciones, el procedimiento de autenticación mutua de usuario final incluye un procedimiento de autenticación mutua de usuario final Diffie-Hellman. En algunas realizaciones, el procedimiento de autenticación mutua de usuario final Diffie-Hellman incluye un procedimiento de autenticación mutua de usuario final Diffie-Hellman de curva elíptica.

En algunas realizaciones, el punto terminal es un segundo elemento seguro que está acoplado en comunicación con un segundo dispositivo de comunicación por voz.

En algunas realizaciones, el elemento seguro utiliza un algoritmo de diversificación simétrica para generar la primera y segunda claves de sesión simétrica para la sesión de voz segura basada en la clave simétrica semilla obtenida. En algunas realizaciones, el algoritmo de diversificación simétrica incluye un algoritmo de diversificación simétrica AES.

En algunas realizaciones, el elemento seguro da salida a cada corriente de carga útil de paquete de voz de salida cifrado dos veces de cada paquete de voz de salida de corriente antes de recibir un próximo paquete de voz de salida respectivo.

En algunas realizaciones, el elemento seguro está configurado para separar y procesar múltiples paquetes de voz de salida en un momento dado.

Un parámetro de diversificación al algoritmo simétrico se obtiene de la totalidad o parte de las respectivas cabeceras de paquetes de voz. Se sabe que cada cabecera es única y comprende varios parámetros como los datos que permiten identificar el paquete (el número de secuencia o valor del índice), la versión, la fuente, la marca de tiempo, CRC, etc. El parámetro de diversificación puede ser uno de esos o una combinación del parámetro de la cabecera, así como el resultado de una operación matemática (por ejemplo, XOR) o criptográfica (por ejemplo, Hash) en los parámetros de la cabecera.

En algunas realizaciones, cada cabecera de paquete de voz de salida incluye un valor de índice respectivo, y la generación de las respectivas cargas útiles de paquetes de voz de salida cifrados una vez en base a las respectivas cabeceras de paquetes de voz de salida utilizando el primer algoritmo de cifrado simétrico incluye el uso del primer algoritmo de cifrado simétrico para generar las respectivas cargas útiles de paquetes de voz de salida cifrados una vez basándose en los valores de índice respectivos en las cabeceras de paquetes de voz de salida respectivos como parámetro de diversificación. El valor del índice podría ser el Número de secuencia (ver, por ejemplo, la cabecera del paquete RTP) incrementado en uno por cada paquete de datos enviado.

En algunas realizaciones, cada cabecera de paquete de voz de salida incluye, además, un respectivo valor de fuente de sincronización (SSRC), y la generación de las respectivas cargas útiles de paquetes de voz de salida cifrados una vez en base a las respectivas cabeceras de paquete de voz de salida utilizando el primer algoritmo de cifrado simétrico incluye además el uso del primer algoritmo de cifrado simétrico para generar las respectivas cargas útiles de paquetes de voz de salida cifrados una vez en base a los valores SSRC respectivos en las cabeceras de paquetes de voz de salida respectivos como parámetros de diversificación. Cabe señalar que el valor SSRC se puede utilizar solo o junto con el valor del índice como un parámetro de diversificación adicional para el primer algoritmo de cifrado simétrico.

En algunas realizaciones, el primer algoritmo de cifrado simétrico genera etiquetas de autenticación de paquetes de voz de salida respectivos en base a la primera clave simétrica de sesión, las respectivas cabeceras de paquetes de voz de salida, y las respectivas cargas útiles de paquetes de voz de salida no cifrados, y emite las correspondientes etiquetas de autenticación de paquetes de voz de salida al dispositivo de comunicación por voz para ensamblar con las respectivas cabeceras de paquetes de voz de salida y las respectivas cargas útiles de paquetes de voz de salida cifrados dos veces para su transmisión al punto terminal en relación con la sesión de voz segura.

En algunas realizaciones, cada cabecera de paquete de voz de salida incluye un valor de índice respectivo, y la generación de las etiquetas de autenticación de paquetes de voz de salida respectivos sobre la base de las respectivas cabeceras de los paquetes de voz de salida utilizando el primer algoritmo de cifrado simétrico incluye el uso del primer algoritmo de cifrado simétrico para generar las respectivas etiquetas de autenticación de paquetes de voz de salida basándose en los valores de índice respectivos en las respectivas cabeceras de paquetes de voz de salida.

En algunas realizaciones, cada cabecera de paquete de voz de salida incluye, además, un valor SSRC respectivo, y la generación de las etiquetas de autenticación de paquetes de voz de salida respectivos sobre la base de las respectivas cabeceras de los paquetes de voz de salida utilizando el primer algoritmo de cifrado simétrico incluye además el uso del primer algoritmo de cifrado simétrico para generar las respectivas etiquetas de autenticación de paquetes de voz de salida en base a los valores SSRC respectivos en las respectivas cabeceras de paquetes de voz de salida.

En algunas realizaciones, el método incluye además las etapas de (i) recibir paquetes de voz de entrada desde el dispositivo de comunicación por voz en relación con la sesión segura de voz, donde cada paquete de voz de entrada incluye una cabecera de paquetes de voz de entrada y una carga útil de paquetes de voz de entrada cifrados dos veces; (ii) utilizar el segundo algoritmo de cifrado simétrico para generar respectivas cargas útiles de paquetes de voz de entrada cifradas una vez en base a la segunda clave de sesión simétrica y las respectivas cargas útiles de paquetes de voz de entrada cifrada dos veces; (iii) utilizar el primer algoritmo de cifrado simétrico para generar las respectivas cargas útiles de paquetes de voz de entrada descifrados en función de la primera clave de sesión simétrica, todas o parte de las respectivas cabeceras de paquetes de voz de entrada (el parámetro de diversificación), y las respectivas cargas útiles cabeceras de paquetes de voz de entrada cifradas una vez; y (iv) enviar las respectivas cargas útiles del paquete de voz de entrada descifrado al dispositivo de comunicación por voz para (a) ensamblar con las respectivas cabeceras del paquete de voz de entrada y (b) la reproducción resultante de las cargas útiles del paquete de voz de entrada descifrado a través de una interfaz de usuario del dispositivo de comunicación por voz en relación con la sesión de voz segura.

En algunas realizaciones, el elemento seguro genera cada carga útil de paquetes de voz de entrada descifrados corriente en cada paquete de voz de entrada corriente antes de recibir un próximo paquete de voz de entrada respectiva. En algunas realizaciones, el elemento seguro está configurado para almacenar y procesar múltiples paquetes de voz de entrada en un momento dado. En algunas realizaciones, cada cabecera de paquete de voz de entrada incluye un valor de índice respectivo, y generar las respectivas cargas útiles de paquete de voz de entrada descifrado en base a todo o parte de las respectivas cabeceras de paquete de voz de entrada usando el primer algoritmo de cifrado simétrico incluye utilizar el primer algoritmo de cifrado simétrico para generar las respectivas cargas útiles de paquetes de voz de entrada descifrados en base a los valores de índice respectivos en las respectivas cabeceras de paquetes de voz de entradas.

En algunas realizaciones, cada cabecera de paquete de voz de entrada incluye, además, un valor SSRC respectivo, y la generación de las respectivas cargas útiles de paquete de voz de entrada descifrados en base a las respectivas cabeceras de paquete de voz de entrada utilizando el primer algoritmo de cifrado simétrico incluye además utilizar el primer algoritmo de cifrado simétrico para generar las respectivas cargas útiles de paquetes de voz de entrada descifrados en base a los valores SSRC respectivos en las respectivas cabeceras de paquetes de voz de entradas.

En algunas realizaciones, cada paquete de voz de entrada incluye además una etiqueta de autenticación de paquetes de voz de entrada, y el método incluye adicionalmente utilizar el primer algoritmo de cifrado simétrico para autenticar los respectivos paquetes de voz de entrada en base a la primera clave de sesión simétrica.

En algunas realizaciones, cada paquete de voz de entrada incluye además una etiqueta de autenticación de paquetes de voz de entrada, y el método incluye, además, utilizar el primer algoritmo de cifrado simétrico para verificar la integridad de los respectivos paquetes de voz de entrada en base a la primera clave de sesión simétrica.

En algunas realizaciones, el primer algoritmo de cifrado simétrico es un algoritmo de cifrado simétrico publicado y el segundo algoritmo de cifrado simétrico es un algoritmo de cifrado simétrico no publicado. En algunas de tales realizaciones, el primer algoritmo de cifrado simétrico es un algoritmo seleccionado del grupo que consta de un algoritmo AES, un algoritmo Blowfish, un algoritmo DES, un algoritmo Triple DES, un algoritmo Serpent y un algoritmo Twofish.

En algunas realizaciones, el primer y segundo algoritmos de cifrado simétrico son dos algoritmos de cifrado simétrico publicados diferentes.

En algunas realizaciones, el primer y segundo algoritmos de cifrado simétrico son dos algoritmos de cifrado simétrico no publicados diferentes.

Otra forma de realización toma la forma de un elemento seguro que incluye (i) una interfaz de comunicación configurada para ser acoplada comunicativamente con un dispositivo de comunicación por voz; (ii) un módulo de negociación de sesiones; (iii) un módulo de generación de claves de sesión; (iv) un primer módulo de cifrado simétrico

que implementa un primer algoritmo de cifrado simétrico; y (v) un segundo módulo de cifrado simétrico que implementa un segundo algoritmo de cifrado simétrico.

En al menos una realización, el módulo de sesión de negociación está configurado para (i) realizar un procedimiento de intercambio de claves con un punto terminal a través de la interfaz de comunicación y el dispositivo de comunicación por voz para obtener una clave de semilla simétrica para una sesión de voz segura con el punto terminal y (ii) pasar la clave semilla simétrica obtenida al módulo de generación de claves de sesión.

En al menos una realización, el módulo de generación de clave de sesión está configurado para (i) recibir la clave simétrica semilla obtenida a partir del módulo de sesión-negociación; (ii) generar claves de sesión simétricas primera y segunda para la sesión de voz segura en base a la clave semilla simétrica obtenida; (iii) pasar la primera clave de sesión simétrica al primer módulo de cifrado simétrico; y (iv) pasar la segunda clave de sesión simétrica al segundo módulo de cifrado simétrico.

En al menos una realización, el primer módulo de cifrado simétrico está configurado para (i) recibir la primera clave de sesión simétrica desde el módulo de generación de clave de sesión; (ii) recibir paquetes de voz de salida desde el dispositivo de comunicación por voz a través de la interfaz de comunicación como parte de la sesión de voz segura, cada paquete de voz de salida comprende una cabecera de paquete de voz de salida y una carga útil de paquete de voz de salida no cifrada; (iii) utilizar el primer algoritmo de cifrado simétrico para generar cargas útiles de paquetes de voz de salida cifradas una vez en función de la primera clave de sesión simétrica, todos o parte de las cabeceras del paquete de voz de salida y las cargas útiles de paquetes de voz de salida no cifrados; y (iv) pasar las cargas útiles del paquete de voz de salida cifradas una vez al segundo módulo de cifrado simétrico.

En al menos una realización, el segundo módulo de cifrado simétrico está configurado para (i) recibir la segunda clave de sesión simétrica desde el módulo de generación de clave de sesión; (ii) recibir las cargas útiles de paquetes de voz de salida cifrados una vez desde el primer módulo de cifrado simétrico; (iii) utilizar el segundo algoritmo de cifrado simétrico para generar cargas útiles de paquetes de voz de salida cifrados dos veces basándose en la segunda clave de sesión simétrica y las cargas útiles de paquetes de voz de salida cifrados una vez; y (iv) generar las cargas útiles de paquetes de voz de salida cifrados dos veces.

En al menos una realización, el dispositivo de comunicación por voz incluye, además, un módulo de montaje de paquete saliente de voz de salida configurado para (i) recibir las cabeceras de paquetes de voz de salida desde el primer módulo de cifrado simétrico; (ii) recibir las cargas útiles de paquetes de voz de salida cifrados dos veces desde el segundo módulo de cifrado simétrico; (iii) ensamblar paquetes de voz de salida cifrados dos veces a partir de las cabeceras del paquete de voz de salida y las cargas útiles del paquete de voz de salida cifrados dos veces; y (iv) enviar las cargas útiles ensambladas de paquetes de voz de salida cifrados dos veces al dispositivo de comunicación por voz para su transmisión al punto terminal en relación con la sesión de voz segura.

En al menos una realización, el segundo módulo de cifrado simétrico está configurado para dar salida a las cargas útiles de paquete de voz de salida cifrados dos veces incluye el segundo módulo de cifrado simétrico que está configurado para dar salida a las cargas útiles de paquetes de voz de salida cifrada dos veces al dispositivo de voz de comunicación para ensamblar con las respectivas cabeceras de paquetes de voz de salida para su transmisión al punto terminal en relación con la sesión de voz segura.

En al menos una realización, el procedimiento de intercambio de claves incluye un procedimiento de intercambio de claves de Diffie-Hellman. En al menos una de tales realizaciones, el procedimiento de intercambio de claves Diffie-Hellman incluye un procedimiento de intercambio de claves Diffie-Hellman de curva elíptica.

En al menos una realización, el módulo de sesión de negociación está configurado además para llevar a cabo un procedimiento de autenticación mutua de usuario final con el punto terminal a través de la interfaz de comunicación y el dispositivo de comunicación por voz para la sesión de voz segura. En al menos una de tales realizaciones, el procedimiento de autenticación mutua de usuario final incluye un procedimiento de autenticación mutua de usuario final Diffie-Hellman; en al menos una de tales realizaciones, el procedimiento de autenticación mutua de usuario final Diffie-Hellman incluye un procedimiento de autenticación mutua de usuario final Diffie-Hellman de curva elíptica.

En al menos una realización, el punto terminal es un segundo elemento seguro que está acoplado en comunicación con un segundo dispositivo de comunicación por voz.

En al menos una realización, el módulo de generación de clave de sesión está configurado para generar la primera y segunda claves de sesión simétrica para la sesión de voz segura basada en la clave simétrica semilla obtenida incluye el módulo de generación de clave de sesión que está configurado para utilizar un algoritmo de diversificación simétrica para generar la primera y segunda claves de sesión simétricas para la sesión de voz segura en base a la clave semilla simétrica obtenida. En al menos una de tales realizaciones, el algoritmo de diversificación simétrica incluye un algoritmo de diversificación simétrica AES.

