(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 774 487**

(51) Int. CI.:

G06F 21/54 (2013.01)
G06F 21/57 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.11.2016 PCT/EP2016/077932**

(87) Fecha y número de publicación internacional: **26.05.2017 WO17085159**

(96) Fecha de presentación y número de la solicitud europea: **17.11.2016 E 16797889 (9)**

(97) Fecha y número de publicación de la concesión europea: **08.01.2020 EP 3378005**

(54) Título: **Método para verificar la integridad de ejecución de una aplicación en un dispositivo de destino**

(30) Prioridad:

19.11.2015 EP 15195379

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.07.2020

(73) Titular/es:

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

(72) Inventor/es:

WYSEUR, BRECHT

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método para verificar la integridad de ejecución de una aplicación en un dispositivo de destino

Introducción

[0001] La presente invención se refiere al campo de la verificación de *software*, en particular para verificar si se puede demostrar la integridad en tiempo de ejecución de una aplicación de *software*.

Estado de la técnica

[0002] La atestación remota es un método para detectar cambios en el ordenador del usuario (o en cualquier *software* incrustado en un dispositivo) por parte de partes autorizadas. Por ejemplo, los centros de confianza pueden identificar cambios no autorizados en el *software*, incluyendo los usuarios que alteran su *software* para eludir las medidas tecnológicas de protección. El dispositivo de destino genera un certificado (una atestación) que hace una declaración sobre la ejecución del *software* y/o la plataforma de ejecución. El dispositivo de destino puede presentar este certificado a una parte remota para mostrar que el *software* sin modificaciones se está ejecutando actualmente.

[0003] La atestación remota puede combinarse con el cifrado de clave pública para que la información enviada solo pueda ser leída por los programas que habían presentado y solicitado la atestación, y no por un tercero no autorizado.

[0004] El método de verificación se basa en la transmisión, por un centro de verificación, de una puesta a prueba o desafío al dispositivo de destino. El *software* utiliza este desafío para producir un resultado, que depende del código del *software* y de la información del tiempo de ejecución y del desafío. El resultado luego se transmite al centro de verificación para su verificación.

[0005] La clave para verificar el resultado es un conocimiento preciso del *software* del dispositivo de destino para producir un resultado de referencia para la comparación.

Breve descripción de la invención

[0006] Un aspecto de la presente invención es proponer un método y un sistema para verificar el *software* incorporado en un dispositivo de destino. En el marco de la presente descripción, se propone un método para verificar la integridad de ejecución de una aplicación en un dispositivo de destino mediante la producción de una firma de aplicación a partir de la información de la aplicación en tiempo de ejecución, donde dicha firma se utiliza para verificar la integridad de ejecución de la aplicación mediante un servidor de verificación, donde dicha aplicación comprende un conjunto de bloques, cada bloque que produce un resumen o *digest*, produciendo así un conjunto de resúmenes relacionados con el conjunto de bloques, que comprende los pasos de:

- recepción, por el dispositivo de destino, de un mensaje que comprende un desafío y una primera función, donde dicha primera función define un método de agregación, donde dicho desafío define una instrucción de agregación,
- determinación, para cada bloque, del resumen correspondiente para dicho bloque,
- agregación de los resúmenes de los bloques según el método de agregación de la primera función y el desafío para producir una atestación relacionada con la aplicación,
- envío de la atestación al servidor de verificación,
- aplicación de una segunda función a la atestación por el servidor de verificación, donde dicha segunda función deshace el efecto del desafío, produciendo así una firma de aplicación independiente del desafío,
- verificación de la integridad de ejecución de la aplicación al comparar la firma de la aplicación producida con una firma de referencia.

Breve resumen de las figuras

[0007] La siguiente Descripción detallada se comprenderá mejor gracias a las figuras adjuntas, en las que

- La Figura 1 ilustra el sistema que comprende una cabecera y un dispositivo de destino, así como los pasos para verificar una aplicación,
- La figura 2 ilustra la generación de la atestación,
- La Figura 3 ilustra la verificación de la atestación,
- La figura 4 ilustra el dispositivo de destino.

