(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 805 125**

(51) Int. CI.:

H04L 9/06	(2006.01)
H04L 9/08	(2006.01)
G06F 3/06	(2006.01)
G06F 12/0862	(2006.01)
G06F 12/0875	(2006.01)
G06F 12/14	(2006.01)
G06F 9/30	(2008.01)
G06F 9/38	(2008.01)
G06F 21/60	(2013.01)
G11C 7/10	(2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.03.2008 E 18165550 (7)**

(97) Fecha y número de publicación de la concesión europea: **27.05.2020 EP 3361668**

(54) Título: **Arquitectura e instrucciones flexibles para el estándar de cifrado avanzado (AES)**

(30) Prioridad:

28.03.2007 US 729199

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.02.2021

(73) Titular/es:

INTEL CORPORATION (100.0%)
2200 Mission College Boulevard
Santa Clara, CA 95052, US

(72) Inventor/es:

GUERON, SHAY;
FEGHALI, WAJDI, K.;
GOPAL, VINODH;
RAGHUNANDAN, MAKARAM;
DIXON, MARTIN, G.;
CHENNUPATY, SRINIVAS y
KOUNAVIS, MICHAEL, E.

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Arquitectura e instrucciones flexibles para el estándar de cifrado avanzado (AES)

Campo

Esta divulgación se refiere a algoritmos criptográficos y, en particular, al algoritmo del estándar de cifrado avanzado (AES).

Antecedentes

La criptología es una herramienta que se basa en un algoritmo y una clave para proteger información. El algoritmo es un algoritmo matemático complejo y la clave es una cadena de bits. Hay dos tipos básicos de sistemas de criptología: sistemas de clave secreta y sistemas de clave pública. Un sistema de clave secreta también denominado un sistema simétrico tiene una clave única ("clave secreta") que comparten dos o más partes. La clave única se utiliza para cifrar y descifrar información.

El estándar de cifrado avanzado (AES), publicado por el Instituto Nacional de Estándares y Tecnología (NIST) como Federal Information Processing Standard (FIPS) 197 es un sistema de clave secreta. AES es un cifrado de bloque simétrico que puede cifrar y descifrar información.

La encriptación (cifrado) realiza una serie de transformaciones utilizando la clave secreta (clave de cifrado) para transformar datos inteligibles denominados "texto plano" en una forma ininteligible denominada "texto cifrado". Las transformaciones en el cifrado incluyen: (1) agregar una clave de ciclo (valor derivado de la clave de cifrado) al estado (una matriz bidimensional de bytes) utilizando una operación O exclusiva (XOR); (2) procesar el estado utilizando una tabla (caja-S) de sustitución no lineal de bytes; (3) desplazar cíclicamente las últimas tres filas del estado mediante diferentes desplazamientos; y (4) tomar todas las columnas del estado y mezclar sus datos (independientemente uno del otro) para producir nuevas columnas.

La desencriptación (cifrado inverso) realiza una serie de transformaciones utilizando la clave de cifrado para transformar los bloques de "texto cifrado" en bloques de "texto plano" del mismo tamaño. Las transformaciones en el cifrado inverso son la inversa de las transformaciones en el cifrado. El algoritmo Rijndael se especifica en el estándar AES para procesar bloques de datos de 128 bits, utilizando claves de cifrado con longitudes de 128, 192 y 256 bits. Las diferentes longitudes de clave se denominan típicamente AES-128, AES-192 y AES-256.

El algoritmo AES transforma el texto plano en texto cifrado o el texto cifrado en texto plano en 10, 12, o 14 ciclos consecutivos, con el número de ciclos dependiente de la longitud de la clave.

El documento EP 1 586 971 A2 da a conocer un aparato microprocesador y un método para proporcionar un tamaño de clave criptográfica configurable. Una instrucción criptográfica prescribe una operación criptográfica.

El documento WO 2005/006197 A2 da a conocer un sistema para el cifrado de memoria que incluye la lectura de un bloque de datos cifrado de la memoria durante la cual se regenera un flujo de claves utilizado para cifrar el bloque de datos de acuerdo con uno o más criterios del bloque de datos cifrado.

El documento "AES PROPOSAL: RIJANDEL", propuesta AES, 3 de septiembre de 1999, páginas 1-45, XP001060386 da a conocer una propuesta AES para el uso de un cifrado de bloques Rijndael.

Breve descripción de los dibujos

Las características de las realizaciones de la materia objeto reivindicada se harán evidentes a medida que avance la siguiente descripción detallada y con referencia a los dibujos, en los que números iguales representan partes iguales, y en los que:

la Fig. 1 es un diagrama de bloques de un sistema que incluye una realización de una arquitectura e instrucciones flexibles para realizar el cifrado y descifrado AES en un procesador de propósito general de acuerdo con los principios de la presente invención

la Fig. 2 es un diagrama de bloques de una realización del procesador mostrado en la Fig. 1;

la Fig. 3 es un diagrama de bloques que incluye una realización de la unidad de ejecución mostrada en la Fig. 2 para realizar el cifrado y descifrado AES de acuerdo con los principios de la presente invención;

la Fig. 4 es un gráfico de flujo que ilustra el flujo de una instrucción de ciclo de cifrado aes a través de la unidad de ejecución mostrada en la Fig. 3;

la Fig. 5 es un diagrama de flujo que ilustra el flujo de una instrucción de último ciclo de cifrado aes a través de la unidad de ejecución mostrada en la Fig. 3;

la Fig. 6 es un diagrama de flujo que ilustra el flujo de una instrucción de ciclo de descifrado aes a través de la unidad de ejecución mostrada en la Fig. 3;

la Fig. 7 es un diagrama de flujo que ilustra el flujo de una instrucción de último ciclo de descifrado aes a través de la unidad de ejecución mostrada en la Fig. 3; y

la Fig. 8 ilustra una realización de una instrucción de ciclo aes con byte inmediato que puede utilizarse para generar claves de ciclo y realizar cifrado y descifrado.

Aunque la siguiente descripción detallada procederá haciendo referencia a realizaciones ilustrativas de la materia objeto reivindicada, muchas alternativas, modificaciones y variaciones de la misma serán evidentes para los expertos en la técnica.

En consecuencia, se pretende que la materia objeto reivindicada se vea de manera amplia y se defina solo como se establece en las reivindicaciones adjuntas.

