(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 397 109**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.09.2005 E 05798616 (8)**

(97) Fecha y número de publicación de la concesión europea: **07.11.2012 EP 1803274**

(54) Título: **Determinación de una clave de cifrado de sesión durante una sesión de servicio de difusión/multidifusión usando un protocolo seguro de transporte en tiempo real**

(30) Prioridad:

21.09.2004 US 946961

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.03.2013

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 MOREHOUSE DRIVE
SAN DIEGO, CALIFORNIA 92121, US

(72) Inventor/es:

HSU, RAYMOND, TAH-SHENG y
WANG, JUN

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Determinación de una clave de cifrado de sesión durante una sesión de servicio de difusión/multidifusión usando un protocolo seguro de transporte en tiempo real

Antecedentes

Campo

La presente invención versa, en general, acerca de las comunicaciones inalámbricas y, más específicamente, acerca de la determinación de una clave segura de cifrado de sesión de transporte en tiempo real.

Antecedentes

Servicios de difusión o multidifusión se refiere a un sistema de comunicaciones usado para transmitir información desde un transmisor a múltiples receptores o usuarios. Ejemplos de sistemas de difusión o de comunicaciones punto a multipunto incluyen sistemas de expedición, tales como los usados por la policía, empresas de transporte por carretera o empresas de taxis, en las que un expedidor central difunde señales a uno o más vehículos. Una señal difundida puede ser dirigida a un vehículo específico o a todos los vehículos simultáneamente.

A medida que las redes móviles de radio, tales como las redes de telefonía celular, se han vuelto omnipresentes, los clientes han empezado a desear la recepción de radiodifusión multimedia, tal como vídeo y teleconferencia, usando protocolo de Internet (IP) por un enlace de comunicaciones inalámbricas. Por ejemplo, los clientes desean poder recibir vídeo de difusión en continuo, tal como emisiones de televisión, en su teléfono móvil u otro dispositivo portátil de comunicaciones inalámbricas. Otros ejemplos del tipo de datos que los clientes desean recibir con su dispositivo de comunicaciones inalámbricas incluyen radiodifusión multimedia y acceso a Internet.

Un canal típico de comunicaciones inalámbricas tiene un ancho de banda limitado y, en ocasiones, puede experimentar tasas de error significativas. Se han desarrollado diversas técnicas para transmitir mensajes según servicios de difusión y multidifusión (BCMCS). En general, estas técnicas incluyen dar forma a los mensajes creando paquetes con una cabecera que incluye información sobre los datos dentro del paquete. En las comunicaciones BCMCS, un proveedor de contenidos o un servidor de contenidos generan un flujo de datos que ha de difundirse a múltiples receptores o usuarios. El flujo de datos se convierte en paquetes de datos para componer un flujo de datos de BCMCS que es luego radiodifundido simultáneamente a múltiples dispositivos de comunicaciones.

Puede desearse que solo algunos WCD reciban flujos de BCMCS. Por ejemplo, un proveedor de contenidos puede desear que solo los WCD autorizados, como los que han pagado una tarifa de abono, puedan recibir el contenido. Dado que los flujos de BCMCS son difundidos por el aire y, por lo tanto, pueden ser recibidos por WCD tanto autorizados como no autorizados, se han desarrollado diferentes formar de asegurar los flujos de BCMCS.

Un protocolo para la transmisión segura de datos, incluyendo flujos de BCMCS, que ha sido desarrollado por el Proyecto Dos de la Asociación de Tercera Generación (3GPP2) se denomina Protocolo Seguro de Transporte en Tiempo Real (SRTP). En una emisión de SRTP, las claves de sesión que se usan para descifrar el flujo de BCMCS se generan a partir de una clave maestra, el índice de paquete (PI) y otros materiales de generación de claves. Dado que la clave de sesión se usa para descifrar el flujo de emisión, periódicamente durante una emisión de SRTP la clave de sesión se actualiza a un nuevo valor para evitar que WCD no autorizados reciban el contenido. La actualización de la clave de sesión requiere coordinación entre el proveedor del sistema de emisión y los WCD autorizados. Además, es deseable aumentar la aleatoriedad de la clave actualizada de sesión, dificultando con ello que un WCD no autorizado determine cuál es la nueva sesión.

Por lo tanto, existe la necesidad en la técnica de mejorar la actualización de la clave de sesión en una sesión de BCMCS de SRTP.

La presente invención versa acerca de un procedimiento y un aparato para determinar una clave actualizada de sesión según se define en las reivindicaciones adjuntas.

Las realizaciones dadas a conocer en el presente documento abordan las necesidades enunciadas en lo que antecede de mejora de actualización de la clave de sesión en una sesión de BCMCS de SRTP. Se describen un procedimiento y un aparato para determinar una clave de cifrado de sesión durante un servicio de difusión/multidifusión (BCMCS) usando el Protocolo Seguro de Transporte en Tiempo Real (SRTP). El procedimiento y el aparato incluyen la recepción de un número de secuencia durante una sesión. Durante la sesión se calcula un índice de paquetes usando el número de secuencia y un contador de bucle que se ha fijado en un valor predeterminado. Se determina una clave actualizada de sesión usando una clave maestra y el índice de paquetes. La determinación de la clave actualizada de sesión puede llevarse a cabo en un servidor de contenidos, en una estación móvil o en ambos.

Otro aspecto es que una clave inicial de sesión puede encontrarse calculando el índice de paquetes usando el número de secuencia y un contador de bucle que ha sido fijado en un valor predeterminado no cero. Se determina

una clave inicial de sesión usando la clave maestra y el índice de paquetes. La determinación de la clave inicial de sesión puede llevarse a cabo en un servidor de contenidos, en una estación móvil o en ambos.