Descripción detallada

[0008] Los esquemas de atestación son esquemas en los que un entorno o aplicación en tiempo de ejecución produce una prueba de integridad (una atestación). Los esquemas de atestación remota son protocolos de desafío-respuesta, donde se solicita a una aplicación que calcule dicha atestación en función del desafío que ha recibido de un servidor de verificación. En función de la respuesta recibida (la atestación), el verificador (una entidad de confianza remota, como un extremo de cabecera) puede emitir un veredicto de fiabilidad sobre la integridad de la ejecución de esa aplicación. Los esquemas de atestación habituales calculan dicha atestación a partir de información de tiempo de ejecución, como el contenido de la memoria. Hay, por ejemplo, esquemas publicados en los que el desafío define una visita predefinida a través de la memoria; la atestación es el *hash* de los valores encontrados durante esta visita.

[0009] Los esquemas de atestación remota conocidos requieren que se emule el entorno de tiempo de ejecución de la aplicación o que al menos la aplicación (o parte de ella) esté disponible por la entidad fiable, de modo que pueda calcular el resultado esperado ante el desafío y verificar la corrección de la atestación recibida. Esto introduce una complejidad significativa que, en la práctica, es muy difícil de manejar debido, por ejemplo, a la diversidad de versiones de la aplicación, y a la cantidad de instancias de aplicación que deben verificarse.

[0010] De acuerdo con la presente especificación, se propone un esquema de atestación en el que el cálculo del veredicto se reduce a verificar si existe una tupla {version, appsign} en un conjunto dado, lo que reduce en gran medida la complejidad de la implementación en la práctica. Esto se logra delegando una parte del esquema de atestación remota (es decir, la parte que asegura que hay un protocolo de desafío-respuesta adecuado) a una "interfaz de atestación remota" (RAF). La solución está diseñada para que la RAF no tenga información sobre la aplicación que se ha de verificar; solo admite el protocolo desafío-respuesta y extrae de la respuesta una firma de aplicación (appsign) que la entidad de verificación (VE) puede usar para emitir su veredicto de fiabilidad sobre la ejecución de la aplicación cliente (App).

[0011] La vista de alto nivel de esta solución se presenta en la Figura 1. La cabecera HE comprende una Entidad de Verificación VE y una Interfaz de Atestación Remota RAF. La entidad de verificación VE solicita a la Interfaz de Atestación Remota RAF que realice una consulta a un dispositivo de destino TD. La Interfaz de Atestación Remota RAF prepara un desafío CH y lo envía al dispositivo de destino TD. Cabe señalar que un dispositivo de destino puede ser cualquier tipo de dispositivo electrónico que incorpore una unidad de procesamiento que ejecute un programa.

[0012] El paso A es la transmisión del desafío al dispositivo de destino. Un desafío es un valor impredecible por el dispositivo de destino. Por ejemplo, puede ser generado aleatoriamente por la Interfaz de Atestación Remota RAF. La transmisión entre la Interfaz de Atestación Remota RAF y el dispositivo de destino TD puede ser un canal bidireccional, como una conexión a Internet, o puede ser una conexión de difusión en la que el desafío CH se envía a una pluralidad de dispositivos de destino TD.

[0013] Una vez que se recibe el desafío, puede comenzar la generación de la atestación (paso B). El dispositivo de destino TD comprende un módulo de atestación AM encargado de producir la atestación. Este módulo de atestación AM puede ser un programa dedicado del dispositivo de destino o un procesador independiente conectado al bus de comunicación principal del procesador principal. En este último caso, el procesador independiente tiene acceso a la memoria que almacena las variables y puede calcular el resumen en estas variables.

[0014] Atestación R = F (CH, APP), donde F representa la función que calcula la atestación en función del desafío CH recibido, y cierta información (de tiempo de ejecución) de la Aplicación (APP) como el espacio de memoria de la aplicación. Dado el desafío CH y la respuesta R, la RAF calcula la firma de la aplicación, que es un valor que solo debe depender de la información de la aplicación independiente del desafío.