Descripción detallada

El estándar de cifrado avanzado (AES) es un algoritmo de cálculo intensivo que se realiza típicamente en software o en un procesador de propósito especial. Por lo tanto, el cifrado generalmente solo se utiliza para cifrar un subconjunto de la información almacenada en las computadoras, por ejemplo, información que puede clasificarse como “alto secreto”. Sin embargo, hay una necesidad de cifrar más información que está almacenada en las computadoras. Por ejemplo, si toda la información almacenada en una computadora móvil estuviera encriptada, esta información estaría protegida en caso de que la computadora móvil fuera robada.

AES es un cifrado de bloque que opera en un bloque de 128 bits de bits con un tamaño de clave de 128, 192 o 256 bits. Se itera una secuencia de operaciones para varios ciclos (10, 12 o 14) según el tamaño de la clave.

La generación de las claves para cada ciclo se puede realizar sobre la marcha (es decir, justo antes de cada ciclo) utilizando los registros implícitos de 128 bits para almacenar la clave de ciclo. Sin embargo, el uso de registros implícitos puede reducir el rendimiento de los procesadores basados en registros x86 debido a la dependencia de un resultado de una instrucción previa

Existen algunas aplicaciones, por ejemplo, una aplicación que procesa los paquetes de red que pueden tener diferentes claves por flujo que se benefician de la generación de claves sobre la marcha. Puede haber otras aplicaciones en las que se requiere un mayor rendimiento con la clave única, por ejemplo, una clave única que se utiliza para cifrar/descifrar el contenido de una unidad de disco. Por lo tanto, surge una necesidad de flexibilidad en la generación de claves. Una realización de la invención proporciona una arquitectura e instrucciones flexibles para realizar el cifrado y descifrado AES en un procesador de propósito general.

La Fig. 1 es un diagrama de bloques de un sistema 100 que incluye una realización de una arquitectura e instrucciones flexibles para realizar el cifrado y descifrado AES en un procesador de propósito general de acuerdo con los principios de la presente invención. El sistema 100 incluye un procesador 101, un concentrador 102 controlador de memoria (MCH) o (concentrador controlador de memoria de gráficos (GMCH)) y un concentrador 104 controlador de entrada/salida (E/S) (ICH). El MCH 102 incluye un controlador 106 de memoria que controla la comunicación entre el procesador 101 y la memoria 108. El procesador 101 y el MCH 102 se comunican a través de un bus 116 del sistema.

El procesador 101 puede ser uno cualquiera de una pluralidad de procesadores, tales como un procesador de un solo núcleo Intel® Pentium IV ®, un procesador de un solo núcleo Intel Celeron, un procesador Intel® XScale o un

procesador multi-núcleo tal como Intel® Pentium D, procesador Intel® Xeon® o procesador Intel® Core® Duo o cualquier otro tipo de procesador.

La memoria 108 puede ser memoria de acceso aleatorio dinámica (DRAM), memoria de acceso aleatorio estática (SRAM), memoria de acceso aleatorio dinámica sincronizada (SDRAM), RAM doble velocidad de datos 2 (DDR2) o memoria de acceso aleatorio dinámica rambus (RDRAM) o cualquier otro tipo de memoria.

El ICH 104 puede estar acoplado al MCH 102 utilizando una interconexión 114 de chip a chip de alta velocidad tal como la interfaz de medios directa (DMI). DMI admite velocidades de transferencia concurrentes de 2 Gigabit/segundo a través de dos líneas unidireccionales.

El ICH 104 puede incluir un controlador 110 de almacenamiento de E/S para controlar la comunicación con al menos un dispositivo 112 de almacenamiento acoplado al ICH 104. El dispositivo de almacenamiento puede ser, por ejemplo, una unidad de disco, una unidad de disco de versátil digital (DVD), una unidad de disco compacto (CD), una matriz redundante de discos independientes (RAID), una unidad de cinta u otro dispositivo de almacenamiento. El ICH 104 puede comunicarse con el dispositivo 112 de almacenamiento a través de una interconexión 118 de protocolo de almacenamiento utilizando un protocolo de almacenamiento en serie como, por ejemplo, la pequeña interfaz de sistema del cómputo conectada en serie (SAS) o conexión de tecnología avanzada en serie (SATA).

El procesador 101 incluye una función 103 AES para llevar a cabo operaciones de cifrado y descifrado aes. La función 103 AES puede utilizarse para cifrar o descifrar información almacenada en la memoria 108 y/o almacenada en el dispositivo 112 de almacenamiento.

La Fig. 2 es un diagrama de bloques de una realización del procesador 101 mostrado en la Fig. 1. El procesador 101 incluye una unidad 206 de extracción y decodificación para decodificar las instrucciones del procesador recibidas de la caché 202 de instrucciones del nivel 1 (L1). Los datos a ser utilizados para ejecutar la instrucción pueden almacenarse en el archivo 208 de registro. En una realización, el archivo 208 de registro incluye una pluralidad de registros de 128 bits, que se utilizan por una instrucción aes para almacenar datos para su utilización por la instrucción aes.

En una realización, el archivo de registro es un grupo de registros de 128 bits similar a los registros MMX de 128 bits proporcionados en los procesadores Intel Pentium MMX, que tienen una extensión del conjunto de instrucciones (SSE) de streaming (Single Instruction Multiple Data) (SIMD). En un procesador SIMD, los datos se procesan en bloques de 128 bits con un bloque de 128 bits cargado al mismo tiempo.

La unidad 202 de extracción y decodificación extrae macroinstrucciones de la caché 202 de instrucciones de L1, decodifica las macroinstrucciones y las separa en operaciones simples llamadas microoperaciones (µops) que pueden almacenarse en la memoria 214 de sólo lectura (ROM) de microcódigo. La unidad 210 de ejecución planifica y ejecuta las microoperaciones. En la realización mostrada, la función 103 AES en la unidad 210 de ejecución incluye microoperaciones para un conjunto de instrucciones aes. La unidad 212 de retiro escribe los resultados de las instrucciones ejecutadas en registros o memoria. Una clave 214 de ciclo utilizada por la instrucción aes puede almacenarse en la caché 204 de datos de L1 y cargarse en la unidad 210 de ejecución para su utilización por las microoperaciones para ejecutar una instrucción aes en el conjunto de instrucciones aes. El almacenamiento de la clave 214 de ciclo en la caché 204 de datos protege la clave de ciclo de los ataques de canal lateral, por ejemplo, intentos de obtener la clave de ciclo para obtener acceso a la información cifrada almacenada en el sistema 100.

La Fig. 3 es un diagrama de bloques que ilustra una realización de la unidad 210 de ejecución mostrada en la Fig. 2 para realizar el cifrado y descifrado AES de acuerdo con los principios de la presente invención. La Fig. 3 se describirá junto con la Fig. 2.