En al menos una realización, el elemento seguro emite una carga útil de paquete de voz de salida corriente cifrado dos veces de un paquete de voz de salida de corriente antes de recibir un próximo paquete de voz de salida respectivo.

En al menos una realización, el elemento seguro está configurado para amortiguar y procesar varios paquetes de voz de salida en un momento dado.

En al menos una realización, cada cabecera de paquete de salida de voz incluye un valor de índice respectivo; y el primer módulo de cifrado simétrico se configura para utilizar el primer algoritmo de cifrado simétrico para generar las cargas útiles de paquetes de voz de salida cifrados una vez en función de las cabeceras del paquete de voz de salida incluye el primer módulo de cifrado simétrico que se configura para utilizar el primer algoritmo de cifrado simétrico para generar las cargas útiles de paquetes de voz de salida una vez cifrados en base a los valores de índice respectivos en las cabeceras de paquetes de voz de salida respectivos.

En al menos una de tales realizaciones, cada cabecera de paquete de voz de salida incluye, además, un valor SSRC respectivo; y el primer módulo de cifrado simétrico que se configura para utilizar el primer algoritmo de cifrado simétrico para generar las cargas útiles de paquetes de voz de salida cifrados una vez en función de las cabeceras del paquete de voz de salida incluye además el primer módulo de cifrado simétrico que se configura para utilizar el primer algoritmo de cifrado simétrico para generar las cargas útiles del paquete de voz de salida cifradas una vez en función de los valores SSRC respectivos en las cabeceras del paquete de voz de salida respectivas.

En al menos una realización, el primer módulo de cifrado simétrico está configurado además para (i) utilizar el primer algoritmo de cifrado simétrico para generar respectivas etiquetas de autenticación en paquetes de voz de salida en base a la primera clave de sesión simétrica, la totalidad o parte de las respectivas cabeceras de paquetes de voz de salida, y las respectivas cargas útiles de paquetes de voz de salida no cifrados y (ii) emitir las etiquetas de autenticación de paquetes de voz de salida respectivos para ensamblar con las respectivas cabeceras del paquete de voz de salida y las respectivas cargas útiles de paquetes de voz de salida cifrados dos veces para su transmisión al punto terminal en relación con la sesión de voz segura.

Por lo menos en tal una realización, cada cabecera de paquete de voz de salida incluye un valor de índice respectivo; y el primer módulo de cifrado simétrico se configura para utilizar el primer algoritmo de cifrado simétrico para generar las respectivas etiquetas de autenticación de paquetes de voz de salida basadas en las respectivas cabeceras de paquetes de voz de salida incluye el primer módulo de cifrado simétrico que está configurado para utilizar el primer algoritmo de cifrado simétrico para generar las respectivas etiquetas de autenticación de paquetes de voz de salida basándose en los valores de índice respectivos en las respectivas cabeceras del paquete de voz de salida.

Por lo menos en tal una realización, cada cabecera de paquete de voz de salida incluye, además, un valor SSRC respectivo; y el primer módulo de cifrado simétrico configurado para utilizar el primer algoritmo de cifrado simétrico para generar las respectivas etiquetas de autenticación de paquetes de voz de salida basadas en las respectivas cabeceras de paquetes de voz de salida incluye además el primer módulo de cifrado simétrico configurado para utilizar el primer algoritmo de cifrado simétrico para generar las respectivas etiquetas de autenticación de paquetes de voz de salida basadas en los valores SSRC respectivos en las respectivas cabeceras de paquetes de voz de salida.

En al menos una realización, el elemento seguro incluye un componente en una PCB del dispositivo de comunicación por voz.

En al menos una realización, el elemento seguro está configurado para ser acoplado de manera comunicativa con el dispositivo de comunicación por voz incluye el elemento seguro que está configurado para ser acoplado de manera comunicativa con el dispositivo de comunicación por voz por medio de una conexión SPI.

En al menos una realización, el elemento seguro está configurado para ser acoplado de manera comunicativa con el dispositivo de comunicación por voz incluye el elemento seguro que está configurado para ser acoplado de manera comunicativa con el dispositivo de comunicación por voz por medio de una interfaz micro SD.

En al menos una realización, el elemento seguro está configurado para ser acoplado de manera comunicativa con el dispositivo de comunicación por voz incluye el elemento seguro que está configurado para ser acoplado de manera comunicativa con el dispositivo de comunicación por voz por medio de una interfaz de SIM.

En al menos una realización, el dispositivo de comunicación por voz incluye un teléfono inteligente.

En al menos una realización, el dispositivo de comunicación por voz incluye unos auriculares.

En al menos una realización, el segundo módulo de cifrado simétrico está configurado además para (i) recibir paquetes de voz de entrada desde el punto terminal a través del dispositivo de comunicación por voz y la interfaz de comunicación, cada paquete de voz de entrada que comprende una cabecera de paquetes voz de entrada y una carga útil de paquete de voz de entrada cifrado dos veces; (ii) utilizar el segundo algoritmo de cifrado simétrico para generar cargas útiles de paquetes de voz de entrada cifrados una vez basándose en la segunda clave de sesión simétrica y

cargas útiles de paquetes de voz de entrada cifrados dos veces; y (iii) pasar la totalidad o parte de las cabeceras del paquete de voz de entrada y las cargas útiles del paquete de voz de entrada cifradas una vez al primer módulo de cifrado simétrico;

En al menos una realización, el primer módulo de cifrado simétrico está configurado además para (i) recibir las cabeceras del paquete de voz de entrada y las cargas útiles de paquetes de voz de entrada cifrados una vez desde el segundo módulo de cifrado simétrico; (ii) utilizar el primer algoritmo de cifrado simétrico para generar cargas útiles de paquetes de voz de entrada descifradas basadas en la primera clave de sesión simétrica, todas o parte de las cabeceras de paquetes de voz de entrada y las cargas útiles de paquetes de voz de entrada cifradas una vez; y (iii) enviar las cargas útiles del paquete de voz de entrada descifrado al dispositivo de comunicación por voz para ensamblar con las respectivas cabeceras del paquete de voz de entrada y la reproducción resultante de las cargas útiles del paquete de voz de entrada descifrado a través de una interfaz de usuario del dispositivo de comunicación por voz en relación con la sesión de voz segura.

En al menos una realización, el elemento seguro genera cada carga útil de paquetes de voz de entrada corriente descifrado de cada paquete de voz de entrada corriente antes de recibir un próximo paquete de voz de entrada respectiva.

En al menos una realización, el elemento seguro está configurado para separar y procesar múltiples paquetes de voz de entrada en un momento dado.

En al menos una realización, cada cabecera de paquete de voz de entrada incluye un valor de índice respectivo; y el primer módulo de cifrado simétrico que está configurado para utilizar el primer algoritmo de cifrado simétrico para generar las cargas útiles de paquetes de voz de entrada descifrados basados en las cabeceras de paquetes de voz de entrada incluye el primer módulo de cifrado simétrico que está configurado para utilizar el primer algoritmo de cifrado simétrico para generar las cargas útiles del paquete de voz de entrada descifrado en función de los valores de índice respectivos en las respectivas cabeceras del paquete de voz de entrada.

En al menos una realización, cada cabecera de paquete de voz de entrada incluye, además, un valor SSRC respectivo; y el primer módulo de cifrado simétrico que se configura para utilizar el primer algoritmo de cifrado simétrico para generar las cargas útiles de paquetes de voz de entrada descifrados basados en las cabeceras de paquetes de voz de entrada incluye además el primer módulo de cifrado simétrico que se configura para utilizar el primer algoritmo de cifrado simétrico para generar las cargas útiles del paquete de voz de entrada descifrado en base a los valores SSRC respectivos en las respectivas cabeceras del paquete de voz de entrada.

Un ejemplo para producir el paquete de voz cifrado una vez de una carga útil, una clave simétrica y un parámetro es utilizar el esquema de cifrado XTS-AES. El parámetro es el valor del índice o el valor SSRC. La clave simétrica se aplica primero a un cifrado de cifrado de bloque utilizando el parámetro como factor de diversificación i (ver Wikipedia “Teoría de cifrado de disco”). Otro ejemplo es utilizar el encadenamiento de bloques de cifrado en el que el parámetro desempeña el papel del vector de inicialización IV (consulte Wikipedia “Modo de funcionamiento de cifrado de bloques”).

En al menos una realización, cada paquete de voz de entrada incluye además una etiqueta de autenticación de paquetes de voz de entrada, y el primer módulo de cifrado simétrico está configurado además para autenticar los paquetes de voz de entrada en base a las respectivas etiquetas de autenticación de paquetes de voz de entrada.

En al menos una realización, cada paquete de voz de entrada incluye además una etiqueta autenticación de paquetes de voz de entrada, y el primer módulo de cifrado simétrico está configurado además para verificar la integridad de los respectivos paquetes de voz de entrada en base a las respectivas etiquetas de autenticación de paquetes de entrada.

En al menos una realización, el primer algoritmo de cifrado simétrico es un algoritmo de cifrado simétrico publicado; y el segundo algoritmo de cifrado simétrico no es un algoritmo de cifrado simétrico publicado. En al menos una de tales realizaciones, el primer algoritmo de cifrado simétrico es un algoritmo seleccionado del grupo que consta de un algoritmo AES, un algoritmo Blowfish, un algoritmo DES, un algoritmo Triple DES, un algoritmo Serpent y un algoritmo Twofish.

En al menos una realización, el primer y segundo algoritmos de cifrado simétrico son dos algoritmos de cifrado simétrico publicados diferentes.

En al menos una realización, el primer y segundo algoritmos de cifrado simétrico son dos algoritmos de cifrado simétrico no publicados diferentes.

Una forma de realización toma la forma de un elemento seguro que incluye (i) un módulo de sesión de generación de clave configurado para generar una primera clave de sesión y una segunda clave de sesión; (ii) un primer módulo de cifrado simétrico que implementa un primer algoritmo de cifrado simétrico usando la primera clave de sesión; (iii) un segundo módulo de cifrado simétrico que implementa un segundo algoritmo de cifrado simétrico usando la segunda

clave de sesión para generar un flujo de datos de doble cifrado, donde el segundo algoritmo de cifrado simétrico opera en una salida cifrada del primer módulo de cifrado simétrico; y (iv) una interfaz de comunicaciones configurada para transmitir el flujo de datos con doble cifrado a un dispositivo de comunicación por voz.

En al menos una realización, el elemento seguro también incluye un módulo de sesión de negociación que está configurado para (i) realizar un procedimiento de intercambio de claves con un punto terminal a través de la interfaz de comunicación y el dispositivo de comunicación por voz para obtener una clave de semillas simétrica para una sesión de voz segura con el punto terminal y (ii) pasar la clave semilla simétrica obtenida al módulo de generación de claves de sesión. En al menos una de tales realizaciones, el módulo de generación de claves de sesión está configurado para (i) recibir la clave semilla simétrica obtenida del módulo de negociación de sesiones; (ii) generar la primera y segunda claves de sesión simétricas para la sesión de voz segura en base a la clave semilla simétrica obtenida; (iii) pasar la primera clave de sesión simétrica al primer módulo de cifrado simétrico; y (iv) pasar la segunda clave de sesión simétrica al segundo módulo de cifrado simétrico.

En al menos una realización, el primer módulo de cifrado simétrico está configurado para (i) recibir la primera clave de sesión simétrica desde el módulo de generación de clave de sesión; (ii) recibir paquetes de voz de salida desde el dispositivo de comunicación por voz a través de la interfaz de comunicación como parte de la sesión de voz segura, donde cada paquete de voz de salida incluye una cabecera de paquete de voz de salida y una carga útil de paquete de voz de salida sin cifrar; (iii) utilizar el primer algoritmo de cifrado simétrico para generar cargas útiles de paquetes de voz de salida cifradas una vez en función de la primera clave de sesión simétrica, todos o parte de las cabeceras del paquete de voz de salida y las cargas útiles del paquete de voz de salida sin cifrar; y (iv) pasar las cargas útiles del paquete de voz de salida cifradas una vez al segundo módulo de cifrado simétrico.

En al menos una realización, el segundo módulo de cifrado simétrico está configurado para (i) recibir la segunda clave de sesión simétrica del módulo de generación de clave de sesión; (ii) recibir las cargas útiles de paquetes de voz de salida cifrados una vez desde el primer módulo de cifrado simétrico; (iii) utilizar el segundo algoritmo de cifrado simétrico para generar cargas útiles de paquetes de voz de salida cifrados dos veces basándose en la segunda clave de sesión simétrica y las cargas útiles de paquetes de voz de salida cifrados una vez; y (iv) generar las cargas útiles de paquetes de voz de salida cifrados dos veces.

La descripción general anterior se proporciona a modo de ejemplo y no de limitación, ya que los que tienen conocimientos ordinarios en la técnica relevante pueden implementar los sistemas y métodos divulgados utilizando uno o más componentes, estructuras, dispositivos y similares equivalentes, y pueden combinar y/o distribuir ciertas funciones de manera equivalente, aunque diferente.

Además, cualquiera de las variaciones y permutaciones descritas en esta divulgación se puede implementar con respecto a cualquier realización, incluso con respecto a cualquier realización de método y con respecto a cualquier realización de sistema. Además, esta flexibilidad y aplicabilidad cruzada de realizaciones está presente a pesar del uso de lenguaje ligeramente diferente (por ejemplo, proceso, método, etapas, funciones, conjunto de funciones y similares) para describir o caracterizar tales realizaciones.

Breve descripción de los dibujos

En el presente documento se describen varias realizaciones de ejemplo con referencia a los siguientes dibujos, en los que números iguales denotan entidades similares.

La Fig. 1 representa un sistema de comunicación, de acuerdo con algunas realizaciones.

La Fig. 2A-2C representan diagramas de bloques de un dispositivo de comunicación, de acuerdo con algunas realizaciones. En particular, la Fig. 2A representa un dispositivo de comunicación sin un elemento seguro, la Fig. 2B representa un dispositivo de comunicación con un elemento seguro extraíble, de acuerdo con algunas realizaciones, y la Fig. 2C representa un dispositivo de comunicación con un elemento seguro no removible, de acuerdo con algunas realizaciones.

La Fig. 3 representa un diagrama de flujo de un método, de acuerdo con algunas realizaciones.