[0015] A continuación, se presenta una construcción concreta para lograr esto. Un experto en la materia reconocerá que son posibles construcciones alternativas, variaciones y extensiones de esta construcción propuesta.

[0016] De acuerdo con una forma de realización, se construye un conjunto de vectores de resúmenes [h0, h1, ..., hn], que dependen únicamente de (partes de) la información (de tiempo de ejecución) de la aplicación, y definen la atestación como alguna función en este vector; la función se ejemplifica por el desafío y es invertible. Usando este desafío, la RAF puede calcular la función inversa, de modo que a partir de la atestación (respuesta) puede reconstruir este vector de resúmenes. La firma de la aplicación es el resultado de alguna función calculada en este vector de resúmenes (o una parte del mismo).

[0017] La figura 2 explica con más detalle el proceso de generación de atestación. El programa por verificar se divide en bloques (B0 ... B3), y el módulo de atestación AM comprende una memoria para almacenar el mapa de los bloques que forman parte de la generación de atestación. El módulo de atestación genera para cada bloque un resumen H que representa el bloque. Este resumen H se puede calcular de la siguiente manera:

- estático: un valor *hash* del bloque, o cualquier operación en el contenido del bloque de memoria,
- dinámico: el contenido de las memorias de tiempo de ejecución, incluyendo, por ejemplo, contenido de registros, de pila (*stack*), de montículo (*heap*) al final de la ejecución del bloque. Para generar los mismos valores en las memorias de tiempo de ejecución cada vez que se ejecuta el bloque, las memorias de tiempo de ejecución se establecen en valores predefinidos antes de la ejecución.

[0018] Una vez que se obtiene el conjunto de resúmenes (H0, H1, ... Hn), el siguiente paso es el cálculo de la atestación, y esta operación depende del desafío. Se aplica una función F(CH) en el conjunto de resúmenes para producir la atestación (H0', H1' ... Hn'). Existe una gran cantidad de posibilidades para la función F, el factor clave es la posibilidad de tener la función inversa F^{-1} que permite recuperar el conjunto de resúmenes.

Ejemplo de función F

[0019] Función de mezcla o *shuffle*: el desafío CH se usa como parámetro para mezclar cada miembro del conjunto. El conjunto resultante contiene todos los resúmenes, y solo la posición en el conjunto se modifica aleatoriamente en función del desafío CH.

[0020] Operación matemática: el resumen resultante H' es el resultado de una operación de al menos dos resúmenes. Ejemplo: H0'= H3 X H6; H1'= H2 x H5, o H0' = H3 + H6; H1'= H0 + H7. La selección de los resúmenes que participan en la operación se basa en el desafío CH. Se pueden ejecutar operaciones complejas como H0'= H3 X H6 + H7; H1'= H2 / H4 x H12 ...

[0021] Función afín: las funciones afines representan funciones de valor vectorial de la forma de, por ejemplo, H0'= A0.H0 + A1.H1 + ... An. Hn donde los coeficientes A0 a An están dados por el desafío.

[0022] Los ejemplos de transformaciones afines incluyen funciones lineales como sumas o multiplicaciones con una constante (la constante podría ser el coeficiente del desafío).

[0023] El conjunto de resúmenes (H0 ... Hn) se puede expresar como una matriz de resúmenes de x líneas e y columnas tal como:

$$H = \begin{Bmatrix} H0 & H1 & H2 \\ H3 & H4 & H5 \\ H6 & H7 & H8 \end{Bmatrix}$$ el desafío también puede ser en forma de una matriz $$C = \begin{Bmatrix} C0 & C1 & C2 \\ C3 & C4 & C5 \\ C6 & C7 & C8 \end{Bmatrix}$$

[0024] Y la atestación resultante H' puede ser una matriz como H' = F(CH,H). Una vez que el módulo de atestación del dispositivo de destino calcula la atestación H', el resultado se envía a la Interfaz de Atestación Remota RAF junto con un identificador de la versión de la aplicación (VER).