La determinación de una clave de sesión puede ser llevada a cabo por un motor de claves de cifrado. El motor de claves de cifrado puede incluir, por ejemplo, un receptor que reciba un número de secuencia durante una sesión. El motor de claves de cifrado puede incluir también un procesador que calcule un valor de índice de paquetes durante la sesión usando el número de secuencia y un contador de bucle que haya sido fijado en un valor predeterminado. El procesador determina una clave actualizada de cifrado de sesión usando una clave maestra y el índice de paquetes. En otro aspecto, el motor de claves de cifrado calcula un valor de índice de paquetes al inicio de una sesión usando el número de secuencia y un contador de bucle que ha sido fijado en un valor predeterminado no cero. El procesador determina una clave inicial de cifrado de sesión usando una clave maestra y el índice de paquetes.

Otras características y ventajas de la presente invención deberían ser evidentes a partir de la siguiente descripción de realizaciones ejemplares, que ilustran, a título de ejemplo, aspectos de la invención.

Breve descripción de los dibujos

La Figura 1 muestra un sistema de comunicaciones construido según la presente invención.

La Figura 2 es un diagrama de bloques que ilustra una arquitectura ejemplar para la transmisión de BCMCS usando SRTP en una red inalámbrica.

La Figura 3 es un diagrama de bloques que ilustra la derivación de una clave de sesión.

La Figura 4 es un diagrama de bloques de un motor ejemplar de claves de cifrado.

La Figura 5 es un diagrama de flujo que ilustra una técnica ejemplar para determinar una clave de cifrado de sesión.

La Figura 6 es un diagrama de bloques de un dispositivo de comunicaciones inalámbricas, o MS, construido según una realización ejemplar de la presente invención.

Descripción detallada

La palabra “ejemplar” se usa en el presente documento con el significado de “servir de ejemplo, modelo o ilustración”. No debe interpretarse de cualquier realización que sea descrita en el presente documento como “ejemplar” que sea preferida o ventajosa con respecto a otras realizaciones.

La Figura 1 muestra un sistema 100 de comunicaciones construido según la presente invención. El sistema 100 de comunicaciones incluye infraestructura 101, múltiples dispositivos 104 y 105 de comunicaciones inalámbricas (WCD) y dispositivos 122 y 124 de comunicaciones por vía terrestre. Los WCD también se denominan móviles o estaciones móviles. En general, los WCD pueden ser móviles o fijos.

La infraestructura 101 también incluye otros componentes, tales como estaciones base 102, controladores 106 de estaciones base, centros 108 de conmutación móvil, una red 120 de conmutación y similares. En una realización la estación base 102 está integrada con el controlador 106 de estaciones base, y en otras realizaciones la estación base 102 y el controlador 106 de estaciones base son componentes separados. Pueden usarse tipos diferentes de redes 120 de conmutación para encaminar las señales en el sistema 100 de comunicaciones; por ejemplo, la red 120 de conmutación puede ser la red de telefonía pública conmutada (PSTN).

La expresión “enlace directo” se refiere al trayecto de la señal desde la infraestructura 101 a un WCD 104 y 105, y la expresión “enlace inverso” se refiere al trayecto de la señal desde un WCD a la infraestructura. Tal como se muestra en la Figura 1, los WCD 104 y 105 reciben señales 132 y 136 por el enlace directo y transmiten señales 134 y 138 por el enlace inverso. En general, las señales transmitidas desde un WCD están concebidas para su recepción en otro dispositivo de comunicaciones, tal como otra unidad remota o un dispositivo 122 y 124 de comunicaciones por vía terrestre, y son encaminadas a través de la red 120 de conmutación. Por ejemplo, si la señal 134 transmitida desde un WCD 104 remitente está concebida para ser recibida por un WCD 105 de destino, la señal es encaminada a través de la infraestructura 101 y se transmite una señal 136 por el enlace directo al WCD 105 de destino. Normalmente, un dispositivo de comunicaciones, tal como un WCD o un dispositivo de comunicaciones por vía terrestre, puede ser a la vez remitente y destinatario de las señales.

Ejemplos de WCD 104 y 105 incluyen teléfonos móviles, ordenadores personales con prestaciones de comunicación inalámbrica y agendas electrónicas (PDA) y otros dispositivos de comunicaciones inalámbricas. El sistema 100 de comunicaciones puede estar diseñado para dar soporte a uno o más estándares inalámbricos. Por ejemplo, los estándares pueden incluir estándares denominados TIA/EIA-95-B (IS-95), TIA/EIA-98-C (IS-98), cdma2000, CDMA de banda ancha (WCDMA) y otros.

También pueden transmitirse señales desde la infraestructura 101 a los WCD 104 y 105. Por ejemplo, puede emitirse a WCD autorizados una señal desde un servidor de contenidos en la infraestructura.

El Proyecto Dos de la Asociación de Tercera Generación (3GPP2) ha publicado una especificación, 3GPP2 X.S0022, que define requisitos para el soporte del servicio de difusión-multidifusión (BCMCS) para redes cdma2000. La especificación indica que el operador de la red puede controlar el cifrado del contenido de un flujo de BCMCS para impedir la recepción no autorizada. Una técnica de cifrado de ese tipo es el Protocolo Seguro de Transporte en Tiempo Real (SRTP).

El SRTP se describe en una Petición de Comentarios (RFC) 3711 del Grupo de Trabajo sobre Redes. Hay disponible un ejemplar de la RFC 3711 en la dirección de Internet de ftp.rfc-editor.org/in-notes/rfc3711.txt. La RFC 3711 describe que cada flujo de SRTP requiere un remitente y un destinatario para mantener la información criptográfica de estado, denominada contexto criptográfico.

El SRTP usa dos tipos de claves: una clave de sesión y una clave maestra. La clave de sesión se usa directamente en una transformación criptográfica, tal como el cifrado y el descifrado. La clave maestra es un número aleatorio que se usa en la derivación de la clave de sesión. Se deriva una clave inicial de sesión al comienzo de una emisión que use SRTP, y luego se renuevan o actualizan las claves de sesión subsiguientes según una tasa de derivación de claves (KDR). La KDR se fija en un valor correspondiente a un número de paquetes que se difunden con una clave particular de sesión antes de que se renueve o actualice la clave de sesión. En otras palabras, se deriva una clave inicial de sesión y luego, periódicamente durante toda la sesión, la clave de sesión usada para cifrar los datos se actualiza o se cambia para evitar el acceso no autorizado al contenido emitido.