Después de haber decodificado una instrucción AES mediante la unidad 206 de extracción y decodificación, la ejecución de una instrucción aes mediante la unidad 210 de ejecución implica realizar las microoperaciones asociadas con la instrucción aes que pueden almacenarse en la ROM 214 de microcódigo.

Un conjunto de instrucciones AES flexibles, de acuerdo con una realización de la presente invención, permite a un programador realizar compensaciones de rendimiento con respecto a la cantidad de datos a ser procesada y al ancho de banda y capacidad de memoria.

Algunas aplicaciones pueden utilizar continuamente la misma clave. En aplicaciones en las que el rendimiento es muy importante, se puede hacer una compensación en términos de calcular previamente una planificación de claves para la clave (es decir, una clave de ciclo por ciclo) una vez y almacenarla en la memoria. Es posible que otras aplicaciones deseen minimizar la cantidad de memoria utilizada para almacenar la planificación de claves mientras que aun logran un buen rendimiento en operaciones de múltiples bloques. Para aplicaciones de este tipo, la planificación de claves puede calcularse previamente para múltiples bloques antes de procesarse. La huella digital de memoria puede minimizarse aún más almacenando solo la clave de cifrado o la clave de cifrado inversa, y luego derivando la otra según sea necesario a expensas de algo de rendimiento.

En un procesador de tipo x86, el área y el número de puertos de ejecución que están disponibles para operaciones de clave de ciclo AES y operaciones de planificación AES limita el rendimiento de una instrucción AES. En un sistema en el que se requiere la expansión de clave para cada cifrado de bloque, el rendimiento puede mejorarse colocando las operaciones de planificación AES y las operaciones de clave de ciclo AES en puertos de ejecución separados. Sin embargo, los puertos de ejecución separados y el área adicional para controlar los puertos separados pueden no estar disponibles en un procesador de tipo x86.

En una realización, se proporciona un conjunto de instrucciones AES que incluye instrucciones aes separadas para realizar un ciclo de cifrado, un ciclo de descifrado, un cifrado de último ciclo, un descifrado de último ciclo y para el cálculo de una clave de ciclo de cifrado o una clave de ciclo de descifrado. En una realización, hay seis instrucciones aes en el conjunto de instrucciones aes. Cada una de las instrucciones de ciclo aes tiene un código (opcode) de operación único. A continuación, en la Tabla 1 se muestran las instrucciones de ciclo aes en el conjunto de instrucciones aes para una realización para una clave de ciclo de ancho fijo (por ejemplo, 128 bits).

Tabla 1

AESENCRYPTRound xmmsrcdst xmm
- Entrada: datos (=destino), clave de ciclo
- Salida: datos después de la transformación a través del ciclo AES utilizando la clave de ciclo

AESENCRYPTLastRound xmmsrcdst xmm
- Entrada: datos (=destino), clave de ciclo
- Salida: datos después de la transformación a través del último ciclo AES utilizando la clave de ciclo

AESDECRYPTRound xmmsrcdst xmm
- Entrada: datos (=destino), clave de ciclo
- Salida: datos después de la transformación a través del ciclo AES utilizando la clave de ciclo

AESDECRYPTLastRound xmmsrcdst xmm
- Entrada: datos (=destino), clave de ciclo
- Salida: datos después de la transformación a través del último ciclo AES utilizando la clave de ciclo

AESNextRoundKey xmmsrc1,2 xmm dst (inmediato)
- Entrada: 128 bits bajos de la clave, 128 bits altos de la clave, indicador de número de ciclo.
- Salida: clave de ciclo siguiente derivada de la entrada

AESPreviousRoundKey xmmsrc1,2 xmm dst (inmediato)
- Entrada: 128 bits bajos de la clave, 128 bits altos de la clave, indicador de número de ciclo
- Salida: clave de ciclo anterior derivada de la entrada

El conjunto de instrucciones aes incluye cuatro instrucciones aes de ciclo (cifrar, descifrar, cifrar último ciclo, descifrar último ciclo) y dos instrucciones de clave de ciclo aes (clave de ciclo siguiente y clave de ciclo anterior). Las instrucciones de ciclo aes en el conjunto de instrucciones aes incluyen operaciones de ciclo único para realizar operaciones de ciclo de cifrado y descifrado que se utilizarán para todos los ciclos excepto el último ciclo. Por ejemplo, en la instrucción de ciclo único AESENCRYPTRound en la Tabla 1, los datos de entrada se almacenan en un registro (xmmsrcdst) de 128 bits y la clave de ciclo se almacena en otro registro (xmm) de 128 bits. Esta instrucción realiza una operación de ciclo aes en los datos de entrada (origen) que están almacenados en el registro xmmsrcdst de 128 bits y sobrescribe los datos de entrada almacenados en el registro xmmsrcdst de 128 bits con el resultado de la ejecución de la operación de ciclo. Por lo tanto, el xmmsrcdst primero almacena los datos de entrada y luego almacena el resultado de la operación de ciclo aes.

El conjunto de instrucciones aes incluye también una instrucción de descifrado aes para un último ciclo de descifrado y una instrucción de cifrado aes para un último ciclo de cifrado. Por ejemplo, en la instrucción de ciclo único 'AESENCRYPTLastRound en la Tabla 1, los datos de entrada se almacenan en un registro (xmmsrcdst) de 128 bits y la clave de ciclo se almacena en otro registro (xmm) de 128 bits. Esta instrucción realiza una operación de ciclo aes en los datos de entrada (origen) que están almacenados en el registro xmmsrcdst y sobrescribe los datos de entrada almacenados en el registro xmmsrcdst con el resultado de la ejecución de la operación de ciclo. Por lo tanto, xmmsrcdst primero almacena los datos de entrada y luego almacena el resultado de la operación de ciclo. El registro xmm almacena la clave de ciclo para la operación de ciclo.

En otra realización, las instrucciones de ciclo y último ciclo, por ejemplo, 'AESENCRYPTRound y AESENCRYPTLastRound pueden tomar la entrada de la memoria (m/128) en lugar del archivo 304 de registro, por ejemplo, la instrucción de ciclo aes puede ser AESENCRYPTRound xmmsrcdst m/128.

Las otras dos instrucciones aes en el conjunto de instrucciones aes generan una clave de ciclo para un ciclo AES dependiente del tamaño de la clave, es decir, 128 bits, 192 bits o 256 bits. Una de las instrucciones de clave de ciclo aes genera una clave de ciclo para utilizar en una operación de cifrado y la otra instrucción de clave de ciclo aes genera una clave de ciclo para utilizar en una operación de descifrado. El campo inmediato en las instrucciones AESNextRoundKey y AESPreviousRoundKey especifica el tamaño de la clave {128, 192, 256}.