[0025] Otro ejemplo de la función F es una función de cifrado de la matriz de resúmenes, la clave utilizada para ese cifrado podría ser el desafío o la información derivada del desafío de acuerdo con una función de derivación conocida por la RAF y el dispositivo de destino.

[0026] La función utilizada para determinar la atestación puede ser una función multivariada que calcula la atestación en función del desafío y la matriz de resúmenes. Esta es preferiblemente una función lineal invertible. Esto se puede definir inequívocamente generando una función invertible basada en el desafío. La matriz resultante se multiplica con la matriz de resúmenes para obtener una atestación que se envía (como una matriz de la misma longitud de la matriz de resúmenes) a la RAF.

[0027] La RAF puede usar el mismo algoritmo para calcular la misma matriz a partir del desafío CH que continúa, y luego calcular su matriz inversa. Esto se aplica a la respuesta que produce la matriz original de resúmenes, que luego se utiliza para calcular la firma de la aplicación.

[0028] En la figura 3, se ilustran las operaciones ejecutadas por la RAF. Se recibe la ATT de atestación (paso C, figura 1) junto con el identificador de la aplicación (VER). La atestación ATT comprende un conjunto de valores (H0', H1' ... Hn') que es único por desafío. La RAF, como generadora del desafío C, puede usarla con la función inversa F^{-1} en la atestación ATT (paso D, figura 1). Esto producirá el conjunto de resúmenes calculados H0, H1 ... Hn.

[0029] Según una forma de realización, se genera una firma S a partir de los resúmenes calculados, por ejemplo, mezclando los resúmenes para producir un único valor S. La función de mezcla puede ser una función *hash* en los resúmenes. Esta firma S se envía a la entidad de verificación VE para su verificación.

[0030] La Entidad de Verificación VE comprende un almacenamiento de datos para almacenar un par de datos de referencia, donde dicho par comprende al menos la firma de referencia SR y la versión de la aplicación. Una vez que el par de la firma actual S y la versión actual V se recibe (paso E) por la Entidad de Verificación, la versión V del par recibido se usa para recuperar la firma de referencia SR del almacenamiento de datos.

[0031] Durante un paso de inicialización anterior, la Entidad de Verificación VE ha generado el conjunto de resúmenes de referencia (H0R, H1R ... HnR) y ha producido la firma de referencia SR, mientras que el conjunto de resúmenes de referencia se produce en un dispositivo cliente de referencia.

[0032] Se realiza una comparación entre la firma actual S y la firma de referencia SR y el resultado de la verificación permite determinar si la aplicación del dispositivo de destino es genuina. La Entidad de Verificación puede informar a un proveedor de servicios que se encarga de entregar el contenido al dispositivo de destino o de enviar un mensaje de validación al dispositivo de destino.

[0033] Según una forma de realización, el paso de producción de la atestación a partir del conjunto de resúmenes se puede combinar con la operación que calcula los resúmenes. Por ejemplo, cuando la función de generación de atestación es una función multivariada, y la función para calcular los resúmenes del bloque (los subresúmenes) es también una función multivariada, estas pueden combinarse. El bloque B0 de la aplicación APP se divide en una pluralidad de subresúmenes B0a, B0b ... B0n. La función F luego define las operaciones, parametrizadas con el desafío C, en los subresúmenes. Ejemplo:
Si H0 = B0a + B0b y H1 = B1a x B1b definen cómo se pueden calcular los resúmenes a partir de los subresúmenes y H0 '= C0 x H0 x H1 + C1 x H1 y H1' = C0 x H1 + C1 x H0, entonces H0 'y H1' se pueden calcular directamente mediante una definición F que depende de las entradas CH y los subresúmenes de la siguiente manera:

H0'= C0 x (B0a + B0b) x (B1a x B1b) + C1 x B1a x B1b

H1'= C0 x B1a x B1b + C1 X (B0a + B0b).

[0034] Este cálculo se puede representar de tal manera que es difícil separar las 2 operaciones.