La Figura 2 es un diagrama de bloques que ilustra una arquitectura ejemplar para la transmisión de BCMCS usando SRTP en una red inalámbrica. Tal como se muestra en la Figura 2, una estación móvil (MS) 202 puede obtener del controlador 204 de BSMCS parámetros relacionados con la seguridad mediante un mecanismo fuera de la banda. La MS 202 recibe entonces de un servidor 206 de contenidos (CS) un contenido de programa que ha sido cifrado usando una clave de sesión. Usando la debida clave de sesión, la MS 202 puede descifrar el contenido. Puede hacer falta la coordinación entre el CS 206 y el controlador 204 de BCMCS para dar soporte a un cifrado de capa superior.

La clave maestra es compartida entre el CS 206 y un grupo de MS 202 que están autorizadas para recibir un contenido específico desde el CS 206. Según se ha hecho notar, se usa para clave maestra para derivar la clave de sesión.

La Figura 3 es un diagrama de bloques que ilustra la derivación de una clave de sesión. Tal como se muestra en la Figura 3, una función 302 de derivación de claves recibe la clave maestra 304, una sal maestra 306 y un índice 308 de paquetes (PI). La función 302 de derivación de claves usa estas entradas para derivar una clave 310 de sesión. La sal maestra 306 es un número aleatorio que es conocido por el servidor 206 de contenidos (Figura 2) y la MS 202.

El PI 308 se calcula por medio de la ecuación

$$PI = 2^{16} * ROC + SEC \qquad \text{Ec. 1}$$

en la que SEC es el número de secuencia del protocolo de transporte en tiempo real (RTP), que la RFC 3711 define que es un número de 16 bits. ROC es el contador de bucle, que cuenta el número de veces que el número secuencia de RTP da la vuelta. La RFC 3711 define que el ROC es un número de 32 bits. Se incrementa SEC en uno para cada paquete de RTP enviado. Normalmente, la clave inicial de sesión se deriva usando un valor inicial de ROC que se fija en cero, y un valor inicial de SEC que puede ser un número aleatorio. En una realización, el valor inicial de ROC puede fijarse en un valor predeterminado no cero. Por ejemplo, puede compartirse un valor inicial no cero de ROC entre el CS 206 y un grupo de MS 202 que están autorizadas para recibir un contenido específico desde el servidor de contenidos. O puede proporcionarse desde el controlador de BCMCS un valor inicial no cero de ROC por medio de un mecanismo fuera de banda antes del inicio de una emisión.

Las claves de sesión subsiguientes son renovadas o actualizadas según una tasa de derivación de claves (KDR). La KDR se expresa en términos del número de incremento de SEC. Por ejemplo, si KDR es 100, las claves de sesión deben ser refrescadas a la tasa de que el CS envíe 100 paquetes de RTP. Es preciso que el CS y las MS conozcan la KDR para sincronizar la generación de las claves de sesión subsiguientes. Con base en la KDR y la SEC recibida, la MS sabe si es preciso renovar o no las claves de sesión.

Tal como se describe en la RFC 3711, dado que el ROC tiene una longitud de 32 bits y la SEC tiene una longitud de 16 bits, el número máximo de paquetes pertenecientes a un flujo de SRTP dado que puede ser asegurado con la misma clave de sesión es de 2^{48} paquetes. Después de que se haya enviado ese número de maquetes de SRTP con una clave dada, ya sea una clave maestra o una clave de sesión, el CS no debe enviar ningún paquete más con esa clave.

A continuación se describe una técnica para determinar una clave de cifrado de sesión. Durante una sesión, se recibe un número de secuencia con cada paquete. Se determina un índice de paquetes usando el número de

secuencia recibido y el valor del ROC, que ha sido fijado en un valor predeterminado, por ejemplo un valor no cero o un valor nulo. Se determina entonces la clave de sesión usando una clave maestra y el índice de paquetes.

Esta técnica puede usarse para determinar una clave inicial de sesión al inicio de una emisión. Por ejemplo, el CS y MS autorizadas pueden compartir un valor predeterminado no cero para ROC que se usa para determinar la clave inicial de sesión. Asimismo, un controlador de BCMCS puede proporcionar al CS y a las MS autorizadas el valor predeterminado no cero de ROC; por ejemplo, por medio de un mecanismo fuera de banda. Durante la sesión, a medida que se reciben paquetes, el valor del ROC cambiará cuando el número de secuencia de RTP dé la vuelta.

También puede usarse esta técnica durante una secuencia de renovación de la clave maestra. Por ejemplo, antes de que expire la clave maestra actual, la MS puede obtener del controlador de BCSMCS una nueva clave maestra, un valor predeterminado para ROC, y un nuevo número de secuencia inicial de RTP. El controlador de BCSMCS puede coordinarse con el CS para la nueva clave maestro, el valor predeterminado de ROC y el número de secuencia inicial de RTP. También se puede transmitir tanto a la MS como al CS el momento en que se usará la nueva clave maestra. Cuando llegue ese momento, el CS calcula el índice de paquetes usando el valor predeterminado de ROC y el nuevo número de secuencia inicial de RTP; luego, el CS deriva las claves de sesión usando la nueva clave maestra y el índice de paquetes. Cuando la MS recibe el paquete con el nuevo número de secuencia inicial de RTP, calcula el índice de paquetes con el valor predeterminado de ROC y luego deriva las claves de sesión usando la nueva clave maestra.

En otro aspecto, pueden mantenerse listas correspondientes de valores predeterminados para ROC en el CS y las MS autorizadas. Luego, en momentos deseados durante la sesión, puede usarse un nuevo valor predeterminado para ROC. Por ejemplo, cuando el CS y las MS autorizadas reciben la clave maestra, también pueden recibir una lista de valores predeterminados para ROC. Luego, durante la sesión el CS y las MS usarán un nuevo valor predeterminado para ROC. Hay muchas maneras de coordinar cuándo el CS y las MS usarían un nuevo valor predeterminado para ROC. Por ejemplo, el CS y las MS podrían usar un nuevo valor predeterminado para ROC a intervalos de tiempo prefijados, después de que se haya recibido un número prefijado de paquetes, siempre que se determine una nueva clave de sesión, cuando se ordene mediante una señal fuera de banda, cuando se incluya una orden dentro de la propia emisión y similares.