En otra realización más, en lugar de un campo inmediato, los diferentes tamaños de clave pueden implementarse como instrucciones separadas cada una con un código de operación único. En esta realización, el número de instrucciones de clave de ciclo aes incluye tres instrucciones separadas para cada operación de clave de ciclo, por ejemplo, AESNextRoundKey_128 AESNextRoundKey_192 y AESNextRoundKey_256 y habría un conjunto similar de tres instrucciones para AESPreviousRoundKey. En esta realización, el número total de instrucciones en el conjunto de instrucciones es 10 en lugar de 6 en la realización discutida anteriormente.

El archivo 304 de registro tiene una pluralidad de registros de 128 bits que pueden utilizarse por las instrucciones aes del conjunto de instrucciones aes. Los registros de 128 bits pueden almacenar operando u operandos de origen, claves de ciclo y el resultado de la instrucción aes. Para la primera ronda, la instrucción aes recibe un operando de origen que puede ser de 128 bits de texto plano a ser cifrado o 128 bits de texto cifrado a ser descifrado. Una clave para generar una planificación de claves para una clave de 128 bits, 192 bits o 256 bits puede almacenarse en cualquiera de los registros 308 de 128 bits en el archivo 304 de registro. Las claves de ciclo también pueden almacenarse en cualquiera de los registros 308 de 128 bits en el archivo de registro. Todas las instrucciones utilizan registros en el archivo de registro y también pueden recibir entrada directamente de la memoria, como se discutió anteriormente.

A continuación, en la Tabla 2 se muestra un ejemplo de código fuente que utiliza una realización del conjunto de instrucciones aes mostrado en la Tabla 1. En el ejemplo, el rendimiento se optimiza en una aplicación para realizar cifrado que utiliza la misma clave para muchos bloques. Una aplicación de este tipo es el uso de una clave única para cifrar el contenido de un disco en el que se utiliza la misma clave para cifrar todos los datos antes de ser almacenados en el disco. En el ejemplo, se realiza el cifrado AES-128.

El tamaño de la clave puede ser 128 bits, 192 bits o 256 bits. El número de ciclos a realizar (n) puede ser 1, 10, 12 o 14 dependiendo del tamaño de la clave, siendo cada clave de ciclo de un tamaño fijo (128 bits). Con un número de valor de ciclos de 10, 12, 14, las microoperaciones aes pueden realizar cifrado y descifrado aes estándar para tamaños de clave de 128 bits, 192 bits o 256 bits.

Cuando se utiliza la misma clave para muchos bloques, la clave de ciclo para cada ciclo (planificación de claves) puede calcularse previamente y almacenarse en la memoria (por ejemplo, caché 204 de datos de nivel 1), de modo que la misma planificación de claves no tiene que recalcularse antes de una operación de cifrado/descifrado en cada bloque.

Tabla 2

```
RK[0] = Clave de Entrada
Para i = 1..10
    RK[i] = AESNextRoundKey (RK[i-1])
Fin
```

```
ESTADO = Bloque de Entrada
ESTADO = ESTADO xor RK[0]

Para i = 1..9
    ESTADO = AESENCRYPTRound (ESTADO, RK[i])
Fin
ESTADO = AESENCRYPTLastRound (ESTADO, RK[10])
```

Una matriz (RK) que tiene 10 elementos se utiliza para almacenar la planificación de claves para la clave. La clave de entrada para el cifrado AES-128 se almacena en RK[0] y las 9 claves de ciclo RK[0] - RK[1] se calculan previamente mediante una llamada a la instrucción AESNextRoundKey del conjunto de instrucciones aes. La instrucción AESNextRoundKey calcula el siguiente ciclo en base a la clave de ciclo actual. Las claves de ciclo calculadas previamente para la planificación de claves pueden almacenarse en la clave 214 de ciclo en la caché 204 de datos de nivel 1.

En este ejemplo, ya que la porción de la planificación de claves (clave expandida), que es la clave de ciclo para el ciclo, se ingresa directamente desde el archivo 304 de registro, una operación O exclusiva (XOR) se realiza en el estado y la clave antes de ingresar al bucle para realizar los ciclos aes. Para cada ciclo 1 a 9, la instrucción AESENCRYPTRound del conjunto de instrucciones aes se llama para realizar la operación de ciclo aes para un ciclo. Para el último ciclo (ciclo 10), la instrucción AESNECYRPTLastRound del conjunto de instrucciones aes se llama para realizar la operación de ciclo aes para el último ciclo.

La información a ser cifrada o descifrada mediante la instrucción aes se carga en un registro 306 de origen/destino en el archivo 304 de registro antes de emitir la primera instrucción aes para iniciar una operación de cifrado o descifrado. La clave a ser utilizada para cifrar/descifrar la información en el registro 306 de origen se almacena en uno o más otros registros 308 en el archivo 308 de registro. En el caso de una clave de 128 bits, los 128 bits completos de la clave se almacenan en cualquiera de los otros registros de 128 bits en el archivo 304 de registro. Para tamaños de clave mayores de 128 bits, los bits más significativos (mayores de 128 bits) se almacenan en otro de los registros de 128 bits.

En el ejemplo mostrado en la Tabla 2, la clave de ciclo para cada ciclo se calcula previamente en base a la clave y se pueden almacenar en la caché 204 de datos de nivel 1 antes de ser cargada en uno cualquiera de los registros 308 en el archivo 304 de registro. La clave para cada ciclo también puede almacenarse en uno o más registros en el archivo 304 de registro o puede almacenarse en la clave 214 de ciclo en la caché 204 de datos de nivel 1.

El AES tiene un tamaño de bloque fijo de 128 bits y un tamaño de clave de 128, 192 o 256 bits y opera en una matriz de 4×4 de bytes (es decir, 16 bytes (tamaño de bloque fijo de 128 bits)), que se conoce como el 'estado'. El algoritmo AES transforma un bloque de texto plano de 128 bits en un bloque de texto cifrado (cifra) de 128 bits o un bloque de texto cifrado de 128 bits en un bloque de texto plano (descifra) de 128 bits en 10, 12 o 14 ciclos consecutivos, con el número de ciclos dependiente del tamaño de la clave (128, 192 o 256 bits).