[0035] Las multiplicaciones y sumas se dan como ejemplo. Cualquier tipo de operaciones matemáticas se puede aplicar con dos o más subresúmenes. Por lo tanto, el conjunto de resúmenes H0'... Hn' se produce directamente a partir de los subresúmeness de una pluralidad de bloques, generalizando el ejemplo anterior.

[0036] Según una forma de realización, el módulo de atestación del dispositivo de destino tiene una definición de los bloques B0 ... Bn. Esta definición se almacena en la memoria del módulo de atestación del dispositivo de destino o se implementa directamente en el *software* del módulo de atestación.

[0037] En otra forma de realización, la Entidad de Verificación VE comprende, en su almacenamiento de datos, una pluralidad de definiciones con el conjunto correspondiente de firmas de referencia y la versión de la aplicación. Una definición debe entenderse como la definición de los bloques de la aplicación que forman parte de la generación de los resúmenes (esto puede ser en forma de un conjunto de rango de memoria o un conjunto de direcciones de memoria) o la definición de los parámetros de inicialización de la ejecución en tiempo de ejecución del bloque. Para cada conjunto de parámetros de inicialización y para una versión dada, se almacena una firma de referencia en la base de datos. El módulo de atestación puede comprender varias definiciones de un conjunto de bloques almacenados en una tabla de memoria. La RAF incluye en el mensaje enviado al dispositivo de destino la indicación (índice de la tabla) de qué definición debe usarse para la determinación de la atestación.

Ejemplo de la tabla de definición

Índice de tabla	Bloque	Bloque	Bloque	Bloque	Bloque	Bloque
1	B3	B5	B12	B2	B1	B9
2	B0	B4	B10	B2	B7	B21
3	B4	B8	B2	B11	B17	B10
4	B1	B3	B6	B5	B13	B16

[0038] Cada bloque puede identificarse mediante una dirección inicial y final del *software* de destino.

[0039] Según otro ejemplo, el módulo de atestación recibe de la RAF la definición de los bloques que forman parte de la atestación.

[0040] Unos ejemplos preferidos de dispositivos de destino son los receptores de audio/vídeo y, en particular, la aplicación responsable de la verificación del derecho a procesar dicho audio/vídeo. Sin embargo, la verificación

puede llevarse a cabo en cualquier dispositivo que tenga un *software* que necesite verificación, como un teléfono inteligente o dispositivo utilizado en un entorno crítico (seguridad de unas instalaciones, por ejemplo).

[0041] La figura 4 ilustra el dispositivo de destino. Comprende un módulo de comunicación COMM para recibir el desafío con la solicitud de realización de la generación de una atestación. Este módulo también se utiliza para enviar la atestación a la RAF. El dispositivo de destino TD comprende una unidad de procesamiento PROC para ejecutar las operaciones relacionadas con la generación de la atestación. Alternativamente, el módulo de procesamiento puede delegar la generación de la atestación a un módulo de atestación AM. Tanto la unidad de procesamiento como el módulo de atestación tienen acceso a la memoria desde la cual puede llevarse a cabo el procedimiento de atestación.

[0042] Aunque se han descrito formas de realización de la presente invención con referencia a formas de realización ejemplares específicas, será evidente que se pueden realizar diversas modificaciones y cambios a estas formas de realización sin apartarse del alcance más amplio de estas formas de realización. Por consiguiente, la especificación y los dibujos deben considerarse en un sentido ilustrativo más que restrictivo. Los dibujos adjuntos que forman parte del presente documento, muestran a modo de ilustración, y no de limitación, formas de realización específicas en las que se puede aplicar el objeto de la invención. Las formas de realización ilustradas se describen con suficiente detalle para permitir que los expertos en la materia apliquen las enseñanzas aquí descritas. Se pueden utilizar otras formas de realización y derivar de ellas, de modo que se puedan realizar sustituciones y cambios estructurales y lógicos sin apartarse del alcance de esta divulgación. Esta descripción detallada, por lo tanto, no debe tomarse en un sentido limitativo, y el alcance de varias formas de realización se define solo por las reivindicaciones adjuntas, junto con el rango completo de equivalentes a los que tienen derecho tales reivindicaciones.