La Fig. 4 representa un diagrama de flujo de llamadas de un proceso, de acuerdo con algunas realizaciones.

La Fig. 5A-5E representan diagramas de bloques de un elemento seguro, de acuerdo con algunas realizaciones.

Descripción detallada

Los presentes sistemas y métodos se describirán ahora con referencia a las figuras. Debe entenderse, sin embargo, que son posibles numerosas variaciones de las disposiciones y funciones descritas. Por ejemplo, se pueden agregar, eliminar, combinar, distribuir, sustituir, reubicar, reordenar y/o cambiar de otro modo uno o más elementos. Además, cuando esta descripción se refiere a una o más funciones que se implementan en y/o por uno o más dispositivos, una

o más máquinas, y/o una o más redes, debe entenderse que una o más de dichas entidades podrían llevar a cabo una o más de tales funciones por sí mismas o en cooperación, y pueden hacerlo mediante la aplicación de cualquier combinación adecuada de hardware, firmware y/o software. Por ejemplo, uno o más procesadores pueden ejecutar uno o más conjuntos de instrucciones de programación como al menos parte de la realización de una o más de las funciones descritas en este documento.

En la presente divulgación, varios elementos de una o más de las realizaciones descritas se denominan módulos que llevan a cabo (es decir, realizan, ejecutan y similares) diversas funciones descritas en el presente documento. Como el término "módulo" se usa en este documento, cada módulo descrito incluye hardware (por ejemplo, uno o más procesadores, microprocesadores, microcontroladores, microchips, circuitos integrados específicos de la aplicación (ASIC), matrices de puertas programables en campo (FPGA), dispositivos de memoria y/o uno o más de cualquier otro tipo o tipos de dispositivos y/o componentes considerados adecuados por los expertos en la técnica pertinente en un contexto dado y/o para una implementación dada. Cada módulo descrito también incluye cualquier instrucción necesaria ejecutable para llevar a cabo una o más funciones descritas como realizadas por el módulo en particular, donde esas instrucciones podrían tomar la forma o al menos incluir instrucciones de hardware (es decir, cableadas), instrucciones de firmware, instrucciones de software y/o similares, almacenadas en cualquier medio legible por ordenador no transitorio considerado adecuado por los expertos en la técnica relevante.

La Fig. 1 representa un sistema 100 de comunicación, de acuerdo con al menos una realización. Como se muestra, un sistema 100 de comunicación incluye un dispositivo 102 de comunicación local, una red 108 y un dispositivo 118 de comunicación remota.

El dispositivo 102 de comunicación podría tomar la forma de, por ejemplo, un ordenador personal, un ordenador de escritorio, un ordenador portátil tipo laptop, un ordenador portátil tipo notebook, un ordenador tipo tableta, un ordenador de mano, un ordenador de vestir, un asistente digital personal (PDA), un teléfono con funciones, una pantalla óptica montada en la cabeza (OHMD) y/o un reloj inteligente, entre muchas otras posibilidades que se conocerán a los expertos en la técnica. En la realización ilustrada en la Figura 1, el dispositivo 102 de comunicación adopta la forma de un teléfono inteligente.

El dispositivo 118 de comunicación remota puede ser cualquier dispositivo adecuado (o combinación de dispositivos) configurado para realizar las funciones de punto terminal remoto descritas en este documento. En algunas realizaciones, el dispositivo 118 de comunicación remota toma una forma similar al dispositivo 102 de comunicación. En algunas configuraciones, el dispositivo 118 de comunicación remota podría tomar la forma de un teléfono criptográfico, un conmutador telefónico privado (PBX), un PBX de protocolo de Internet (IP - PBX), y/o cualquier otra entidad capaz de llevar a cabo las funciones de punto terminal remoto descritas.

Como se muestra en la Fig. 1, el dispositivo 102 de comunicación local y el dispositivo 118 de comunicación remota se comunican a través de la red 108 usando enlaces 112 y 114 de comunicación, respectivamente. En algunas realizaciones, la red 108 es una red de área amplia (WAN) tal como una red celular, una red Wi-Fi o cualquier otra WAN conocida por los expertos en la técnica. Alternativamente, la red 108 puede ser una red de área personal (PAN), tal como Bluetooth o redes de comunicación de campo cercano (NFC), así como varias otras conocidas por los expertos en la técnica.

La Fig. 2A representa un diagrama de bloques de un dispositivo 102 de comunicación. Como se muestra, el dispositivo 102 de comunicación incluye un procesador 202 conectado a PCB 218, almacenamiento 204 de datos que incluye instrucciones 214 de programa, una interfaz 206 de comunicación y una interfaz 208 de usuario, cada uno de los cuales está interconectado a través de un bus 212 de sistema. En la realización ilustrada en la Fig. 1, el punto 106 terminal remoto adopta la forma de un teléfono de escritorio criptográfico. Aquellos que tengan experiencia en la técnica relevante apreciarán que el dispositivo 102 de comunicación podría tener componentes adicionales y/o diferentes, y quizás una disposición diferente de componentes, entre muchas otras variaciones posibles que podrían enumerarse en el presente documento.

El procesador 202 puede incluir uno o más procesadores de cualquier tipo que los expertos en la técnica consideren adecuados, algunos ejemplos incluyen un microprocesador, un circuito integrado de aplicación específica (ASIC) y un procesador de señales digitales (DSP).

El almacenamiento 204 de datos puede tomar la forma de cualquier medio legible por computadora no transitorio o una combinación de dichos medios, algunos ejemplos incluyen memoria flash, memoria de solo lectura (ROM) y memoria de acceso aleatorio (RAM), por nombrar solo algunos, ya que podría usarse uno o más tipos de tecnología de almacenamiento de datos no transitorios que los expertos en la técnica consideren adecuados.

Como se muestra en la Fig. 2A, el almacenamiento 204 de datos contiene instrucciones 214 de programa ejecutables por el procesador 202 para realizar diversas funciones, aunque el almacenamiento 204 de datos puede contener datos diferentes y/o adicionales. En una realización en la que el dispositivo 102 de comunicación local está configurado para llevar a cabo uno o más procesos y/o funciones (tales como los procesos y funciones descritos con referencia a la Figura 1), las instrucciones 214 de programa son ejecutables por el procesador 202 para llevar a cabo esas funciones.

En los casos en los que otras entidades descritas en el presente documento tienen una estructura similar a la del dispositivo 102 de comunicación local como se describe en relación con al menos la Fig. 1, las respectivas instrucciones 214 de programa almacenadas por los respectivos almacenamientos 204 de datos de esos respectivos dispositivos son ejecutables por sus respectivos procesadores 202 para llevar a cabo funciones realizadas por esos dispositivos.

La interfaz 206 de comunicación puede incluir cualquier hardware necesario (por ejemplo, conjuntos de chips, antenas, tarjetas Ethernet, etc.) y/o software para realizar una o más formas de comunicación con uno o más componentes y/o entidades (tales como dispositivo 102 de comunicación local y dispositivo 118 de comunicación remota, como ejemplos). La interfaz 206 de comunicación se puede configurar para comunicarse de acuerdo con uno o más protocolos como Bluetooth, NFC, Asociación de datos infrarrojos (Ir-DA), ZigBee, Wi-Fi, Bus serie universal (USB), IEEE 1394 (FireWire) y/o IEEE 802.3 (Ethernet)), como ejemplos.

La interfaz 208 de usuario puede incluir una o más pantallas, pantallas táctiles, altavoces, micrófonos, teclas de marcación, botones, interruptores, diodos emisores de luz (LED) y similares. Uno o más componentes de interfaz de usuario (por ejemplo, un componente de pantalla táctil y pantalla interactiva) podrían proporcionar funcionalidad tanto de entrada como de salida del usuario. Y podrían implementarse otros componentes de la interfaz de usuario en un contexto dado, como lo saben los expertos en la técnica.

La Fig. 2B representa un dispositivo 102 de comunicación, de acuerdo con algunas realizaciones. Como se muestra, el dispositivo 102 de comunicación en la Fig. 2B es similar al dispositivo 102 de comunicación mostrado en la Fig. 2A, con la adición del elemento 210 seguro. El elemento 210 seguro puede incluir hardware y/o software para realizar funciones o procesos criptográficos, por ejemplo, cifrado, descifrado, generación de firmas, verificación de firmas y/o generación de claves. En una realización, el elemento 210 seguro está contenido dentro de un perímetro definido explícitamente que establece los límites físicos del módulo criptográfico y que contiene procesadores y/u otros componentes de hardware que almacenan y protegen cualquier componente de software y firmware del módulo criptográfico. En algunas realizaciones, el elemento 210 seguro podría tomar la forma de (o incluir) un criptoprocesador seguro, una tarjeta inteligente, una tarjeta digital segura (SD), una tarjeta micro SD, una tarjeta SIM y/o cualquier otro módulo criptográfico, como lo sabe un experto en la técnica que puede insertarse en el dispositivo 102 de comunicación. En la Fig. 2B, el elemento 210 seguro puede ser una tarjeta micro SD (o cualquier otro factor de forma conocido) configurada para comunicarse con el procesador 202 en la PCB 218 a través de un bus 212 de sistema. La Fig. 2C representa una realización alternativa del dispositivo 102 de comunicación, en la que el elemento 210 seguro puede estar físicamente conectado (soldado) a la PCB 218.

La Fig. 3 representa un diagrama de flujo de un método, de acuerdo con algunas realizaciones. Como se muestra, el método 300 comienza en la etapa 302 realizando un procedimiento de intercambio de claves con un punto terminal a través del dispositivo de comunicación por voz para obtener una clave semilla simétrica para una sesión de voz segura con el punto terminal. En la etapa 304, se generan claves de sesión simétricas primera y segunda para la sesión de voz segura en base a la clave semilla simétrica obtenida. En la etapa 306, los paquetes de voz de salida se reciben desde el dispositivo de comunicación por voz en relación con la sesión de voz segura, cada paquete comprende voz de salida una cabecera de paquete de voz de salida y una carga útil de paquete de voz de salida sin cifrar. En la etapa 308, se generan paquetes de voz de salida cifrados dos veces utilizando algoritmos de cifrado simétrico primero y segundo. El primer algoritmo de cifrado simétrico genera respectivas cargas útiles de paquetes de voz de salida cifradas una vez en función de la primera clave de sesión simétrica, todos o parte de las respectivas cabeceras de paquetes de voz de salida y las respectivas cargas útiles de paquetes de voz de salida no cifrados. El segundo algoritmo de cifrado simétrico genera respectivas cargas útiles de paquetes de voz de salida cifrada dos veces en base a la segunda clave de sesión simétrica y las respectivas cargas útiles de paquetes de voz de salida cifrados una vez. En la etapa 310, las respectivas cargas útiles de paquetes de voz de salida dos veces encriptadas se envían al dispositivo de comunicación por voz para ensamblar con las respectivas cabeceras de paquetes de voz de salida para su transmisión al punto terminal en relación con la sesión de voz segura.

En algunas realizaciones, el elemento seguro es un componente implementado en una PCB del dispositivo de comunicación por voz. En algunas realizaciones, el elemento seguro se acopla comunicativamente con el dispositivo de comunicación por voz a través de una conexión SPI.

En algunas realizaciones, el elemento seguro está acoplado comunicativamente con el dispositivo de comunicación por voz a través de una interfaz micro SD. En algunas realizaciones, el elemento seguro se acopla comunicativamente con el dispositivo de comunicación por voz a través de una interfaz SIM.

En algunas realizaciones, el dispositivo de comunicación por voz incluye un teléfono inteligente. En algunas realizaciones, el dispositivo de comunicación por voz incluye unos auriculares.

En algunas realizaciones, el procedimiento de intercambio de claves incluye un procedimiento de intercambio de claves Diffie-Hellman. En algunas realizaciones, el procedimiento de intercambio de claves Diffie-Hellman incluye un procedimiento de intercambio de claves Diffie-Hellman de curva elíptica.

En algunas realizaciones, el método incluye además realizar un procedimiento de autenticación mutua de usuario final con el punto terminal a través del dispositivo de comunicación por voz para la sesión de voz segura. En algunas realizaciones, el procedimiento de autenticación mutua de usuario final incluye un procedimiento de autenticación mutua de usuario final Diffie-Hellman. En algunas realizaciones, el procedimiento de autenticación mutua de usuario final Diffie-Hellman incluye un procedimiento de autenticación mutua de usuario final Diffie-Hellman de curva elíptica.

En algunas realizaciones, el punto terminal es un segundo elemento seguro que está acoplado comunicativamente con un segundo dispositivo de comunicación por voz.

En algunas realizaciones, el método incluye además el uso del primer algoritmo de cifrado simétrico para generar etiquetas de autenticación de paquetes de voz de salida respectivos basados en la primera clave de sesión simétrica, todos o parte de las cabeceras de paquetes de voz de salida respectivos, y las respectivas cargas útiles de paquetes de voz de salida no cifrados, y emitir las respectivas etiquetas de autenticación de paquetes de voz de salida al dispositivo de comunicación por voz para ensamblar con las respectivas cabeceras de paquetes de voz de salida y las respectivas cargas útiles de paquetes de voz de salida cifrada dos veces para su transmisión al punto terminal en relación con la sesión de voz segura.

En algunas realizaciones, el método incluye además recibir paquetes de voz de entrada desde el dispositivo de comunicación por voz en relación con la sesión de voz segura, cada paquete de voz de entrada comprende una cabecera de paquete de voz de entrada y una carga útil del paquete de voz de entrada cifrada dos veces, utilizando el segundo algoritmo de cifrado simétrico para generar respectivas cargas útiles de paquetes de voz de entrada cifradas una vez en función de la segunda clave de sesión simétrica y las respectivas cargas útiles de paquetes de voz de entrada cifrados dos veces, utilizando el primer algoritmo de cifrado simétrico para generar las respectivas cargas útiles de paquete de voz de entrada descifradas basadas en la primera clave de sesión simétrica, todo o parte de las respectivas cabeceras de paquetes de voz de entradas, y las respectivas cargas útiles de paquetes de voz de entrada cifradas una vez, y salida de las respectivas cargas útiles descifradas de paquetes de voz de entrada al dispositivo de comunicación por voz para el reensamblaje con las respectivas cabeceras de paquetes de voz de entrada y la reproducción resultante de las cargas útiles de paquetes de voz de entrada descifrado a través de una interfaz de usuario del dispositivo de comunicación por voz en relación con la sesión de voz segura.