Antes de realizar el cifrado por ciclo u operación de descifrado, la unidad 210 de ejecución recupera el estado y la clave que se almacenan en el archivo 304 de registro. Cada operación de ciclo de cifrado/descifrado se realiza utilizando las microoperaciones para la instrucción aes almacenada en el planificador 302 de claves en la memoria 214 de solo lectura (ROM). En la realización mostrada, el estado (estado de bloque de 128 bits) se almacena en el registro 306 y la clave se almacena en uno o más de los otros registros 308 en el archivo 304 de registro. Una vez completada la ejecución de la instrucción aes, el estado resultante se almacena en el registro 306 en el archivo 304 de registro. El estado puede ser una fecha de ciclo intermedia a ser utilizada por un próximo ciclo aes o el resultado final de la operación de cifrado o descifrado AES.

En la realización mostrada, un planificador 302 de claves genera la clave de ciclo a ser utilizada en un ciclo. El planificador 302 de claves puede implementarse como operaciones de microcódigo y puede incluir operaciones de microcódigo para realizar la secuencia de operaciones para generar claves de ciclo para claves de 128 bits, 196 bits y 256 bits, tal como se define en la publicación 197 de FIPS.

En otra forma de realización, el planificador de claves puede implementarse como una secuencia de máquina de estados hardware en la unidad 210 de ejecución. En otra realización más, una parte del planificador de claves puede implementarse como operaciones de microcódigo almacenadas en la ROM 214 de microcódigo y el resto del

planificador de claves puede implementarse como una secuencia de máquina de estados hardware en la unidad 210 de ejecución.

El planificador 302 de claves expande los n-bytes de una clave en b-bytes de una clave expandida (planificador de claves) con los primeros n-bytes de la clave expandida siendo la clave original. Por ejemplo, para una clave de 128 bits, la clave de 128 bits se expande en una clave expandida de 176 bytes, es decir, 11x16 bytes (128 bits), siendo los primeros 16 bytes la clave de 128 bits original y, por lo tanto, el número de ciclos es 10. Los 24 bytes de una clave de 192 bits se expanden en 208 bytes (13x16 bytes) para proporcionar 12 “claves de ciclo” una para cada uno de los 12 ciclos y los 32 bytes de una clave de 256 bits se expanden en 240 bytes (15x16 bytes) para proporcionar 14 “claves de ciclo”, una para cada uno de los 14 ciclos.

Tras la decodificación del código (opcode) de operación en una instrucción aes, una serie de parámetros a ser utilizados para controlar el flujo en la instrucción aes para un ciclo aes se almacenan en la lógica 322 de control. Los parámetros incluyen el tipo de operación (cifrado o descifrado) y si es un último ciclo.

La lógica 324 de ciclo aes puede incluir microoperaciones para las siguientes etapas: estado 314 de bloque, caja-S 316 caja-s/inversa, desplazar filas 316 y mezcla inversa, mezclar columnas 320 o nulas (denominadas “mezclar columnas”) y agregar clave 326 de ciclo.

En el estado 314 de bloque, la entrada de 128 bits (estado) a la lógica 324 de ciclo aes se le agrega una clave (porción de 128 bits de la clave expandida asociada con el ciclo) utilizando XOR bit a bit para producir un valor (estado) intermedio de 128 bits.

En la caja-S 316 caja-S/inversa, cada byte de este valor intermedio de 128 bits se sustituye por otro valor de byte que puede almacenarse y recuperarse a partir de una tabla de búsqueda, también denominada como una caja de sustitución o “caja-S”. La caja-S toma un cierto número de bits de entrada, m, y los transforma en un cierto número de bits de salida, n, y normalmente se implementa como una tabla de búsqueda. Normalmente se utiliza una tabla de búsqueda fija. Esta operación proporciona no linealidad mediante el uso de la función inversa sobre el campo de Galois (GF) (2^8). Por ejemplo, la salida de n bits se puede encontrar seleccionando una fila en la tabla de búsqueda utilizando los dos bits externos de la entrada de m bits y seleccionando una columna utilizando los bits internos de la entrada de m bits.

En desplazar filas 318, los resultados de la caja-S 316 caja-S/inversa pasan a través de una transformada lineal de bits en la que los bytes en cada fila de la matriz (estado de 128 bits (16 bytes)) de 4x4 recibida desde la etapa de sub bytes se desplazan cíclicamente a la izquierda. El número de posiciones que se desplaza cada byte difiere para cada fila en la matriz de 4x4.

En mezclar columnas 320, los resultados de desplazar filas 320 pasan a través de una transformada lineal de bits en la que cada columna de la matriz (estado) de 4x4 se trata como un polinomio a través de un campo binario de Galois (GF) (2^8) y luego se multiplica módulo $x^4 + 1$ con un polinomio fijo $c(x) = 3x^3 + x^2 + x + 2$. Un último ciclo aes difiere de los otros ciclos aes en que omite el mezclar columnas 320.

Agregar clave 324 de ciclo después de la etapa de mezclar columnas 320 realiza una función O exclusiva en la clave de ciclo a partir de la clave expandida y el resultado de desplazar filas 318 o mezclar columnas 320 para el ciclo aes.

Por ejemplo, la siguiente instrucción aes puede emitirse para llevar a cabo un ciclo de descifrado aes:

AESDECRYPTRound xmmsrcdst xmm

Este ejemplo realiza una operación de ciclo de cifrado AES de 128 bits con una clave cuya clave expandida se representa como {RK[1], RK[2],... RK[10]}. La clave de ciclo se puede generar emitiendo una instrucción (inmediata) AESPreviousRoundKey xmmsrc1,2 xmm dst antes de emitir la instrucción AESDECRYPTRound. La clave de ciclo puede cargarse directamente en el estado 314 de bloque desde la caché 204 de datos de nivel 1 o puede almacenarse primero en un registro (xmm) en el archivo 304 de registro y luego cargarse en el estado 314 de bloque desde el registro.

Cuando se utiliza una clave diferente para cifrar/descifrar cada bloque, por ejemplo, en el caso de un controlador de interfaz de red (NIC) que está cifrando/descifrando paquetes de datos, la clave de ciclo puede calcularse sobre la

marcha antes de realizar el cifrado/descifrado para cada ciclo, como se muestra en el pseudocódigo siguiente en la Tabla 3 para el cifrado AES-128:

Tabla 3

```
RK[0] = Clave de Entrada
ESTADO = Bloque de Entrada
ESTADO = ESTADO xor RK[0]

Para i = 1..9
    RK[i] = AESNextRoundKey (RK[i-1])
    ESTADO = AESENCRYPTRound (ESTADO, RK[i])
Fin
R[10] = AESNextRoundKey (RK[9])
ESTADO = AESENCRYPTLastRound (ESTADO, RK[10])
```

En este ejemplo, la clave de ciclo para el ciclo se genera antes de realizar el cifrado utilizando la clave de ciclo para cada uno de los 10 ciclos en la planificación de claves (clave expandida), es decir, ciclos 1-9 y ciclo 10 (el último ciclo).