[0043] En este documento se puede hacer referencia a dichas formas de realización de la materia inventiva, de manera individual y/o colectiva, por el término "invención" simplemente por conveniencia y sin la intención de limitar voluntariamente el alcance de esta aplicación a ningún concepto inventivo si se divulga más de uno. Por lo tanto, aunque se han ilustrado y descrito formas de realización específicas en este documento, debe apreciarse que cualquier disposición calculada para lograr el mismo propósito puede ser sustituida por las formas de realización específicas mostradas. Esta divulgación está destinada a cubrir todas y cada una de las adaptaciones o variaciones de diversas formas de realización. Las combinaciones de las formas de realización anteriores, y otras formas de realización no descritas específicamente en este documento, serán evidentes para los expertos en la técnica al revisar la descripción anterior.

REIVINDICACIONES

1. Método para verificar, por un servidor de verificación, la integridad de ejecución de una aplicación en un dispositivo de destino en el que el servidor de verificación recibe una firma de aplicación generada a partir de la información de la aplicación en tiempo de ejecución en el dispositivo de destino, donde dicha firma se utiliza para verificar la integridad de ejecución de la aplicación en el dispositivo de destino, donde dicha aplicación comprende un conjunto de bloques, cada bloque que produce un resumen, produciendo así un conjunto de resúmenes relacionados con el conjunto de bloques, que comprende los pasos de:

- envío al dispositivo de destino de un mensaje que comprende un desafío y una primera función, donde dicha primera función define un método de agregación, y dicho desafío define una instrucción de agregación,
- recepción de una atestación del dispositivo de destino, donde esta atestación es generada por el dispositivo de destino mediante la determinación, para cada bloque, del resumen correspondiente para dicho bloque, la agregación de los resúmenes de los bloques de acuerdo con el método de agregación de la primera función y el desafío para producir la atestación relacionada con la solicitud,
- aplicación de una segunda función a la atestación por el servidor de verificación, donde dicha segunda función deshace el efecto del desafío produciendo así una firma de aplicación independiente del desafío,
- verificación de la integridad de ejecución de la aplicación mediante la comparación de la firma de la aplicación producida con una firma de referencia.

2. Método según la reivindicación 1, en el que la primera función es una función de mezcla (*shuffle*), que mezcla el conjunto de resúmenes de acuerdo con el desafío.

3. Método según la reivindicación 1, en el que la primera función es una función afín en la matriz de resúmenes de acuerdo con el desafío.

4. Método según la reivindicación 1, en el que la primera función es una función multivariable aplicada en la matriz de resúmenes de acuerdo con el desafío.

5. Método según cualquiera de las reivindicaciones 1 a 4, en el que el mensaje comprende además una descripción de los bloques de la aplicación que forman parte de la verificación de integridad.

6. Método según cualquiera de las reivindicaciones 1 a 5, en el que un bloque comprende una pluralidad de subbloques, cada uno de los cuales produce un subresumen, donde la atestación se produce directamente a partir de los subresúmenes entre los bloques usando la primera función y el desafío.

7. Sistema para verificar la integridad de ejecución de una aplicación en un dispositivo de destino (TD) que comprende una Entidad de Verificación (VE) y una Interfaz de Atestación Remota (RAF), donde dicha Interfaz de Atestación Remota está configurada (RAF) para:

- generar un desafío (C),
- transmitir el desafío (C) con una primera función al dispositivo de destino, donde dicha primera función define un método de agregación, donde dicho desafío define una instrucción de agregación,
- recibir una atestación (ATT) del dispositivo de destino, donde esta atestación es generada por el dispositivo de destino mediante la determinación, para cada bloque, del resumen correspondiente para dicho bloque, la agregación de los resúmenes de los bloques de acuerdo con el método de agregación de la primera función y el desafío para producir la atestación relacionada con la aplicación,
- aplicar una segunda función a la atestación (ATT), donde dicha segunda función deshace el efecto del desafío, produciendo así un conjunto de resúmenes (H0, H1, ... Hn) independientes del desafío,
- transmitir el conjunto de resúmenes (H0, H1, ... Hn) o una firma (S) que es una mezcla en el conjunto de resúmenes (H0, H1, ... Hn) a la Entidad de verificación (VE),

y donde la Entidad de Verificación está configurada para:

- verificar la integridad de ejecución de la aplicación mediante la comparación del conjunto de resúmenes recibidos (H0, H1, ... Hn) o la firma (S) con una referencia.