En algunas realizaciones, cada paquete de voz de entrada incluye además una etiqueta de autenticación de paquete de voz de entrada, y el método incluye además el uso del primer algoritmo de cifrado simétrico para autenticar los respectivos paquetes de voz de entrada en función de las respectivas etiquetas de autenticación de paquete de voz de entrada.

En algunas realizaciones, cada paquete de voz de entrada incluye además una etiqueta de autenticación de paquete de voz de entrada, y el método incluye además el uso del primer algoritmo de cifrado simétrico para verificar la integridad de los respectivos paquetes de voz de entrada en función de las respectivas etiquetas de autenticación de paquete de voz de entrada.

En algunas realizaciones, el primer algoritmo de cifrado simétrico es un algoritmo de cifrado simétrico publicado y el segundo algoritmo de cifrado simétrico no es un algoritmo de cifrado simétrico publicado. En algunas realizaciones, el primer algoritmo de cifrado simétrico es un algoritmo seleccionado del grupo que consta de un algoritmo AES, un algoritmo Blowfish, un algoritmo DES, un algoritmo Triple DES, un algoritmo Serpent y un algoritmo Twofish. En algunas realizaciones, los algoritmos de cifrado simétrico primero y segundo son dos algoritmos de cifrado simétrico publicados diferentes.

En algunas realizaciones, los métodos y sistemas descritos en este documento pueden tomar la forma de varios componentes. En algunas realizaciones, los métodos pueden implementarse usando chips, procesadores y otros componentes diversos soldados a una PCB en un dispositivo de comunicación. Alternativamente, los métodos pueden implementarse en una tarjeta microSD, una tarjeta SIM o varios otros factores de forma que pueden insertarse en el dispositivo de comunicación. En algunas realizaciones, el elemento seguro puede implementarse en un dispositivo que está acoplado comunicativamente al dispositivo de comunicación.

La Fig. 4 representa un diagrama de flujo de llamadas 400, de acuerdo con algunas realizaciones. Como se muestra, el elemento 1 seguro realiza un intercambio de claves con el elemento 2 seguro en 402. En algunos casos, el intercambio de claves se realiza mediante un procedimiento Diffie-Hellman. En algunas realizaciones, también se realiza una autenticación mutua. El elemento 1 seguro recibe un paquete de datos sin cifrar del dispositivo 1 móvil en 404. Como se mencionó anteriormente, el paquete de datos sin cifrar puede ser datos de voz, sin embargo, también puede ser otra forma de paquete de datos como texto, vídeo o imágenes. El elemento 1 seguro genera, en 406, un paquete de datos cifrado dos veces basado en los algoritmos de cifrado descritos en el método 300. El paquete de datos cifrado dos veces se envía, en 408, desde el dispositivo 1 móvil al dispositivo 2 móvil a través de la red. En algunas realizaciones, la red puede ser una red de área amplia (WAN) tal como una red celular, Wi-Fi o varias otras WAN conocidas por los expertos en la técnica. Alternativamente, los dispositivos móviles 1 y 2 pueden comunicarse entre sí a través de redes de área personal (PAN), tales como Bluetooth, o redes de comunicación de campo cercano (NFC), para transmitir imágenes o texto, en algunas realizaciones.

El elemento 2 seguro recibe, en 410, el paquete de datos cifrado dos veces desde el dispositivo 2 móvil, y utiliza los algoritmos de descifrado descritos anteriormente, genera, en 412, un paquete de datos descifrado y lo proporciona al dispositivo 2 móvil. Un usuario puede proporcionar entrada al dispositivo 2 móvil, que puede proporcionar, en la etapa 414, la entrada para asegurar el elemento 2 en forma de un paquete de datos sin cifrar. El elemento 2 seguro crea de forma similar, en la etapa 416, un paquete de datos cifrado dos veces para transmitir, en la etapa 418, de vuelta al dispositivo 1 móvil utilizando el dispositivo 2 móvil a través de la red. El dispositivo 1 móvil entrega el paquete de datos doblemente cifrado recibido al elemento 1 seguro en 420, que lo descifra usando algoritmos similares usados para generar, en 422, el paquete de datos dos veces cifrado, y envía el paquete de datos descifrado al dispositivo 1 móvil para reproducción, por ejemplo.

La Fig. 5A representa un diagrama de bloques de un dispositivo 500 móvil, de acuerdo con algunas realizaciones. Se describirán varias realizaciones en relación con las Figs. 5B-5E. La Fig. 5B representa el elemento 502 de seguridad, de acuerdo con algunas realizaciones. Como se muestra, el elemento 502 seguro incluye un módulo 505 de negociación de sesión, un módulo 510 de generación de clave de sesión, un primer algoritmo 515 de cifrado simétrico y un segundo algoritmo 520 de cifrado simétrico. Por conveniencia, la aplicación 525 móvil también se muestra para ilustrar el empaquetamiento, de acuerdo con algunas realizaciones. La aplicación 525 móvil puede estar ejecutándose en un dispositivo de comunicación por voz o cualquier otro tipo de dispositivo de comunicación. Las realizaciones descritas en el presente documento están asociadas con dispositivos de comunicación por voz, sin embargo, debe tenerse en cuenta que son posibles otros tipos de dispositivos de comunicación. Algunos ejemplos son los dispositivos de comunicación de texto, los dispositivos de comunicación de audio, los dispositivos de comunicación de video y similares. El módulo 505 de negociación de sesión está configurado para realizar un procedimiento de intercambio de claves con un punto terminal a través de la interfaz de comunicación y el dispositivo de comunicación por voz para obtener una clave semilla simétrica 'S' para una sesión de voz segura con el punto terminal, y para pasar la clave semilla simétrica obtenida para el módulo de generación de claves de sesión. En algunas realizaciones, el módulo 505 de negociación de sesión usa un algoritmo de firma digital de curva elíptica (ECDSA). El módulo 510 de generación de claves de sesión recibe la clave semilla simétrica 'S' obtenida del módulo de negociación de sesión, genera una primera y segunda claves de sesión simétricas '1' y '2' para la sesión de voz segura basada en la clave semilla simétrica obtenida, pasa la primera clave de sesión simétrica '1' al primer módulo 515 de cifrado simétrico, y pasa la segunda clave de sesión simétrica '2' al segundo módulo 520 de cifrado simétrico.

En algunas realizaciones, el módulo de generación de claves de sesión se configura para generar la primera y segunda claves de sesión simétricas para la sesión de voz segura basada en la clave semilla simétrica obtenida incluye configurar el módulo de generación de claves de sesión para utilizar un algoritmo de diversificación simétrica para generar la primera y segunda claves de sesión simétricas para la sesión de voz segura basada en la clave semilla simétrica obtenida. En alguna realización, la diversificación simétrica incluye un algoritmo de diversificación simétrica AES.

El primer módulo 515 de cifrado simétrico está configurado para recibir la primera clave de sesión simétrica '1' del módulo 510 de generación de clave de sesión y para recibir paquetes de voz de salida del dispositivo de comunicación por voz a través de la interfaz de comunicación como parte de la sesión de voz segura. Cada paquete de voz de salida recibido incluye una cabecera de paquete de voz de salida y una carga útil de paquete de voz de salida sin cifrar. la cabecera del paquete de voz de salida garantiza que cada paquete de carga útil de paquete de voz de salida sin cifrar esté cifrado de forma única, independientemente del contenido. En algunas formas de realización, el paquete de voz de salida sin cifrar recibido incluye una cabecera de paquete de voz de salida de 16 bits unido a la carga útil del paquete de voz de salida sin cifrar. En tales realizaciones, la cabecera puede analizarse a partir de la carga útil utilizando un analizador en el elemento seguro, que se muestra como analizador 530. En algunas realizaciones, el primer módulo 515 de cifrado simétrico genera cargas útiles de paquetes de voz de salida cifradas una vez basadas en la primera clave de sesión simétrica '1', todo o parte de las cabeceras del paquete de voz de salida, y las cargas útiles del paquete de voz de salida sin cifrar, y pasa las cargas útiles del paquete de voz de salida cifradas una vez al segundo módulo 520 de cifrado simétrico.

En algunas realizaciones, el primer módulo 515 de cifrado simétrico está configurado además para utilizar el primer algoritmo de cifrado simétrico para generar etiquetas de autenticación de paquetes de voz de salida respectivos basados en la primera clave de sesión simétrica, las cabeceras de paquete de voz de salida respectivos y cargas útiles de paquetes de voz de salida no cifrados respectivos, y generar las respectivas etiquetas de autenticación de paquetes de voz de salida para ensamblar con las respectivas cabeceras de paquetes de voz de salida y las respectivas cargas útiles de paquetes de voz de salida cifrados dos veces para su transmisión al punto terminal en relación con la sesión de voz segura (como se muestra en la Fig. 5C).

En algunas realizaciones, cada cabecera de paquete de voz de salida incluye un valor SSRC respectivo, y el primer módulo 515 de cifrado simétrico está configurado para utilizar el primer algoritmo de cifrado simétrico para generar las respectivas etiquetas de autenticación de paquete de voz de salida basadas en las respectivas cabeceras de paquetes de voz incluyen el primer módulo 515 de cifrado simétrico que está configurado para utilizar el primer algoritmo de cifrado simétrico para generar las etiquetas de autenticación de paquetes de voz de salida respectivos basados en los valores de índice respectivos en las respectivas cabeceras de paquetes de voz de salida.

En algunas realizaciones, cada cabecera de paquete de voz de salida incluye además un valor SSRC respectivo, y el primer módulo 515 de cifrado simétrico está configurado para utilizar el primer algoritmo de cifrado simétrico para generar las etiquetas de autenticación de paquetes de voz de salida respectivos basados en las respectivas cabeceras de paquetes de voz de salida incluyen además el primer módulo 515 de cifrado simétrico que está configurado para utilizar el primer algoritmo de cifrado simétrico para generar las etiquetas de autenticación de paquetes de voz de salida respectivos basados en los valores SSRC respectivos en las cabeceras de paquetes de voz de salida respectivos.

El segundo módulo 520 de cifrado simétrico está configurado para recibir la segunda clave de sesión simétrica '2' del módulo 510 de generación de claves de sesión y para recibir las cargas útiles de paquetes de voz de salida cifrados una vez del primer módulo 515 de cifrado simétrico. El segundo módulo 520 de cifrado simétrico genera cargas útiles de paquetes de voz de salida cifrados dos veces basándose en la segunda clave de sesión simétrica '2' y las cargas útiles de paquetes de voz de salida cifrados una vez, y pasa las cargas útiles de paquetes de voz de salida cifrados dos veces al módulo 535 de ensamblaje de paquetes de voz de salida en la aplicación 525 móvil.

En algunas realizaciones, el módulo 535 de ensamble de paquetes de voz de salida en el dispositivo de comunicación por voz está configurado para recibir las cabeceras del paquete de voz de salida y, en algunas realizaciones, las etiquetas de autenticación de paquetes de voz de salida del primer módulo 515 de cifrado simétrico, y recibir las cargas útiles de paquetes de voz de salida cifrados dos veces desde el segundo módulo 520 simétrico de cifrado. El módulo 530 de ensamblaje de paquetes de voz de salida ensambla paquetes de voz de salida cifrados dos veces a partir de las cabeceras de paquetes de voz de salida, las cargas útiles de paquetes de voz de salida cifrados dos veces y, en algunas realizaciones, las etiquetas de autenticación de paquetes de voz de salida y envía los paquetes de voz de salida ensamblados dos veces cifrados a través de la interfaz de comunicación al dispositivo de comunicación por voz para su transmisión al punto terminal como parte de las sesiones de voz seguras.

En algunas realizaciones, el segundo módulo 520 de cifrado simétrico que está configurado para generar las cargas útiles de paquetes de voz de salida cifrados dos veces incluye configurar el segundo módulo de cifrado simétrico para enviar las cargas útiles de paquetes de voz de salida cifrados dos veces al dispositivo de comunicación por voz. para ensamblar con las respectivas cabeceras de paquetes de voz de salida para su transmisión al punto terminal en relación con la sesión de voz segura.

En algunas realizaciones, el procedimiento de intercambio de claves incluye un procedimiento de intercambio de claves Diffie-Hellman. En algunas realizaciones, el procedimiento de intercambio de claves Diffie-Hellman incluye un procedimiento de intercambio de claves Diffie-Hellman de curva elíptica.

En algunas realizaciones, el módulo 505 de negociación de sesión está configurado además para realizar un procedimiento de autenticación mutua del usuario final con el punto terminal a través de la interfaz de comunicación y el dispositivo de comunicación por voz para la sesión de voz segura. En algunas realizaciones, el procedimiento de autenticación mutua de usuario final incluye un procedimiento de autenticación mutua de usuario final Diffie-Hellman. En algunas realizaciones, el procedimiento de autenticación mutua de usuario final Diffie-Hellman incluye un procedimiento de autenticación mutua de usuario final Diffie-Hellman de curva elíptica.

En algunas realizaciones, el punto terminal es un segundo elemento seguro que está acoplado comunicativamente con un segundo dispositivo de comunicación por voz. En algunas realizaciones, el elemento 502 seguro incluye un componente en una PCB del dispositivo de comunicación por voz. En algunas realizaciones, el elemento 502 seguro está configurado para acoplarse comunicativamente con el dispositivo de comunicación por voz, incluye el elemento seguro configurado para acoplarse comunicativamente con el dispositivo de comunicación por voz por medio de una interfaz micro SD. En algunas realizaciones, configurar el elemento seguro para que se acople comunicativamente con el dispositivo de comunicación por voz incluye configurar el elemento seguro para que se acople comunicativamente con el dispositivo de comunicación por voz por medio de una interfaz SIM. En algunas realizaciones, el dispositivo de comunicación por voz incluye un teléfono inteligente. En algunas realizaciones, el dispositivo de comunicación por voz incluye unos auriculares.

En algunas realizaciones, el primer algoritmo 515 de cifrado simétrico es un algoritmo de cifrado simétrico publicado, y el segundo algoritmo 520 de cifrado simétrico no es un algoritmo de cifrado simétrico publicado. En algunas realizaciones, el primer algoritmo de cifrado simétrico es un algoritmo seleccionado del grupo que consta de un algoritmo AES, un algoritmo Blowfish, un algoritmo DES, un algoritmo Triple DES, un algoritmo Serpent y un algoritmo Twofish. En algunas realizaciones, los algoritmos de cifrado simétrico primero y segundo son dos algoritmos de cifrado simétrico publicados diferentes.