La Figura 4 es un diagrama de bloques de un motor ejemplar 402 de claves de cifrado. La determinación de una clave de sesión puede llevarse a cabo mediante un motor 402 de claves de cifrado que incluye un receptor 404 y un procesador 406. En una realización, el receptor 404 está configurado para recibir, por ejemplo desde un controlador de BSMCS, una clave maestra, al menos un valor predeterminado de ROC y un número de secuencia inicial antes del inicio de una sesión. El receptor también puede estar configurado para recibir números de secuencia que estén incluidos dentro de los paquetes durante una sesión. El procesador 406 puede estar configurado para calcular un índice de paquetes usando el número de secuencia y un valor de ROC. El valor de ROC puede ser uno de los valores predeterminados recibidos antes del inicio de la sesión, o algún otro valor predeterminado que esté coordinado entre un CS y una MS autorizada. El valor de ROC cambiará durante una sesión a medida que se reciban paquetes y el número de secuencia dé la vuelta. El procesador 404 determina entonces la clave de cifrado usando la clave maestra y el índice de paquetes.

La Figura 5 es un diagrama de flujo que ilustra una técnica ejemplar para determinar una clave de cifrado de sesión. El flujo comienza en el bloque 502, en el que se recibe un número de secuencia. Por ejemplo, el número de secuencia podría recibirse de un controlador de BCMCS. El flujo prosigue al bloque 504, en el que se calcula el índice de paquetes usando el número de secuencia y un contador de bucle que tenga un valor predeterminado. Por ejemplo, el valor del contador de bucle (ROC) puede tener un valor predeterminado, o el valor de ROC puede ser uno de al menos un valor predeterminado recibido antes del inicio de la sesión, o algún otro valor predeterminado que esté coordinado entre un CS y una MS autorizada. El valor de ROC cambiará durante una sesión a medida que se reciban paquetes y el número de secuencia dé la vuelta. El flujo prosigue entonces al bloque 506, en el que se determina entonces una clave de cifrado de sesión usando una clave maestra y el índice de paquetes.

MS ejemplar

La Figura 6 es un diagrama de bloques de un dispositivo de comunicaciones inalámbricas, o MS, construido según una realización ejemplar de la presente invención. El dispositivo 602 de comunicaciones incluye una interfaz 606 de red, un procesador 608 de señales digitales (DSP), un procesador anfitrión 610, un dispositivo 612 de memoria, un producto 614 de programa y una interfaz 616 de usuario.

Señales procedentes de la infraestructura, tales como flujos de BCMCS, son recibidas por la interfaz 606 de red y enviadas al procesador anfitrión 610. El procesador anfitrión 610 recibe las señales y, dependiendo del contenido de la señal, responde con acciones apropiadas. Por ejemplo, el procesador anfitrión 610 puede determinar que la señal incluye una clave maestra y al menos un valor predeterminado de ROC, y el procesador anfitrión 610 puede guardar estos valores, por ejemplo en el dispositivo 612 de memoria, para su uso posterior en la determinación de una clave de cifrado de sesión. El procesador anfitrión 610 también puede determinar que la señal forma parte de un paquete de BCMCS de SRTP y puede extraer del paquete un valor de número de secuencia. El procesador anfitrión puede entonces determinar una clave de cifrado de sesión para descifrar el contenido del propio paquete de datos recibido,

o puede encaminar el paquete de datos recibido al DSP 608, en el que se determina la clave de cifrado de sesión. El procesador anfitrión 610 también puede recibir paquetes de datos del DSP 608 y encaminar estos paquetes a la interfaz 606 de red para su transmisión a la infraestructura.

Asimismo, las señales recibidas desde la interfaz 606 de red pueden ser enviadas al DSP 608. El DSP 608 puede recibir las señales y, dependiendo del contenido de la señal, responde con acciones apropiadas. Por ejemplo, el DSP 608 puede determinar que la señal incluye una clave maestra y al menos un valor predeterminado de ROC, y el DSP 608 puede guardar estos valores, por ejemplo en el dispositivo 612 de memoria, para su uso posterior en la determinación de una clave de cifrado de sesión. El DSP 608 también puede determinar que la señal forma parte de un paquete de BCMCS de SRTP y puede extraer del paquete un valor de número de secuencia. El DSP 608 puede entonces determinar una clave de cifrado de sesión para descifrar el contenido del propio paquete de datos recibido, o puede encaminar el paquete de datos recibido al procesador anfitrión 610, en el que se determina la clave de cifrado de sesión. El DSP 608 también puede recibir paquetes de datos del procesador anfitrión 610 y encaminar estos paquetes a la interfaz 606 de red para su transmisión a la infraestructura.

En una realización, la interfaz 606 de red puede ser un transceptor y una antena para comunicarse con la infraestructura por un canal inalámbrico. En otra realización, la interfaz 606 de red puede ser una tarjeta de interfaz de red usada para comunicarse con la infraestructura por líneas terrestres.

Tanto el procesador anfitrión 610 como el DSP 608 están conectados con un dispositivo 612 de memoria. El dispositivo 612 de memoria puede usarse para guardar datos durante la operación del WCD, así como para guardar código de programa que será ejecutado por el procesador anfitrión 610 o el DSP 608. Por ejemplo, pueden guardarse en el dispositivo 612 de memoria la clave maestra y al menos un valor predeterminado de ROC. Además, el procesador anfitrión, el DSP o ambos pueden operar bajo el control de instrucciones de programación que están guardados temporalmente en el dispositivo 612 de memoria. El procesador anfitrión y el DSP también pueden incluir memoria de almacenamiento de programas propios, así como almacenamiento para guardar la clave maestra y al menos un valor predeterminado de ROC. Cuando se ejecutan las instrucciones de programación, el procesador anfitrión 610 o el DSP 608 o ambos llevan a cabo sus funciones, tales como determinar una clave de cifrado de sesión. Pueden recibirse las etapas de programación de un producto 614 de programa. El producto 614 de programa puede guardar y transferir las etapas de programación a la memoria 612 para su ejecución por el procesador anfitrión, la CPU o ambos.