8. Sistema según la reivindicación 7, en el que la Interfaz de Atestación Remota (RAF) está configurada para transmitir al dispositivo de destino (TD) la definición de los bloques que forman parte de la atestación (ATT).

9. Sistema según la reivindicación 7 u 8, en el que la primera función es una función de mezcla, que mezcla el conjunto de resúmenes de acuerdo con el desafío.

10. Sistema según la reivindicación 7 u 8, en el que la primera función es una función afín en el conjunto de resúmenes de acuerdo con el desafío.

11. Sistema según la reivindicación 7 u 8, en el que la primera función es una función multivariable aplicada en la matriz de resúmenes de acuerdo con el desafío.

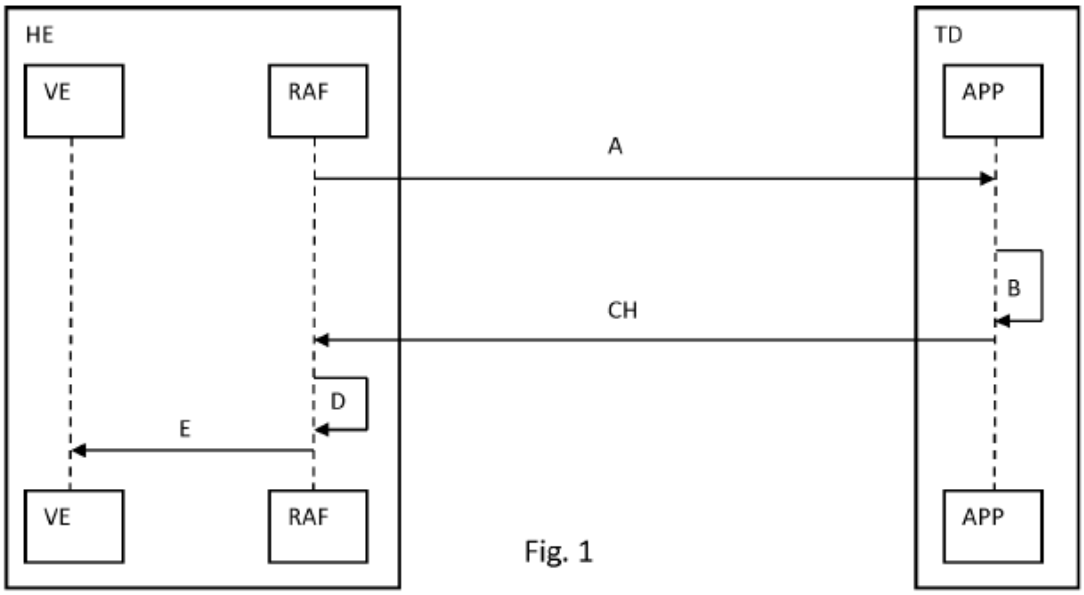

Fig. 1

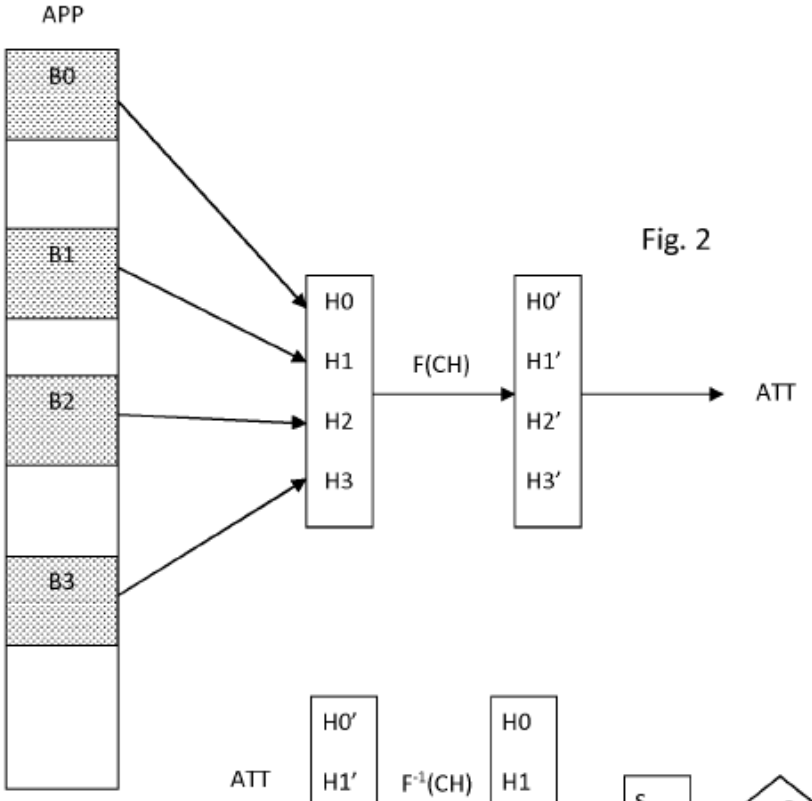

Fig. 2

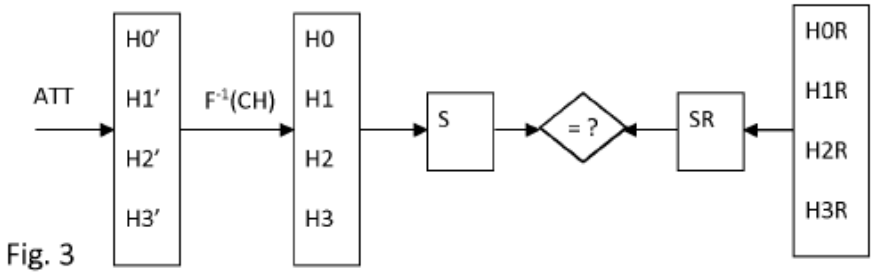

Fig. 3

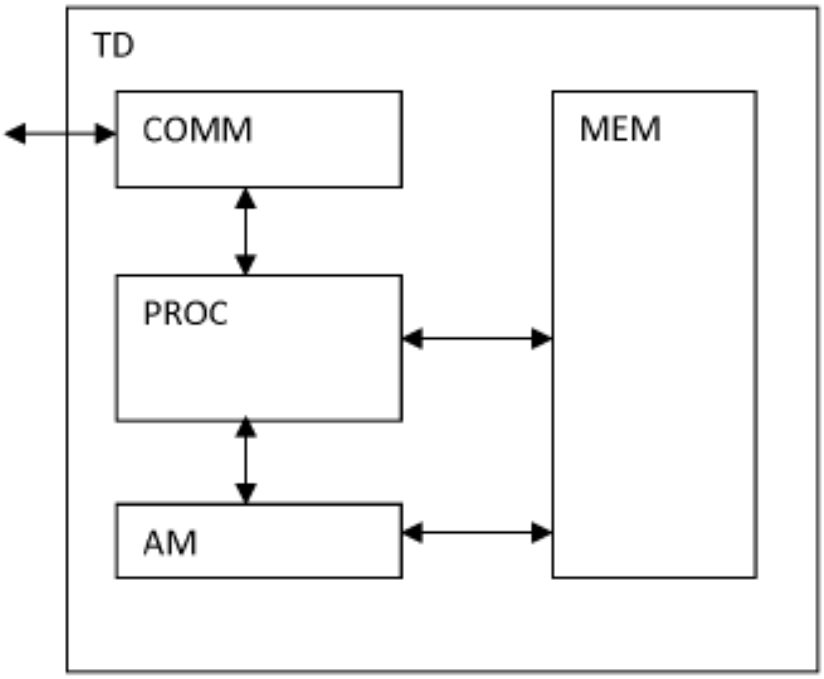

Fig. 4