El conjunto de instrucciones aes que incluyen instrucciones de ciclo aes únicas e instrucciones de generación de claves de ciclo aes únicas permite variantes de AES con diferente número de ciclos y planificación de claves, es decir, variantes de AES no definidas por la publicación 197 de FIPS. Por lo tanto, las instrucciones de aes de ciclo único en el conjunto de instrucciones aes proporcionan flexibilidad para realizar el cifrado y descifrado aes.

Ya que el número de ciclos realizados por el conjunto de instrucciones aes no es fijo, se puede realizar cualquier número de ciclos, si se requiere. Por ejemplo, el número de ciclos se puede hacer variar para soportar estándares de cifrado/descifrado futuros si se introducen nuevos estándares para ataques de resumen o MAC o ataques a AES.

La Fig. 4 es un diagrama de flujo que ilustra el flujo de una instrucción de ciclo de encriptación aes a través de la unidad 210 de ejecución mostrada en la Fig. 3.

En el bloque 400, la unidad 210 de ejecución espera una instrucción de ciclo de cifrado aes. Si la unidad 206 de extracción y decodificación ha decodificado una instrucción de ciclo de cifrado AES, el procesamiento continúa con el bloque 402. Si no, el procesamiento permanece en el bloque 400 esperando una instrucción de ciclo de cifrado aes.

En el bloque 402, durante la decodificación de la instrucción mediante la unidad 206 de extracción y decodificación, una indicación de que el cifrado se va a realizar se almacena en la lógica 322 de control y la clave de ciclo y el estado (origen) de bloque de 128 bits para uso en la ejecución del ciclo de cifrado se carga en la unidad 210 de ejecución desde el archivo 304 de registro. El procesamiento continúa con el bloque 404.

En el bloque 404, una operación de sustitución se realiza en el estado de bloque de 128 bits, es decir, el resultado del bloque 406 o 418. Cada byte del estado de bloque de 128 bits se sustituye con otro valor de byte que se puede almacenar y recuperar de una tabla de búsqueda también denominada caja de sustitución o “caja-S”. La caja-S toma un cierto número de bits de entrada, m, y los transforma en un cierto número de bits de salida, n, y normalmente se implementa como una tabla de búsqueda. El resultado se almacena como un estado de bloque de 128 bits. El procesamiento continúa con el bloque 406.

En el bloque 406, el estado (matriz de 4x4) de bloque de 128 bits pasa a través de una transformada lineal de bits en la que bytes en cada fila de la matriz de 4x4 se desplazan cíclicamente a la izquierda. El número de posiciones que se desplaza cada byte difiere para cada fila en la matriz de 4x4. El procesamiento continúa con el bloque 408.

En el bloque 408, el estado (matriz de 4x4) de bloque de 128 bits pasa a través de una transformada lineal de bits en el que cada columna de la matriz (estado) de 4x4 se trata como un polinomio sobre $GF(2^8)$ y luego se multiplica módulo $x^4 + 1$ con un polinomio fijo $c(x) = 3x^3 + x^2 + x + 2$. El procesamiento continúa con el bloque 410.

En el bloque 410, una función O exclusiva se realiza en la clave de ciclo a partir de la clave expandida y el resultado de desplazar filas 318 o mezclar columnas 320 para el ciclo aes. El procesamiento continúa con el bloque 412.

En el bloque 412, el resultado de la operación de cifrado para el ciclo (estado de bloque de 128 bits) se almacena en el registro 302 de origen/destino en el archivo 304 de registro. El procesamiento para la instrucción de cifrado aes se completa.

La Tabla 4 a continuación muestra un ejemplo del resultado de realizar el cifrado AES-128 utilizando una clave de 128 bits en un bloque de 128 bits ingresada después de la ejecución del pseudocódigo mostrado en la Tabla 3.

Tabla 4

Entrada de 128 bits:	00112233445566778899aabbccddeeff (hexadecimal)
Clave de 128 bits:	000102030405060708090a0b0c0d0e0f (hexadecimal)
Resultado de 128 bits:	69c4e0d86a7b0430d8cdb78070b4c55a (hexadecimal)

La Fig. 5 es un diagrama de flujo que ilustra el flujo de una instrucción de último ciclo de cifrado aes a través a través de la unidad 210 de ejecución mostrada en la Fig. 3.

En el bloque 500, la ejecución espera a una instrucción de último ciclo de cifrado aes. Si la unidad 206 de extracción y decodificación ha decodificado una instrucción de último ciclo de cifrado AES, el procesamiento continúa con el bloque 502. Si no, el procesamiento permanece en el bloque 500 esperando una instrucción aes.

En el bloque 502, una búsqueda de caja-S se realiza para el último ciclo de una manera similar a la búsqueda de caja-S discutida en conjunción con el bloque 404 (Fig. 4). El procesamiento continúa con el bloque 504.

En el bloque 504, una operación de desplazar filas se realiza para el último ciclo de una manera similar a la descrita en conjunción con los otros ciclos en el bloque 406 (Fig. 4). El procesamiento continúa con el bloque 506.

En el bloque 506, una función O exclusiva se realiza en la clave de ciclo a partir de la clave expandida y el resultado de desplazar filas 318 o mezclar columnas 320 para el ciclo aes. El procesamiento continúa con el bloque 508.

En el bloque 508, el resultado de la operación de último ciclo de cifrado se almacena en el registro 306 de origen/destino en el archivo 304 de registro. El procesamiento para la instrucción aes se completa.

La Fig. 6 es un diagrama de flujo que ilustra el flujo de una instrucción de ciclo de descifrado aes a través de la unidad 210 de ejecución mostrada en la Fig. 3.

En el bloque 600, la ejecución espera una instrucción de ciclo de descifrado aes. Si la unidad 206 de extracción y decodificación ha descifrado una instrucción de ciclo de descifrado AES, el procesamiento continúa con el bloque 602. Si no, el procesamiento permanece en el bloque 600 esperando una instrucción de ciclo de descifrado aes.