El producto 614 de programa puede ser chips semiconductores de memoria, tales como memoria RAM, memoria flash, memoria ROM, memoria EPROM, memoria EEPROM, registros, así como otros dispositivos de almacenamiento, tales como un disco duro, un disco extraíble, un CD-ROM o cualquier otra forma de medio de almacenamiento conocida en la técnica que pueda guardar instrucciones legibles por ordenador. Además, el producto 614 de programa puede ser el fichero fuente que incluye las etapas de programa que se recibe desde la red y se guarda en memoria y luego es ejecutado. De esta manera, las etapas de procesamiento necesarias para la operación según la invención pueden ser implementadas en el producto 614 de programa. En la Figura 6, se muestra al medio ejemplar de almacenamiento acoplado con el procesador anfitrión, de tal modo que el procesador anfitrión pueda leer información del medio de almacenamiento y escribir información en el mismo. Alternativamente, el medio de almacenamiento puede ser integral al procesador anfitrión.

La interfaz 616 de usuario está conectada tanto con el procesador anfitrión 610 como con el DSP 608. Por ejemplo, la interfaz de usuario puede incluir un teclado o teclas o botones especiales de función que se encaminan al procesador anfitrión 610 y que pueden ser usados por un usuario para solicitar una operación específica por parte del dispositivo remitente. La interfaz 616 de usuario puede incluir también un altavoz que esté conectado al DSP 610 y que se use para producir datos de audio para el usuario.

Los expertos en la técnica entenderán que la información y las señales pueden ser representadas usando cualquiera de varias tecnologías y técnicas diferentes. Por ejemplo, en toda la anterior descripción, los datos, las instrucciones, las órdenes, la información, las señales, los bits, los símbolos y los chips a los que se puede hacer referencia pueden ser representados por tensiones, corrientes, ondas electromagnéticas, campos o partículas magnéticos, campos o partículas ópticos o cualquier combinación de los mismos.

Los expertos en la técnica apreciarán, además, que diversos bloques lógicos ilustrativos, módulos, circuitos y etapas de algoritmo descritos en conexión con las realizaciones dadas a conocer en el presente documento pueden ser implementados como soporte físico electrónico, soporte lógico de ordenador o combinaciones de ambos. Para ilustrar claramente esta intercambiabilidad de soporte físico y soporte lógico, diversos componentes ilustrativos, bloques, módulos, circuitos y etapas han sido descritos en lo que antecede generalmente en términos de su funcionalidad. Que tal funcionalidad se implemente como soporte físico o soporte lógico depende de la aplicación particular y de limitaciones de diseño impuestas en el sistema en su conjunto. Los expertos en la técnica pueden implementar la funcionalidad descrita de varias maneras para cada aplicación particular, pero no debiera interpretarse que tales decisiones de implementación causen un alejamiento del alcance de la presente invención.

Los diversos bloques lógicos ilustrativos, módulos y circuitos descritos en relación con las realizaciones dadas a conocer en el presente documento pueden implementarse o realizarse con un procesador de uso general, un

procesador de señales digitales (DSP), un circuito integrado para aplicaciones específicas (ASIC), una matriz de puertas programables in situ (FPGA) u otro dispositivo lógico programable, puerta discreta o lógica de transistor, componentes de soporte físico discretos o cualquier combinación de los mismos diseñada para llevar a cabo las funciones descritas en el presente documento. Un procesador de uso general puede ser un microprocesador, pero, de forma alternativa, el procesador puede ser cualquier procesador convencional, controlador, microcontrolador o máquina de estado. Un procesador también puede ser implementado como una combinación de dispositivos de cálculo, por ejemplo una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores en conjunción con un núcleo de DSP o cualquier otra configuración de ese tipo.

Los procedimientos o las técnicas descritos en conexión con las realizaciones dadas a conocer en el presente documento pueden ser implementados directamente en soporte físico, en un módulo de soporte lógico ejecutado por un procesador o en una combinación de los dos. Un módulo de soporte lógico puede residir en la memoria RAM, en memoria flash, memoria ROM, memoria EPROM, memoria EEPROM, registros, un disco duro, un disco extraíble, un CD-ROM, almacenamiento en DVD o cualquier otra forma de medio de almacenamiento conocido en la técnica. Un medio de almacenamiento ejemplar está acoplado con el procesador de tal modo que el procesador pueda leer información del medio de almacenamiento y escribir información en el mismo. De forma alternativa, el medio de almacenamiento puede ser integral al procesador. El procesador y el medio de almacenamiento pueden residir en un ASIC. El ASIC puede residir en un terminal de usuario. De forma alternativa, el procesador y el medio de almacenamiento pueden residir como componentes discretos en un terminal de usuario.

Se proporciona la anterior descripción de las realizaciones dadas a conocer para permitir que cualquier persona experta en la técnica realice o use la presente invención. Diversas modificaciones de estas realizaciones resultarán inmediatamente evidentes para los expertos en la técnica, y los principios genéricos definidos en el presente documento pueden ser aplicados a otras realizaciones sin apartarse del alcance de la invención. Así, no se pretende que la presente invención esté limitada a las realizaciones mostradas en el presente documento, sino que debe otorgársele el alcance más amplio coherente con los principios y características novedosas dados a conocer en el presente documento.

REIVINDICACIONES

1. Un procedimiento de determinación de claves actualizadas de cifrado de sesión **caracterizado** el procedimiento **porque** comprende:

proporcionar una lista de valores predeterminados;
recibir números de secuencia durante una sesión;
determinar claves actualizadas de cifrado de sesión usando una clave maestra y valores de índices de paquete calculados usando los números de secuencia recibidos e incrementando los valores de contador de un contador de bucle que habían sido fijados en un valor predeterminado proveniente de la lista; y, en momentos deseados,
restablecer el valor creciente de contador del contador de bucle a un siguiente valor predeterminado proveniente de la lista y seguir determinando valores actualizados de sesión usando la clave maestra y valores de índices de paquetes calculados usando los números de secuencia recibidos e incrementando los valores de contador del contador de bucle que han sido restablecidos al siguiente valor predeterminado proveniente de la lista.