La Fig. 5D representa una realización del elemento 502 seguro que descifra los paquetes de voz recibidos dos veces cifrados. Como se muestra, el segundo módulo 520 de cifrado simétrico recibe paquetes de voz de entrada cifrados dos veces desde el punto terminal a través del dispositivo de comunicación por voz que ejecuta la aplicación 525 móvil y la interfaz de comunicación, donde cada paquete de voz de entrada recibido cifrado dos veces incluye una cabecera de paquete de voz de entrada y una carga útil de paquete de voz de entrada cifrada dos veces. El segundo módulo

520 de cifrado simétrico genera cargas útiles de paquetes de voz de entrada cifradas una vez basadas en la segunda clave de sesión simétrica '2' y las cargas útiles de paquetes de voz de entrada cifradas dos veces, y pasa las cabeceras de paquetes de voz de entrada y las cargas útiles de paquetes de voz de entrada cifrados una vez al primer módulo 515 de cifrado simétrico.

El primer módulo 515 de cifrado simétrico recibe las cabeceras del paquete de voz de entrada y las cargas útiles del paquete de voz de entrada cifrado una vez del segundo módulo de cifrado simétrico, y genera cargas útiles de paquetes de voz de entrada descifradas basadas en la primera clave de sesión simétrica '1', todos o parte de las cabeceras de los paquetes de voz de entrada y las cargas útiles de los paquetes de voz de entrada cifradas una vez. El primer módulo 515 de cifrado simétrico envía las cargas útiles del paquete de voz de entrada descifrado al dispositivo de comunicación por voz para ensamblar con las respectivas cabeceras del paquete de voz de entrada y la reproducción resultante de las cargas útiles del paquete de voz de entrada descifrado a través de una interfaz de usuario del dispositivo de comunicación por voz en relación con la sesión de voz segura.

En algunas realizaciones, el elemento seguro emite cada carga útil de paquete de voz de entrada descifrado corriente de cada paquete de voz de entrada corriente antes de recibir un paquete de voz de entrada siguiente respectivo.

En algunas formas de realización, el elemento seguro está configurado para separar y procesar múltiples paquetes de voz de entrada en un momento dado.

En algunas realizaciones, cada cabecera de paquete de voz de entrada incluye un valor de índice respectivo, y el primer módulo de cifrado simétrico está configurado para utilizar el primer algoritmo de cifrado simétrico para generar las cargas útiles del paquete de voz de entrada descifrado basado en las cabeceras de paquetes de voz de entrada incluyen el primer módulo de cifrado simétrico que se configura para utilizar el primer algoritmo de cifrado simétrico para generar las cargas útiles de paquetes de voz de entrada descifrados basándose en los valores de índice respectivos en las cabeceras de paquetes de voz de entrada respectivos.

En algunas realizaciones, cada cabecera de paquete de voz de entrada incluye además un valor SSRC respectivo, y el primer módulo de cifrado simétrico está configurado para utilizar el primer algoritmo de cifrado simétrico para generar las cargas útiles del paquete de voz de entrada descifrado en base a la cabecera de paquete de voz de entrada e incluyen además el primer módulo de cifrado simétrico que se configura para utilizar el primer algoritmo de cifrado simétrico para generar las cargas útiles de paquetes de voz de entrada descifrados en base a los valores SSRC respectivos en las cabeceras de paquetes de voz de entrada respectivos.

En algunas realizaciones, cada paquete de voz de entrada incluye además una etiqueta de autenticación de paquetes de voz de entrada, y el primer módulo de cifrado simétrico está configurado además para autenticar los paquetes de voz de entrada en función de las etiquetas de autenticación de paquetes de voz de entrada (como se muestra en la Figura 5E). En algunas realizaciones, cada paquete de voz de entrada incluye además una etiqueta de autenticación de paquetes de voz de entrada, y el primer módulo de cifrado simétrico está configurado además para verificar la integridad de los respectivos paquetes de voz de entrada en función de las etiquetas de autenticación de paquetes de voz de entrada respectivos.

De acuerdo con las realizaciones anteriores, todo o parte de la cabecera del paquete se usa como parámetro de diversificación en combinación con el primer cifrado simétrico para generar la carga útil del paquete cifrado una vez (de entrada, o salida). En tal caso, incluso si la carga útil es la misma para dos paquetes, el resultado de la carga útil cifrada será diferente debido al hecho de que al menos una parte de la cabecera es diferente. En una realización alternativa, el parámetro de diversificación no se aplica al primer cifrado simétrico (o descifrado simétrico) sino al segundo cifrado simétrico (o descifrado simétrico). Desde un punto de vista criptográfico, el nivel de seguridad obtenido por la carga útil del paquete cifrado dos veces es el mismo. En una realización adicional, el parámetro de diversificación se puede aplicar en el primer y segundo cifrado simétrico (o descifrado).

Aunque las características y elementos se describen anteriormente en combinaciones particulares, los expertos en la técnica apreciarán que cada característica o elemento se puede utilizar solo o en cualquier combinación con las otras características y elementos sin apartarse del alcance de la presente divulgación. Las realizaciones descritas en forma de método pueden tener realizaciones de sistema análogas y viceversa.

REIVINDICACIONES

1. Un método (300) llevado a cabo por un elemento (210, 502) seguro que está acoplado comunicativamente con un dispositivo (102) de comunicación por voz, el método comprende:

realizar (302) un procedimiento de intercambio de claves con un punto (118) terminal a través del dispositivo de comunicación por voz para obtener una clave semilla simétrica para una sesión de voz segura con el punto terminal;

generar (304) claves de sesión simétricas primera y segunda para la sesión de voz segura en base a la clave semilla simétrica obtenida;

recibir (306) paquetes de voz de salida desde el dispositivo de comunicación por voz en relación con la sesión de voz segura, cada paquete de voz de salida comprende una cabecera de paquete de voz de salida y una carga útil de paquete de voz de salida sin cifrar;

utilizar (308) un primer algoritmo de cifrado simétrico para generar respectivas cargas útiles de paquetes de voz de salida cifradas una vez basadas en la primera clave de sesión simétrica, todos o parte de las respectivas cabeceras del paquete de voz de salida, y las respectivas cargas útiles de paquetes de voz de salida no cifrados;

utilizar (308) un segundo algoritmo de cifrado simétrico para generar respectivas cargas útiles de paquetes de voz de salida cifrados dos veces basándose en la segunda clave de sesión simétrica y las respectivas cargas útiles de paquetes de voz de salida cifradas una vez; y

emitir (310) las respectivas cargas útiles de paquetes de voz de salida cifrada dos veces al dispositivo de comunicación por voz para ensamblar con las respectivas cabeceras de paquetes de voz de salida para su transmisión al punto (118) terminal en relación con la sesión de voz segura.

2. El método (300) de la reivindicación 1, en el que:

cada cabecera de paquete de voz de salida comprende un valor de índice respectivo; y

utilizar (308) el primer algoritmo de cifrado simétrico para generar las respectivas cargas útiles de paquetes de voz de salida cifrados una vez en base a todas o parte de las respectivas cabeceras de paquetes de voz de salida comprende utilizar el primer algoritmo de cifrado simétrico para generar las respectivas cargas útiles cifradas de paquetes de voz de salida basadas en los valores de índice respectivos en las respectivas cabeceras del paquete de voz de salida.

3. El método (300) de la reivindicación 1 o 2, en el que:

cada cabecera de paquete de voz de salida comprende además un valor de fuente de sincronización (SSRC) respectivo; y

utilizar (308) el primer algoritmo de cifrado simétrico para generar las respectivas cargas útiles de paquetes de voz de salida cifrados una vez en base a todos o parte de las respectivas cabeceras de paquetes de voz de salida comprende además utilizar el primer algoritmo de cifrado simétrico para generar las respectivas cargas útiles cifradas de paquetes de voz de salida basadas en los valores SSRC respectivos en las respectivas cabeceras de paquetes de voz de salida.

4. El método (300) de cualquiera de las reivindicaciones 1-3, que comprende, además:

utilizar (308) el primer algoritmo de cifrado simétrico para generar etiquetas de autenticación de paquetes de voz de salida respectivos basados en la primera clave de sesión simétrica, todo o parte de las respectivas cabeceras de paquetes de voz de salida y las respectivas cargas útiles de paquetes de voz de salida no cifrados; y

emitir (310) las respectivas etiquetas de autenticación de paquetes de voz de salida al dispositivo de comunicación por voz para ensamblar con las respectivas cabeceras de paquetes de voz de salida y las respectivas cargas útiles de paquetes de voz de salida cifrados dos veces para su transmisión al punto terminal en relación con la sesión de voz segura.

5. El método (300) de la reivindicación 4, en el que:

cada cabecera de paquete de voz de salida comprende un valor de índice respectivo; y

usar (308) el primer algoritmo de cifrado simétrico para generar las respectivas etiquetas de autenticación de paquetes de voz de salida basadas en las respectivas cabeceras de paquetes de voz de salida comprende utilizar el primer algoritmo de cifrado simétrico para generar las respectivas etiquetas de autenticación de paquetes de voz de salida basadas en los valores de índice respectivos en las respectivas cabeceras de paquetes de voz de salida.

6. El método (300) de la reivindicación 5, en el que:

cada cabecera de paquete de voz de salida comprende además un valor de fuente de sincronización (SSRC) respectivo; y

usar (308) el primer algoritmo de cifrado simétrico para generar las respectivas etiquetas de autenticación de paquetes de voz de salida basadas en las respectivas cabeceras de paquetes de voz de salida comprende además utilizar el primer algoritmo de cifrado simétrico para generar las respectivas etiquetas de autenticación de paquetes de voz de salida basadas en los respectivos valores SSRC en las respectivas cabeceras de paquetes de voz de salida.

7. El método (300) de cualquiera de las reivindicaciones 1-6, que comprende, además:

recibir paquetes de voz de entrada desde el dispositivo de comunicación por voz en relación con la sesión de voz segura, cada paquete de voz de entrada comprende una cabecera de paquete de voz de entrada y una carga útil cifrada del paquete de voz de entrada;

usar el segundo algoritmo de cifrado simétrico para generar respectivas cargas útiles de paquetes de voz de entrada cifradas una vez en base a la segunda clave de sesión simétrica y las respectivas cargas útiles de paquetes de voz de entrada cifrada dos veces;

utilizar el primer algoritmo de cifrado simétrico para generar respectivas cargas útiles de paquetes de voz de entrada descifrados en base a la primera clave de sesión simétrica, todas o parte de las respectivas cabeceras de paquetes de voz de entrada y las respectivas cargas útiles de paquetes de voz de entrada cifradas una vez; y

emitir las respectivas cargas útiles de paquetes de voz de entrada descifradas al dispositivo de comunicación por voz para ensamblar con las respectivas cabeceras de paquetes de voz de entrada y la reproducción resultante de las cargas útiles de paquetes de voz de entrada descifrados a través de una interfaz de usuario del dispositivo de comunicación por voz en relación con la sesión de voz segura.

8. El método (300) de la reivindicación 7, en el que:

cada cabecera de paquete de voz de entrada comprende un valor de índice respectivo; y

utilizar el primer algoritmo de cifrado simétrico para generar las respectivas cargas útiles de paquetes de voz de entrada descifrados en base a todo o parte de las respectivas cabeceras de paquetes de voz de entrada comprende utilizar el primer algoritmo de cifrado simétrico para generar las respectivas cargas útiles de paquetes de voz de entrada descifrados en base a los valores de índice respectivos en las respectivas cabeceras del paquete de voz de entrada.

9. El método (300) de la reivindicación 8, en el que:

cada cabecera de paquete de voz de entrada comprende además un valor de fuente de sincronización (SSRC) respectivo; y

utilizar el primer algoritmo de cifrado simétrico para generar las respectivas cargas útiles de paquetes de voz de entrada descifrados en base a la totalidad o parte de las respectivas cabeceras de paquetes de voz de entrada comprende además utilizar el primer algoritmo de cifrado simétrico para generar las respectivas cargas útiles de paquetes de voz de entrada descifrados basados en los respectivos valores SSRC en las respectivas cabeceras de paquetes de voz de entrada.

10. El método (300) de la reivindicación 7, en el que cada paquete de voz de entrada comprende además una etiqueta de autenticación de paquete de voz de entrada, el método comprende, además:

utilizar el primer algoritmo de cifrado simétrico para autenticar los respectivos paquetes de voz de entrada en base a las respectivas etiquetas de autenticación de paquetes voz de entrada.

11. El método (300) de la reivindicación 7, en el que cada paquete de voz de entrada comprende además una etiqueta de autenticación de paquete de voz de entrada, además el método comprende:

usar el primer algoritmo de cifrado simétrico para verificar la integridad de los respectivos paquetes de voz de entrada basándose en las respectivas etiquetas de autenticación de paquetes de voz de entrada.

12. El método (300) de cualquiera de las reivindicaciones 1-11, en el que:

el primer algoritmo de cifrado simétrico es un algoritmo de cifrado simétrico publicado; y

el segundo algoritmo de cifrado simétrico es un algoritmo de cifrado simétrico no publicado.

13. El método (300) de cualquiera de las reivindicaciones 1-12, en el que el primer y segundo algoritmos de cifrado simétrico son dos algoritmos de cifrado simétrico publicados diferentes.

14. El método (300) de cualquiera de las reivindicaciones 1-13, en el que el primer y el segundo algoritmos de cifrado simétrico son dos algoritmos de cifrado simétrico diferentes no publicados.