En el bloque 602, durante la decodificación de la instrucción mediante la unidad 206 de extracción y decodificación, una indicación de que debe realizarse un ciclo de descifrado se almacena en la lógica 322 de control y la clave de ciclo y el origen (estado de bloque de 128 bits) para el uso en la realización del ciclo de descifrado se cargan en la unidad 210 de ejecución desde el archivo 304 de registro. El procesamiento continúa con el bloque 604.

En el bloque 604, la operación a ser realizada es el descifrado. Se realiza una operación de sustitución en el estado de bloque de 128 bits realizando una búsqueda inversa de caja-s, como se define en el estándar AES. El procesamiento continúa con el bloque 606.

En el bloque 606, se realiza una operación inversa de desplazar filas, como se define por la publicación 197 de FIPS. El procesamiento continúa con el bloque 608.

En el bloque 608, se realiza una operación inversa de desplazar filas, como se define por la publicación 197 de FIPS. El procesamiento continúa con el bloque 610.

En el bloque 610, se realiza una función O exclusiva en la clave de ciclo a partir de la clave expandida y el resultado de desplazar filas 318 o mezclar columnas 320 para el ciclo aes. El procesamiento continúa con el bloque 612.

En el bloque 612, el resultado de la operación de descifrado para el ciclo (estado de bloque de 128 bits) se almacena en el registro 302 de origen/destino en el archivo 304 de registro. El procesamiento para la instrucción de ciclo de descifrado aes se completa.

La Fig. 7 es un diagrama de flujo que ilustra el flujo de una instrucción de último ciclo de descifrado aes a través de la unidad 210 de ejecución mostrada en la Fig. 3.

En el bloque 700, la unidad 210 de ejecución espera una instrucción de último ciclo de descifrado aes. Si se ha decodificado una instrucción de último ciclo de descifrado AES mediante la unidad 206 de extracción y decodificación, el procesamiento continúa con el bloque 702. Si no, el procesamiento permanece en el bloque 700 esperando una instrucción de último ciclo de descifrado aes.

En el bloque 702, se realiza una operación de sustitución en el estado de bloque de 128 bits para el último ciclo realizando una búsqueda inversa de caja-s, tal como se define por la publicación 197 de FIPS. El procesamiento continúa con el bloque 704.

En el bloque 704, se realiza una operación inversa de desplazar filas para el último ciclo, como se define por la publicación 197 de FIPS. El procesamiento continúa con el bloque 706.

En el bloque 706, se realiza una función O exclusiva en la clave de ciclo a partir de la clave expandida y el resultado de desplazar filas 318 o mezclar columnas 320 para el ciclo aes. El procesamiento continúa con el bloque 708.

En el bloque 708, el resultado de la operación de último ciclo de descifrado se almacena en el registro 306 de origen/destino en el archivo 304 de registro. El procesamiento de la instrucción de último ciclo de descifrado aes se completa.

En una realización, los bloques en los diagramas de flujo de las Figs. 4-7 pueden implementarse como una secuencia de máquina de estados hardware en la unidad 210 de ejecución. En otra realización las porciones de los bloques pueden implementarse como un microprograma que puede almacenarse en la memoria 214 de solo lectura (ROM). La realización en la que los bloques se implementan como una secuencia de máquina de estados hardware puede proporcionar un mayor rendimiento.

La Fig. 8 ilustra una realización de una instrucción de ciclo aes con byte inmediato que puede utilizarse para generar claves de ciclo y realizar cifrado y descifrado. En lugar del conjunto de instrucciones aes mostrado en la Tabla 1, se proporciona una sola instrucción de ciclo aes para realizar las funciones del conjunto de instrucciones aes. La función particular a ser realizada por la instrucción aes única está codificada en bits en el byte (key_select_modifier) inmediato. El byte inmediato permite que la instrucción de ciclo aes se expanda para agregar nuevas características en lugar de crear una pluralidad de nuevas instrucciones con cada instrucción teniendo un código de operación único.

La instrucción de ciclo aes se puede definir simbólicamente como sigue:

dest: = aes_key_round (origen2, origen1), key_select_modifier

La instrucción aes_key_round se emite a una unidad 210 de ejecución particular en base al número de puerto con el fin de realizar una operación de cifrado o descifrado AES. En la realización mostrada, el número 4 de puerto es el puerto de ejecución designado para la instrucción de ciclo AES. La unidad 210 de ejecución se divide en muchos puertos paralelos (superescalar). Sin embargo, no todos los puertos son iguales. Algunos puertos tienen recursos especializados, tal como un multiplicador entero grande o un multiplicador o divisor de coma flotante. Las instrucciones más simples y más comunes, tal como la suma, la resta y el O exclusivo, se soportan en múltiples puertos para obtener el máximo rendimiento. Por lo tanto, para cada instrucción o microoperación, la lógica de control de emisión determina el puerto al cual emitir la microoperación/instrucción. En esta realización, la instrucción aes siempre se emite al número 4 de puerto. Sin embargo, en otras realizaciones se pueden utilizar otros números de puerto.

Haciendo referencia a la Fig. 8, dest almacena 128 bits de clave expandida para el ciclo N, origen2 almacena 128 bits de clave expandida para el ciclo N-1, y orgien almacena 128 bits de clave expandida para el ciclo N-2. El key_select_modifier es un valor inmediato de 8 bits utilizado para proporcionar el número (N) de ciclo actual, la dirección de operación (cifrado/descifrado) y tamaño de clave AES. Para AES-128, origen1 no es necesario y se ignora. La unidad de ejecución es la unidad AES y no se utilizan banderas (entero o coma flotante).

En una realización, la codificación de bits de los cuatro bits menos significativos del valor inmediato indican el número de ciclo, por ejemplo, un número de ciclo de 1-10 para AES-128, un número de ciclo de 1-12 para AES-192 y un número de ciclo de 2-14 para AES-256. Para AES-128 y 192, el número 0 de ciclo no es válido ya que el primer ciclo utiliza la clave de entrada no modificada. Para AES-256, los números 0 y 1 de ciclo no son válidos, ya que la clave de entrada de 256 bits no modificada se utiliza para los 2 primeros ciclos de 128 bits.

El bit 4 del byte inmediato indica la dirección de operación (cifrado o descifrado), por ejemplo, en una realización 0 = cifrar y 1 = descifrar y en otra realización 1 = cifrar y 0 = descifrar. Los bits 5 y 6 del byte inmediato indican el tamaño de clave AES. En una realización, el tamaño de clave AES se define como se muestra en la Tabla 5 a continuación:

Tabla 5

Bits [6:5]	Tamaño de Clave
00	128
01	192
10	256
11	Reservado

En otra realización, los bits [6:5] que tienen un valor de 11 es también un indicador para un tamaño de clave de 128 bits. En esta realización, todos los valores de bits [6:5] son válidos y pueden analizarse.