2. Un procedimiento según se define en la Reivindicación 1 en el que la sesión es una sesión SRTP.

3. Un procedimiento según se define en la Reivindicación 1 en el que las claves determinadas actualizadas de cifrado de sesión se usan para cifrar el contenido proporcionado por un servidor de contenidos.

4. Un procedimiento según se define en la Reivindicación 1 en el que la clave maestra se recibe de un controlador BCMCS.

5. Un procedimiento según se define en la Reivindicación 1 en el que la determinación de las claves actualizadas de cifrado de sesión se lleva a cabo en un servidor de contenidos.

6. Un procedimiento según se define en la Reivindicación 1 en el que la determinación de las claves actualizadas de cifrado de sesión se lleva a cabo en una estación móvil.

7. Un procedimiento según se define en la Reivindicación 6 en el que las claves actualizadas de cifrado de sesión se usan para descifrar el contenido proporcionado por un servidor de contenidos.

8. Un procedimiento según se define en la Reivindicación 1 en el que los números de secuencia se reciben en paquetes de datos de sesión.

9. Un procedimiento según se define en la Reivindicación 1 en el que los momentos deseados se basan en un número preestablecido de paquetes recibidos.

10. Un procedimiento según se define en la Reivindicación 1 en el que los momentos deseados se basan en intervalos de tiempo preestablecidos.

11. Un procedimiento según se define en la Reivindicación 1 en el que cada uno de los valores predeterminados de la lista tiene un valor no cero.

12. Un aparato (402) **caracterizado porque** comprende:

un medio para recibir (404) números de secuencia durante una sesión;
un medio para determinar (406) claves actualizadas de cifrado de sesión usando una clave maestra y valores de índices de paquete calculados usando los números de secuencia recibidos e incrementando los valores de contador de un contador de bucle que habían sido fijados en un valor predeterminado proveniente de una lista de valores predeterminados; y
un medio para restablecer (406), en momentos deseados, el valor creciente de contador del contador de bucle a un siguiente valor predeterminado proveniente de la lista y seguir determinando valores actualizados de sesión usando la clave maestra y valores de índices de paquetes calculados usando los números de secuencia recibidos e incrementando los valores de contador del contador de bucle que han sido restablecidos al siguiente valor predeterminado proveniente de la lista.

13. El aparato de la Reivindicación 12 que, además, comprende:

medios para proporcionar la lista de valores predeterminados.

14. Un aparato según se define en las Reivindicaciones 12 o 13 en el que la sesión es una sesión SRTP.

15. Un aparato según se define en las Reivindicaciones 12 o 13 en el que el valor predeterminado es un valor no cero.

16. Un aparato según se define en las Reivindicaciones 12 o 13 en el que las claves determinadas de cifrado de sesión se usan para cifrar el contenido proporcionado por un servidor de contenidos.

17. Un aparato según se define en la Reivindicación 16 en el que la clave maestra se recibe de un controlador BCMCS.

18. Un aparato según se define en las Reivindicaciones 12 o 13 en el que el medio para determinar las claves actualizadas de cifrado de sesión está situado en un servidor de contenidos.

19. Un aparato según se define en las Reivindicaciones 12 o 13 en el que el medio para determinar las claves actualizadas de cifrado de sesión está situado en una estación móvil.

20. Un aparato según se define en la Reivindicación 19 en el que las claves determinadas actualizadas de cifrado de sesión se usan para descifrar el contenido proporcionado por un servidor de contenidos.

21. Un aparato según se define en las Reivindicaciones 12 o 13 en el que los números de secuencia se reciben en paquetes de datos de sesión.

22. Un aparato según se define en las Reivindicaciones 12 o 13 en el que los momentos deseados se basan en un número preestablecido de paquetes recibidos.

23. Un aparato según se define en las Reivindicaciones 12 o 13 en el que los momentos deseados se basan en intervalos de tiempo preestablecidos.

24. Un aparato según se define en las Reivindicaciones 12 o 13 en el que cada uno de los valores predeterminados de la lista tiene un valor no cero.

25. Un aparato de cualquiera de las reivindicaciones 12-24 en el que el aparato es un motor de claves de cifrado y en el que, además:

el medio de recepción comprende un receptor; y
el medio de determinación y el medio de restablecimiento comprenden un procesador;
y en el que el aparato comprende, además, una memoria configurada para guardar una lista de valores predeterminados.

26. Un medio legible por ordenador que implementa un procedimiento de determinación de una clave actualizada de cifrado de sesión **caracterizado porque** comprende el procedimiento de cualquiera de las reivindicaciones 1-11.