15. Un elemento (502) seguro que comprende:

una interfaz de comunicación;

un módulo (510) de generación de claves de sesión;

un primer módulo (515) de cifrado simétrico;

un segundo módulo (520) de cifrado simétrico;

y un módulo de negociación de sesión (505) que está configurado para:

realizar un procedimiento de intercambio de claves con un punto (118) terminal a través de la interfaz de comunicación y un dispositivo (102) de comunicación por voz para obtener una clave semilla simétrica para una sesión de voz segura con el punto terminal; y pasar la clave semilla simétrica obtenida al módulo (510) de generación de clave de sesión,

en el que el módulo (510) de generación de clave de sesión está configurado para:

recibir la clave semilla simétrica obtenida del módulo (505) de negociación de sesión;

generar claves de sesión simétricas primera y segunda para la sesión de voz segura en base a la clave semilla simétrica obtenida;

pasar la primera clave de sesión simétrica al primer módulo de cifrado simétrico; y

pasar la segunda clave de sesión simétrica al segundo módulo de cifrado simétrico;

en el que el primer módulo (515) de cifrado simétrico está configurado para:

recibir la primera clave de sesión simétrica del módulo de generación de claves de sesión;

recibir paquetes de voz de salida desde el dispositivo de comunicación por voz a través de la interfaz de comunicación como parte de la sesión de voz segura, cada paquete de voz de salida comprende una cabecera de paquete de voz de salida y una carga útil de paquete de voz de salida sin cifrar;

utilizar un primer algoritmo de cifrado simétrico para generar cargas útiles de paquetes de voz de salida cifradas una vez en función de la primera clave de sesión simétrica, todos o parte de las cabeceras del paquete de voz de salida y las cargas útiles de paquetes de voz de salida no cifrados; y

pasar las cargas útiles del paquete de voz de salida cifradas una vez al segundo módulo de cifrado simétrico;

en el que el segundo módulo de cifrado simétrico (520) está configurado para:

recibir la segunda clave de sesión simétrica del módulo de generación de clave de sesión;

recibir las cargas útiles del paquete de voz de salida cifradas una vez desde el primer módulo de cifrado simétrico;

utilizar un segundo algoritmo de cifrado simétrico para generar cargas útiles de paquetes de voz de salida cifrados dos veces en función de la segunda clave de sesión simétrica y las cargas útiles de paquetes de voz de salida cifrados una vez; y

enviar las cargas útiles del paquete de voz de salida dos veces encriptadas al dispositivo (102) de comunicación por voz a través de la interfaz de comunicación para ensamblar con las respectivas cabeceras del paquete de voz de salida para su transmisión al punto (118) terminal en relación con la sesión de voz segura.

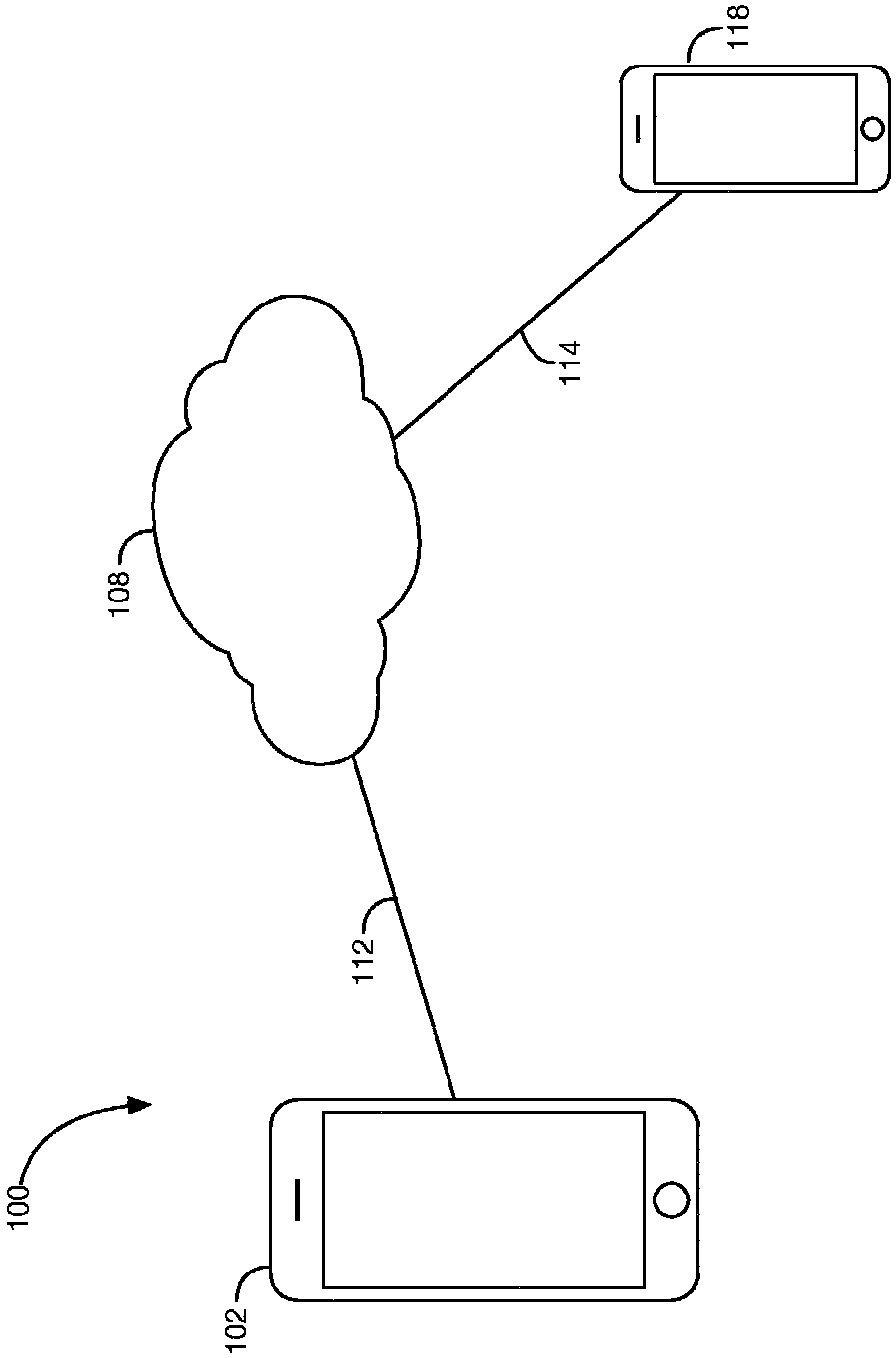

FIG. 1

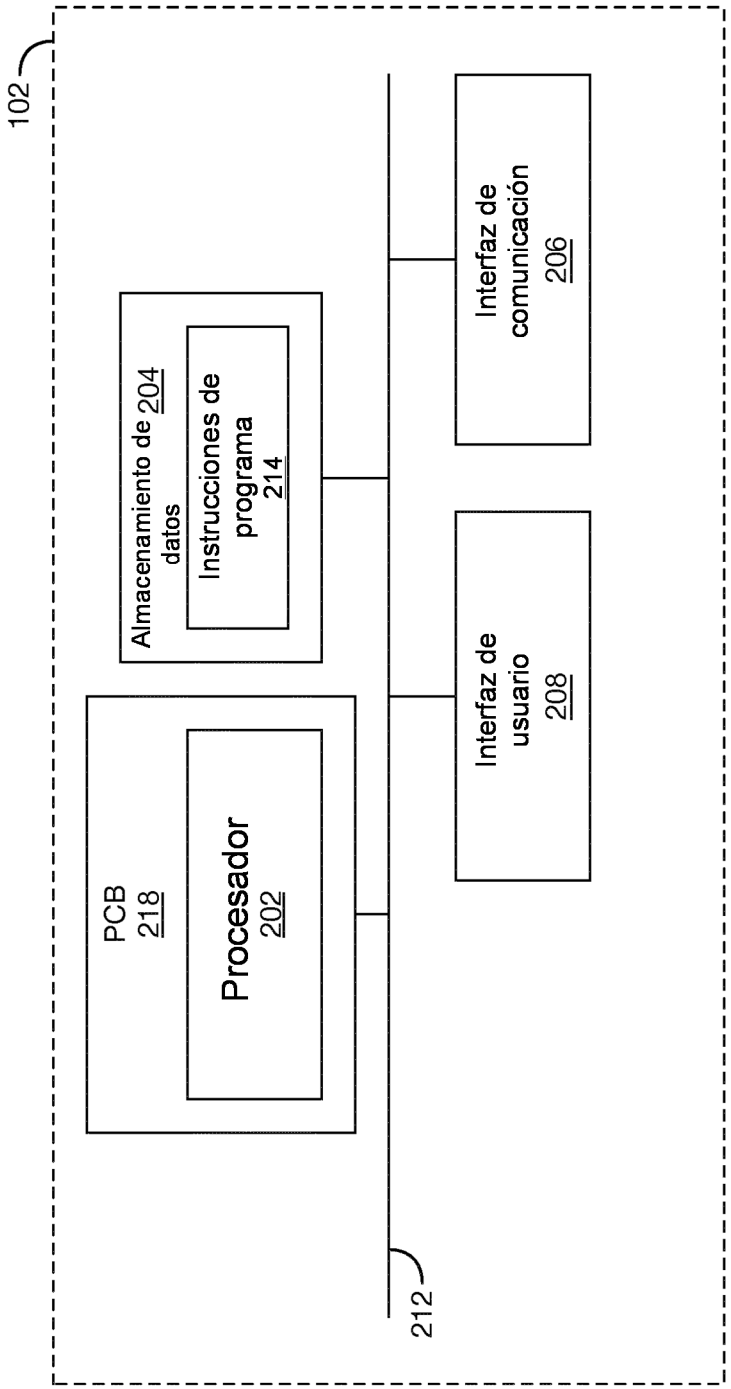
102
PCB
218
Procesador
202
Almacenamiento de datos 204
Instrucciones de programa
214
Interfaz de usuario
208
Interfaz de comunicación
206
212

FIG. 2A

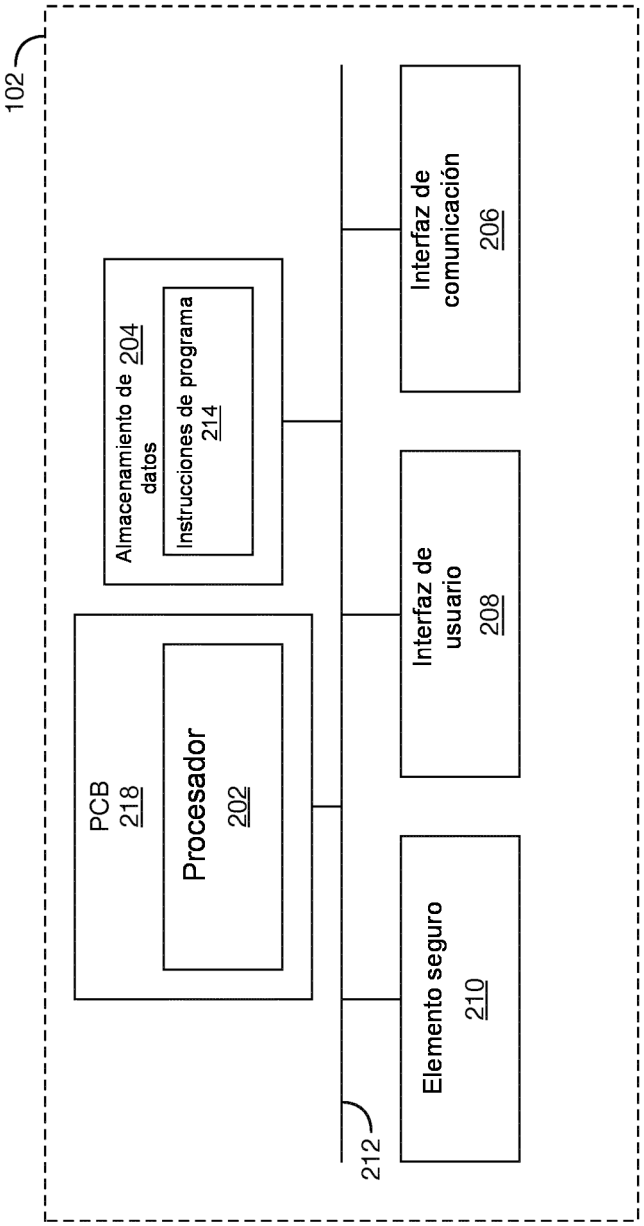
102
PCB
218
Procesador
202
Almacenamiento de datos
204
Instrucciones de programa
214
Interfaz de comunicación
206
Interfaz de usuario
208
Elemento seguro
210
212

FIG. 2B

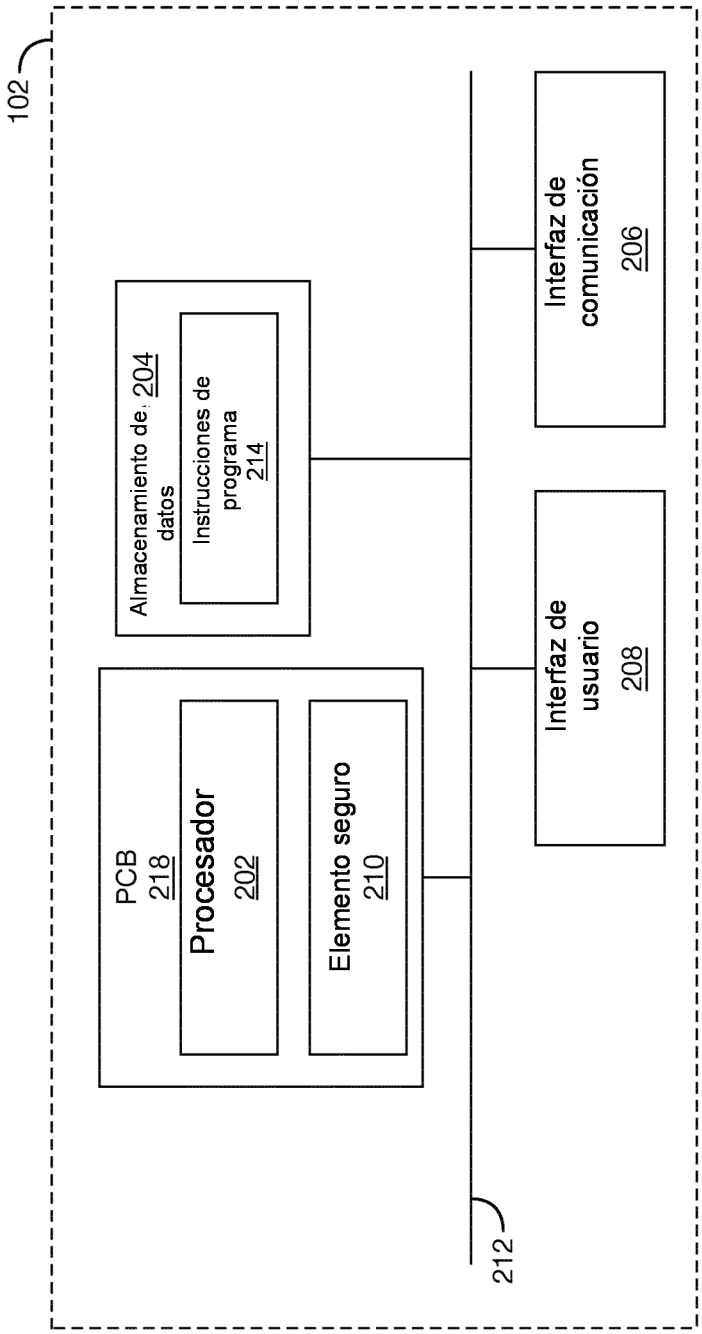
102
Almacenamiento de datos 204
Instrucciones de programa 214
Interfaz de comunicación 206
PCB 218
Procesador 202
Elemento seguro 210
Interfaz de usuario 208
212