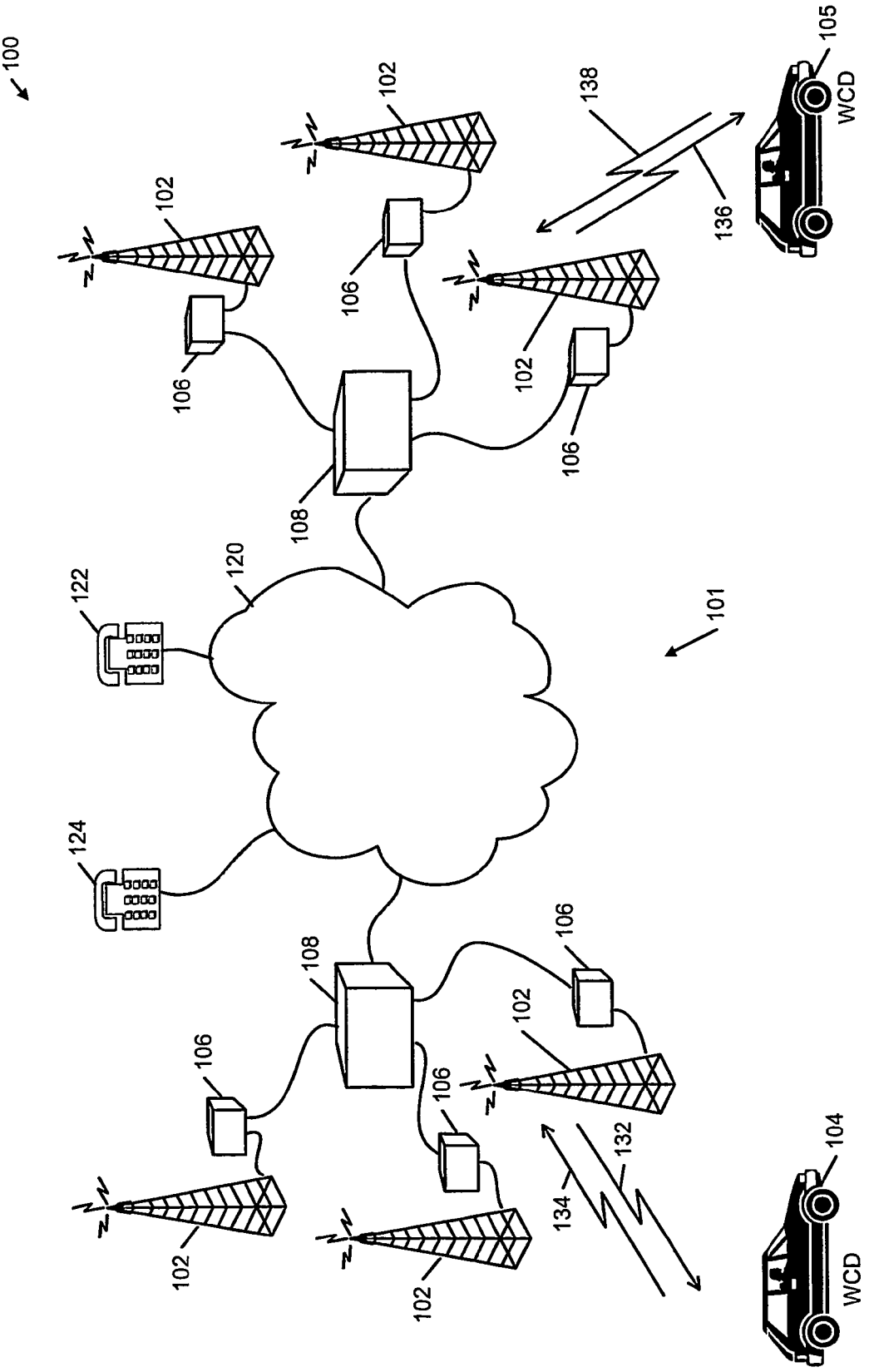

FIGURA 1

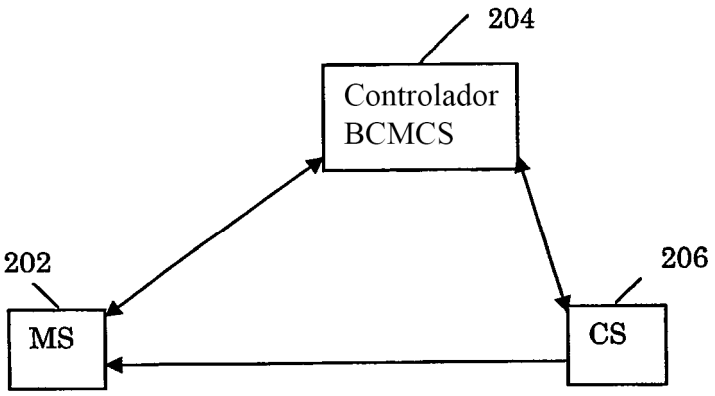

FIG.2

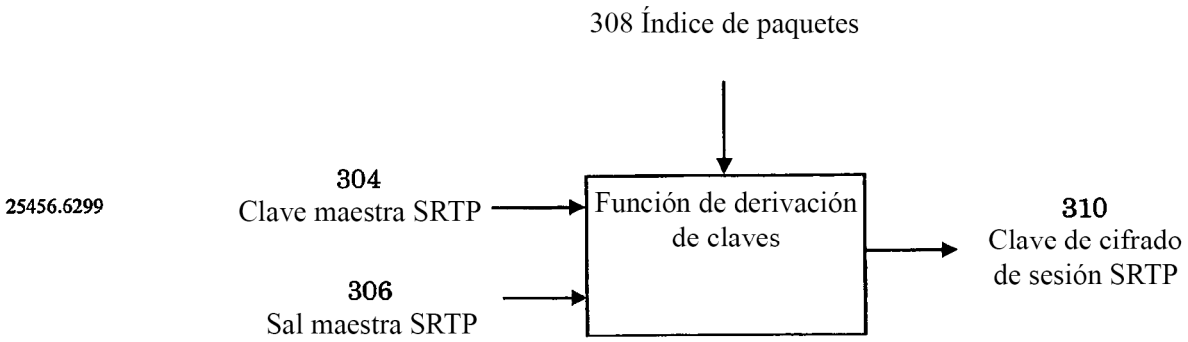
308 Índice de paquetes
25456.6299
304
Clave maestra SRTP
306
Sal maestra SRTP
Función de derivación de claves
310
Clave de cifrado de sesión SRTP

FIG. 3

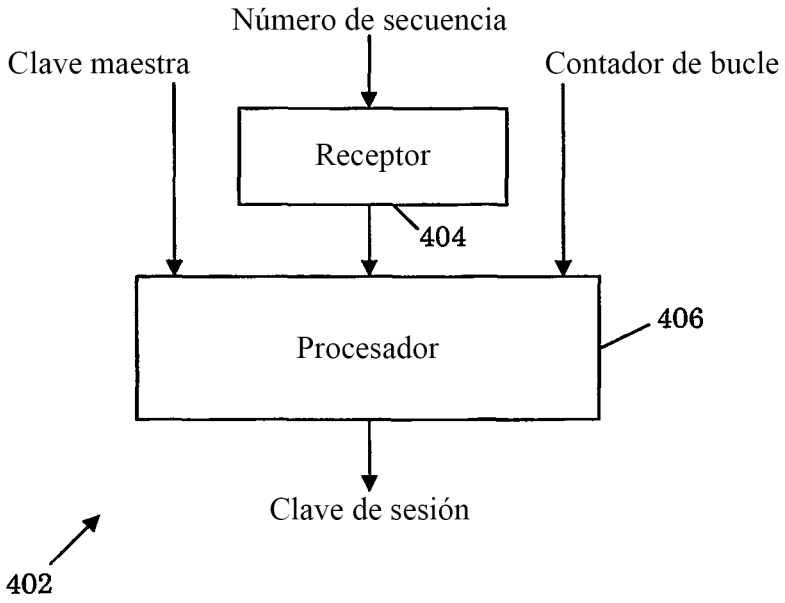
Número de secuencia
Clave maestra
Contador de bucle
Receptor
404
Procesador
406
Clave de sesión
402

FIG. 4

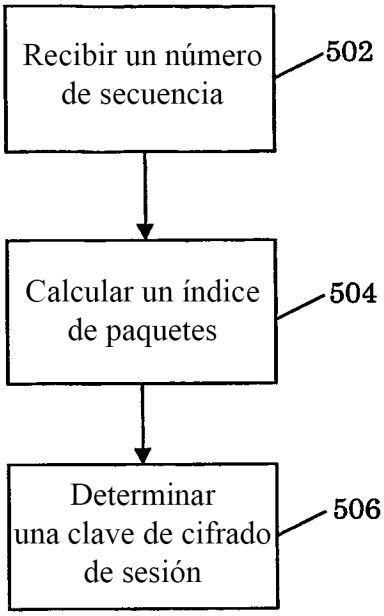
Recibir un número de secuencia
502
Calcular un índice de paquetes
504
Determinar una clave de cifrado de sesión
506

Figura 5

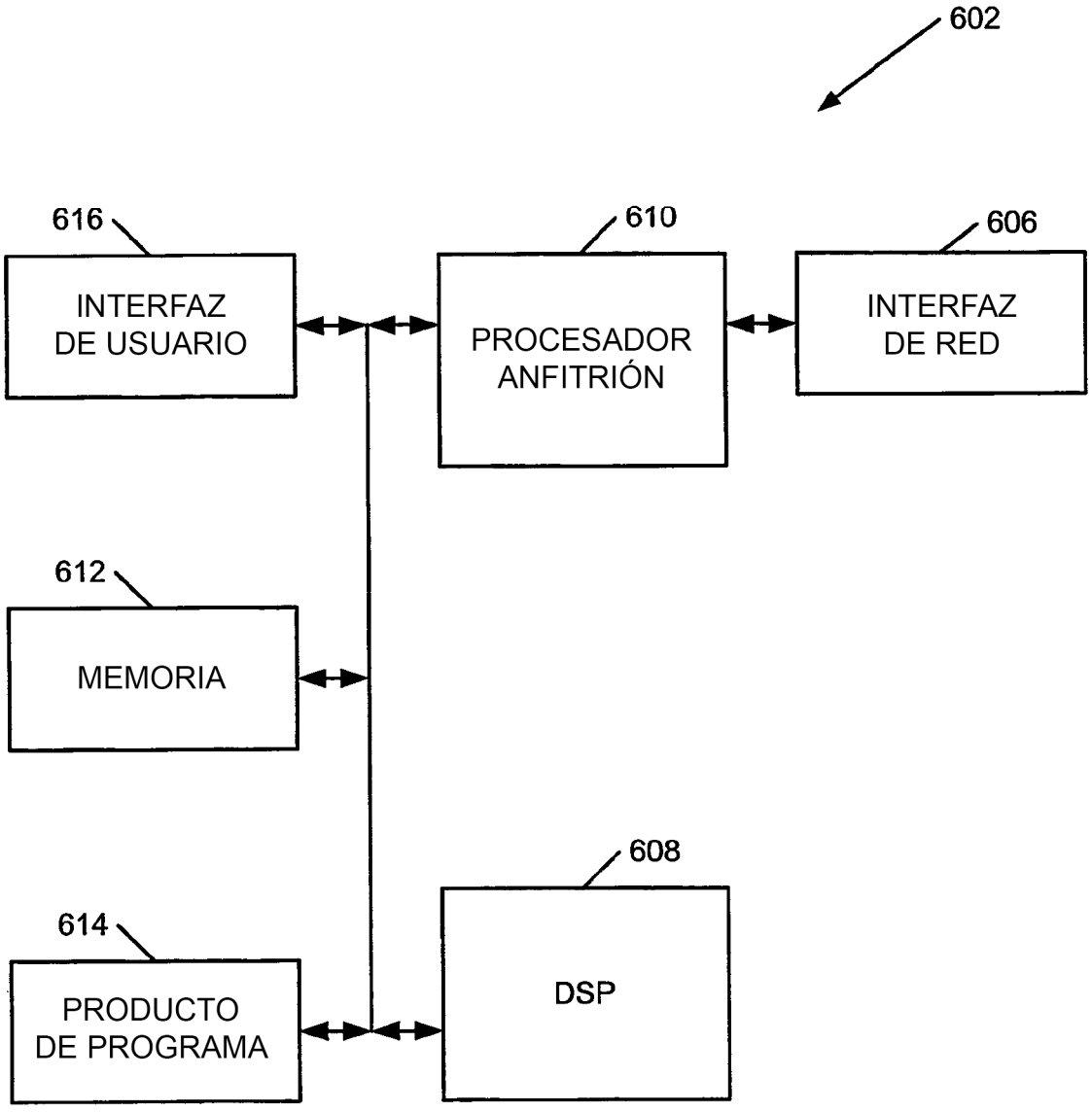
602
616
INTERFAZ DE USUARIO
610
PROCESADOR ANFITRIÓN
606
INTERFAZ DE RED
612
MEMORIA
608
DSP
614
PRODUCTO DE PROGRAMA

FIGURA 6