FIG. 2C

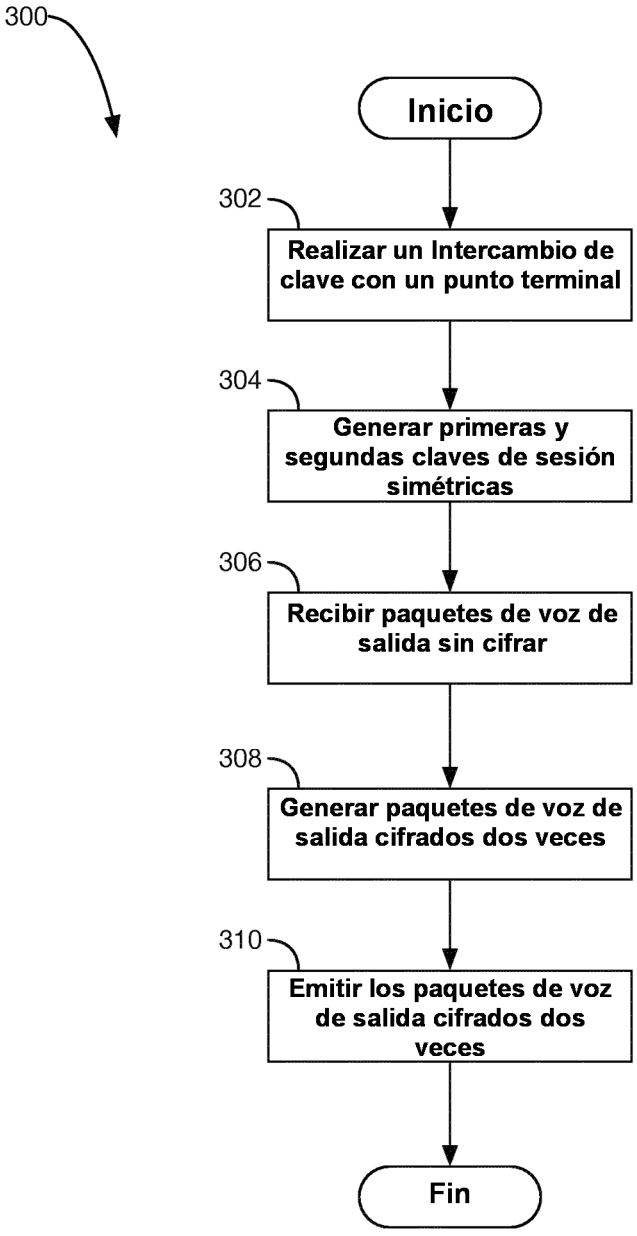
300
Inicio
302
Realizar un Intercambio de clave con un punto terminal
304
Generar primeras y segundas claves de sesión simétricas
306
Recibir paquetes de voz de salida sin cifrar
308
Generar paquetes de voz de salida cifrados dos veces
310
Emitir los paquetes de voz de salida cifrados dos veces
Fin

FIG. 3

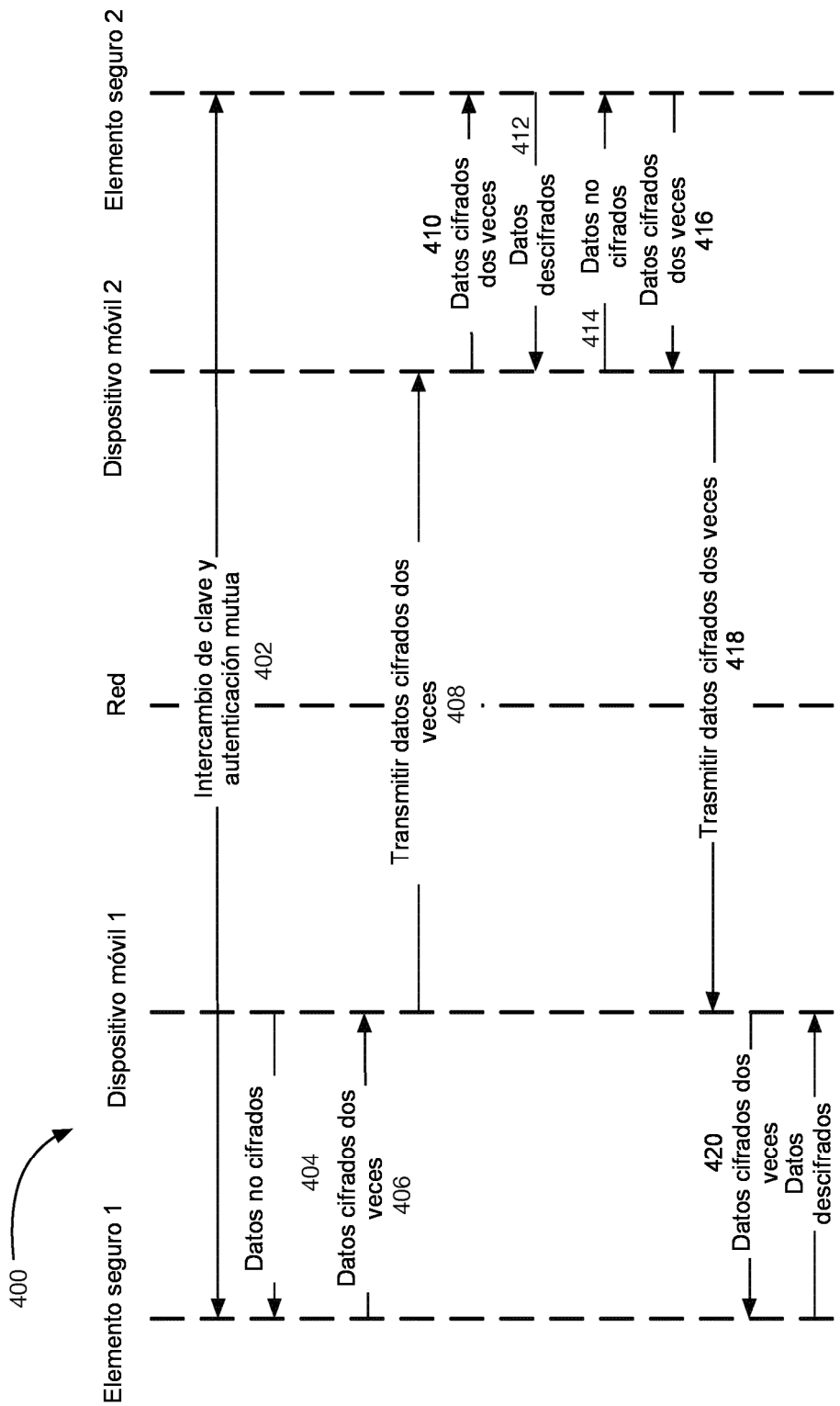
400
Elemento seguro 1
Dispositivo móvil 1
Red
Dispositivo móvil 2
Elemento seguro 2
Intercambio de clave y autenticación mutua
402
Datos no cifrados
404
Datos cifrados dos veces
406
Transmitir datos cifrados dos veces
408
410
Datos cifrados dos veces
Datos descifrados
412
Datos no cifrados
414
Datos cifrados dos veces
416
Trasmitir datos cifrados dos veces
418
420
Datos cifrados dos veces
Datos descifrados
422

FIG. 4

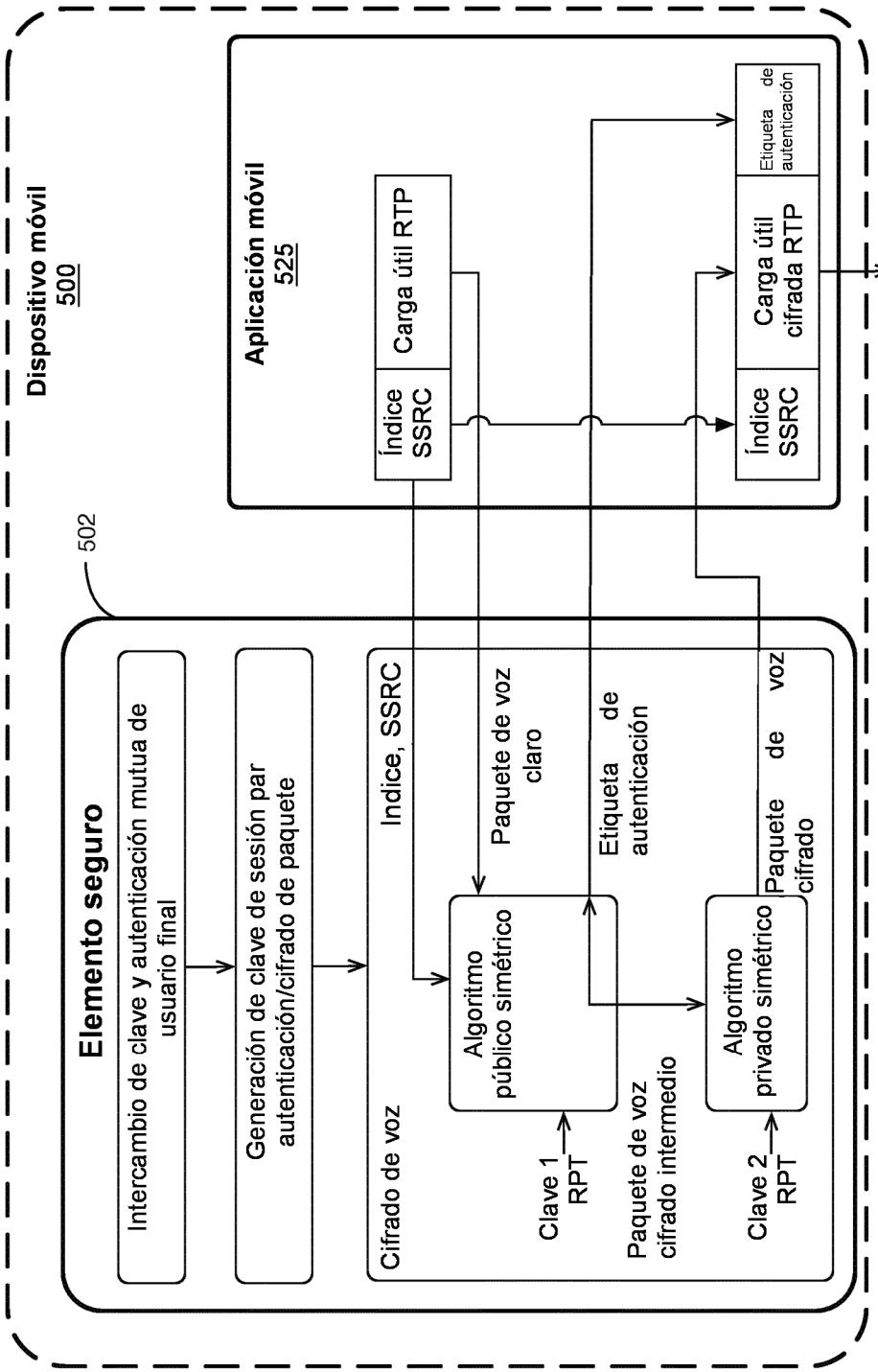
Dispositivo móvil
500
Aplicación móvil
525
Índice SSRC
Carga útil RTP
Índice SSRC
Carga útil cifrada RTP
Etiqueta de autenticación
502
Elemento seguro
Intercambio de clave y autenticación mutua de usuario final
Generación de clave de sesión par autenticación/cifrado de paquete
Cifrado de voz
Indice, SSRC
Algoritmo público simétrico
Paquete de voz claro
Etiqueta de autenticación
Algoritmo privado simétrico
Paquete de voz cifrado
Clave 1 RPT
Paquete de voz cifrado intermedio
Clave 2 RPT

FIG. 5A

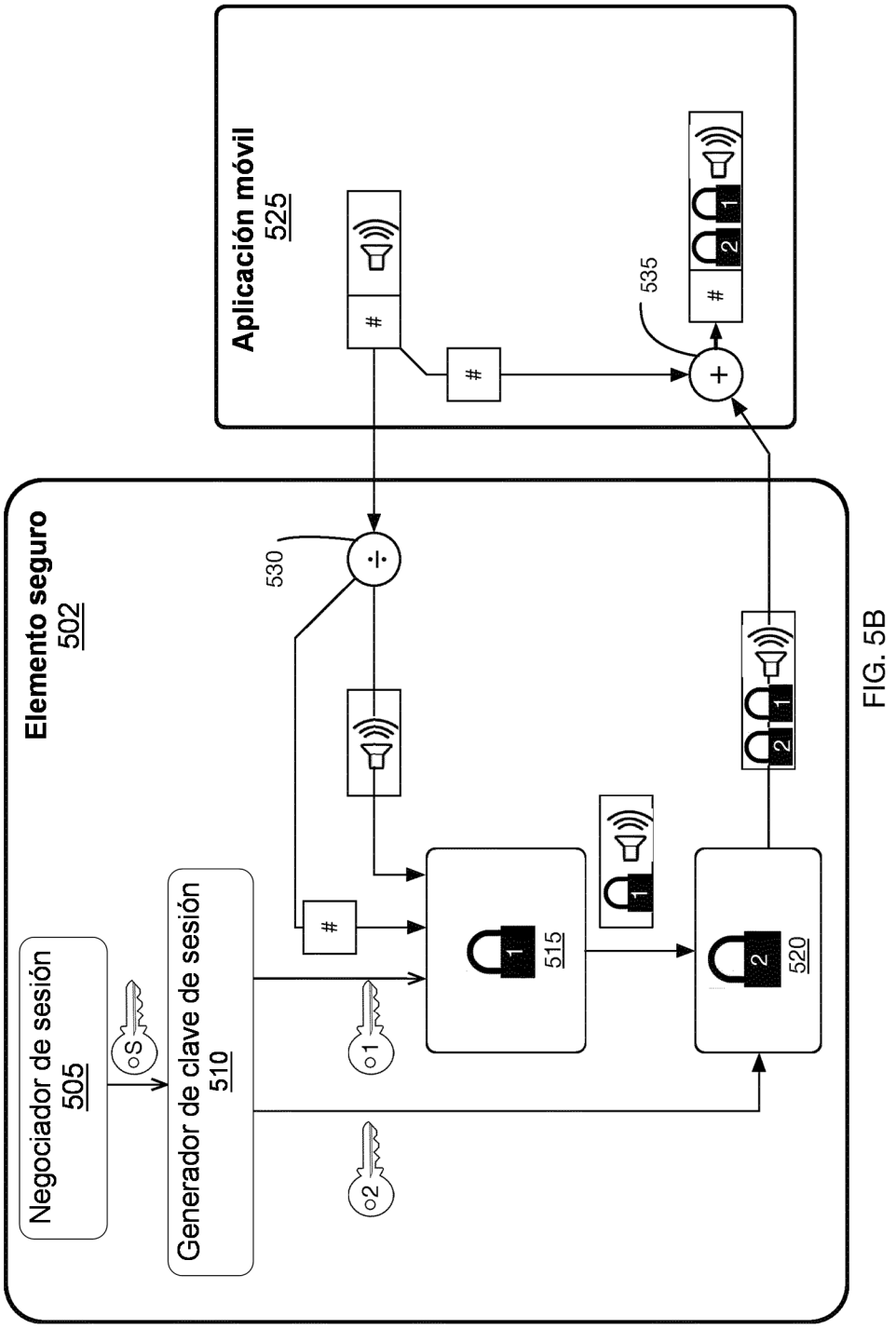
Aplicación móvil
525
Elemento seguro
502
Negociador de sesión
505
Generador de clave de sesión
510
515
520
530
535
#
+
÷
S
1
2

FIG. 5B

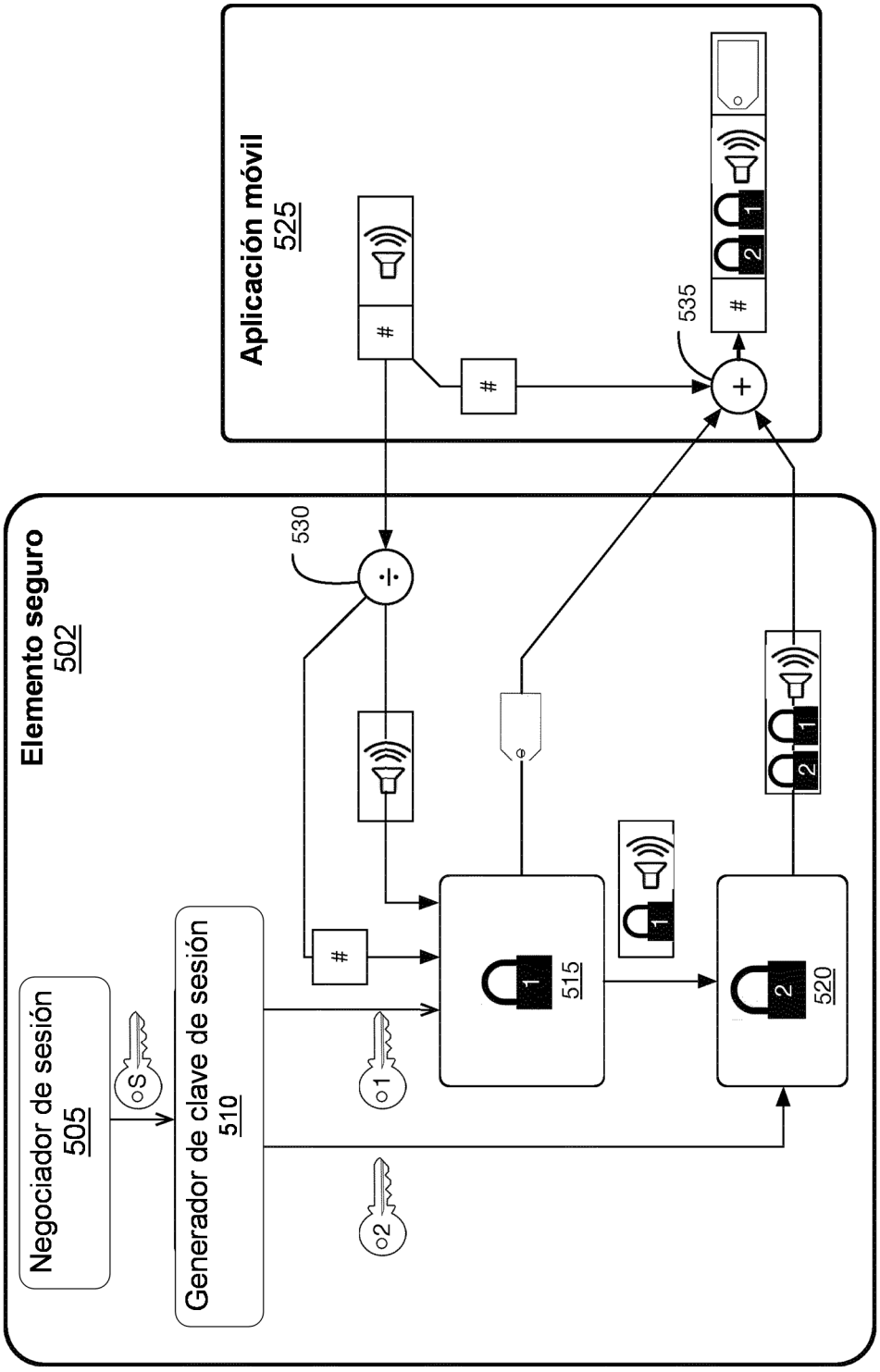
Elemento seguro
502
Negociador de sesión
505
Generador de clave de sesión
510
Aplicación móvil
525
530
535
515
520
S
1
2
#
+
÷

FIG. 5C

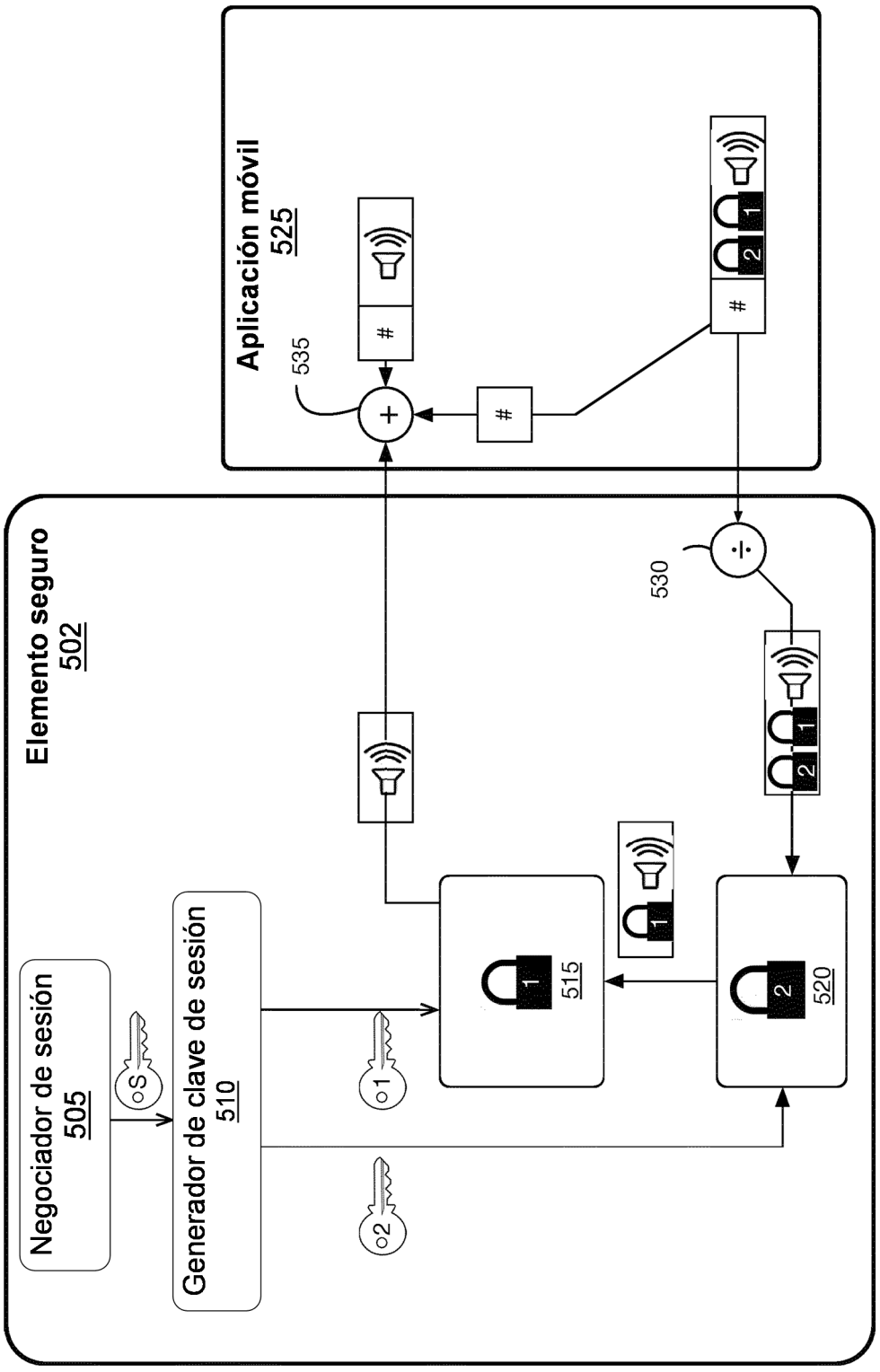
Aplicación móvil
525
535
#
+
#
#
1
2
530
÷
Elemento seguro
502
Negociador de sesión
505
Generador de clave de sesión
510
S
1
2
1
515
1
520
2
1
2

FIG. 5D

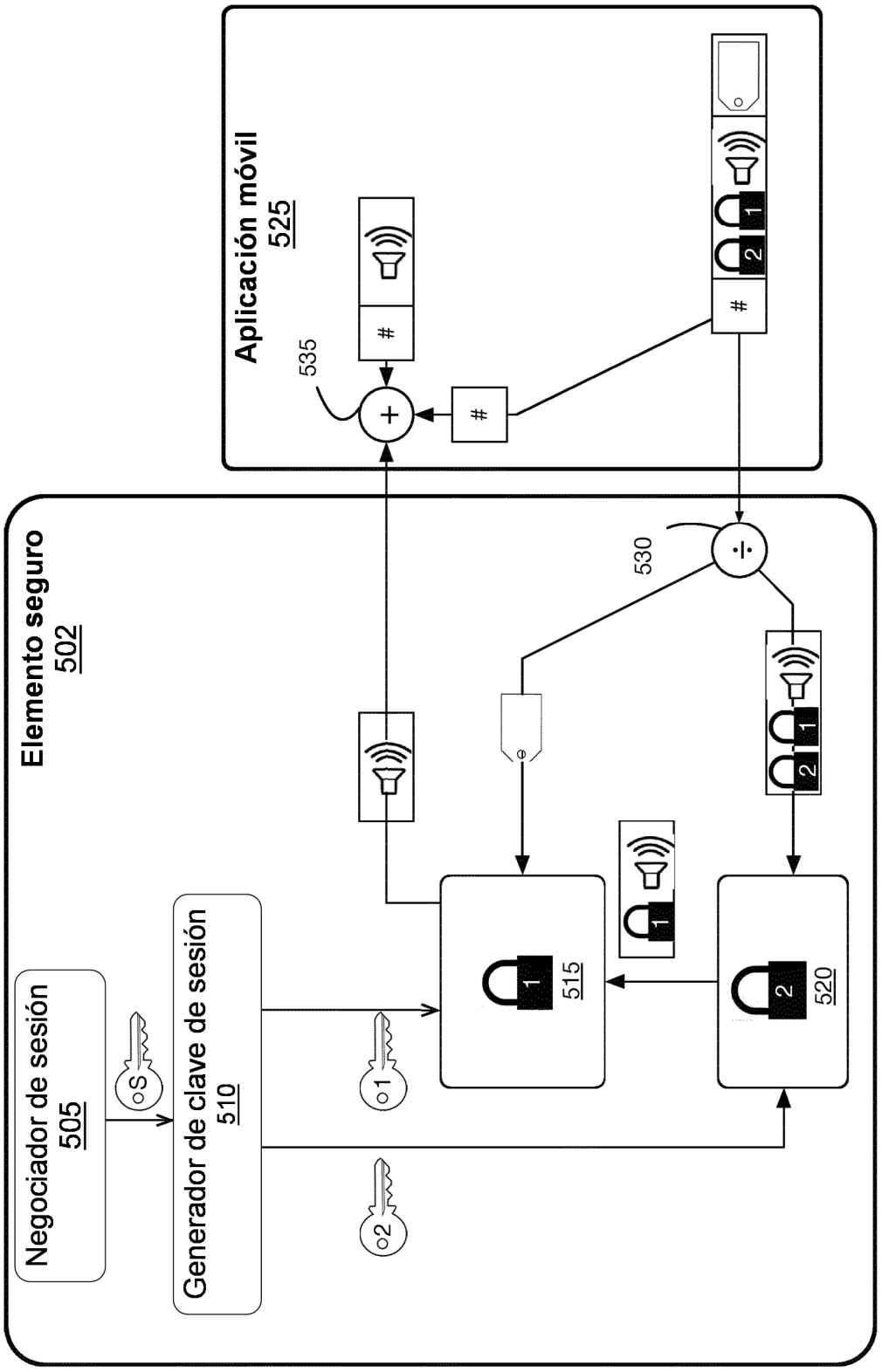
Aplicación móvil
525
535
#
+
#
#
1
2
Elemento seguro
502
530
÷
Negociador de sesión
505
Generador de clave de sesión
510
S
1
2
1
515
2
520
1
2

FIG. 5E