Será evidente para los expertos en la técnica que los métodos involucrados en realizaciones de la presente invención pueden realizarse en un producto de programa informático que incluye un medio utilizable por computadora. Por ejemplo, un medio utilizable por computadora de este tipo puede consistir en un dispositivo de memoria de solo lectura, tal como un disco compacto de memoria de solo lectura (CD ROM) o dispositivos ROM convencionales, o un disquete de computadora, que tiene un código de programa legible por computadora almacenado en el mismo.

Si bien las realizaciones de la invención se han mostrado y descrito particularmente con referencias a las realizaciones de la misma, los expertos en la técnica entenderán que se pueden realizar diversos cambios en la forma y los detalles sin apartarse del alcance de las realizaciones de la invención abarcadas por las reivindicaciones adjuntas.

La siguiente sección de la descripción consiste en párrafos numerados que simplemente proporcionan declaraciones de realizaciones de la invención ya descritas en el presente documento. Los párrafos numerados en esta sección no son reivindicaciones. Las reivindicaciones se exponen a continuación en la sección posterior titulada “reivindicaciones”.

1. Un aparato que comprende: una unidad de ejecución para realizar una secuencia de operaciones para una instrucción aes, la secuencia de operaciones para realizar un número programable de ciclos aes, las operaciones hacen que la unidad de ejecución: si el número de ciclos aes es mayor que 1: cargar una clave en un registro de clave temporal; y antes de realizar cada ciclo aes, generar una clave de ciclo para el ciclo aes en base a la clave; y para cada ciclo aes, realizar una secuencia de operaciones de ciclo aes en una entrada al ciclo aes y la clave de ciclo para el ciclo aes para proporcionar una siguiente entrada a un siguiente ciclo aes o un resultado para la instrucción aes.

2. El aparato de la cláusula 1, en donde si el número de ciclos aes es igual a 1, antes de realizar la secuencia de operaciones de ciclo aes, la unidad de ejecución debe:
cargar una clave de ciclo calculada previamente para el ciclo aes en base a la clave.

3. El aparato de la cláusula 2, en donde la secuencia de las operaciones de ciclo aes hace que la unidad de ejecución: realice una operación O exclusiva (XOR) en una entrada al ciclo y la clave de ciclo para que el ciclo aes produzca un valor intermedio; realizar una operación de sustitución para cada byte en el valor intermedio en base a los valores almacenados en una tabla de búsqueda; y pasar los resultados de la operación de sustitución a través de una transformada lineal de bits que desplaza filas en el valor intermedio.

4. El aparato de la cláusula 1, en donde la secuencia de operaciones de ciclo aes para el número de ciclos -1 aes hace que la unidad de ejecución: realice una operación O exclusiva (XOR) en la entrada al ciclo aes y la clave de ciclo para que el ciclo aes produzca un valor intermedio; realizar una operación de sustitución para cada byte en el valor intermedio en base a los valores almacenados en una tabla de búsqueda; pasar los resultados de la operación de

sustitución a través de una transformada lineal de bits que desplaza filas en el valor intermedio; y pasar los resultados de la operación de sustitución a través de la transformada lineal de bits que mezcla columnas en el valor intermedio.

5. El aparato de la cláusula 4, en donde la secuencia de operaciones de ciclo aes para el último ciclo hace que la unidad de ejecución: realice una operación O exclusiva (XOR) en una entrada al ciclo y la clave de ciclo para que el ciclo aes produzca un valor intermedio; realice una operación de sustitución para cada byte en el valor intermedio en base a los valores almacenados en una tabla de búsqueda; y pase los resultados de la operación de sustitución a través de una transformada lineal de bits que desplaza filas en el valor intermedio.

6. El aparato de la cláusula 1, en donde el resultado es un valor cifrado.

7. El aparato de la cláusula 1, en donde el resultado es un valor descifrado.

8. El aparato de la cláusula 1, en donde la clave y la entrada para un primer ciclo aes se almacenan en un archivo de registro.

9. El aparato de la cláusula 1, en donde el archivo de registro incluye una pluralidad de registros de 128 bits.

10. Un método que comprende: si el número de ciclos aes programables para una instrucción aes es mayor que 1, cargar una clave en un registro de clave temporal y antes de realizar cada ciclo aes, generar una clave de ciclo para el ciclo aes en base a la clave; y, para cada ciclo aes, realizar una secuencia de operaciones de ciclo aes en una entrada al ciclo aes y la clave de ciclo para que el ciclo aes proporcione una siguiente entrada a un siguiente ciclo aes o un resultado para la instrucción aes.

11. El método de la cláusula 10, en donde si el número de ciclos aes es igual a 1, antes de realizar la secuencia de operaciones de ciclo aes, cargar una clave de ciclo calculada previamente para el ciclo aes en base a la clave.

12. El método de la cláusula 11, en donde realizar la secuencia de operaciones de ciclo aes comprende: realizar una operación O exclusiva (XOR) en una entrada al ciclo y la clave de ciclo para que el ciclo aes produzca un valor intermedio; realizar una operación de sustitución para cada byte en el valor intermedio en base a los valores almacenados en una tabla de búsqueda; y pasar los resultados de la operación de sustitución a través de una transformada lineal de bits que desplaza filas en el valor intermedio.

13. El método de la cláusula 10, en donde realizar la secuencia de operaciones de ciclo aes para el número de ciclos -1 comprende: realizar una operación O exclusiva (XOR) en la entrada al ciclo aes y la clave de ciclo para que el ciclo aes produzca un valor intermedio; realizar una operación de sustitución para cada byte en el valor intermedio en base a los valores almacenados en una tabla de búsqueda; pasar resultados de la operación de sustitución a través de una transformada lineal de bits que desplaza filas en el valor intermedio; y pasar los resultados de la operación de sustitución a través de la transformada lineal de bits que mezcla columnas en el valor intermedio.

14. El método de la cláusula 13, en donde realizar la secuencia de operaciones de ciclo aes para un último ciclo aes comprende: realizar una operación O exclusiva (XOR) en una entrada al ciclo y la clave de ciclo para que el ciclo aes produzca un valor intermedio; realizar una operación de sustitución para cada byte en el valor intermedio en base a los valores almacenados en una tabla de búsqueda; y pasar los resultados de la operación de sustitución a través de una transformada lineal de bits que desplaza filas en el valor intermedio.

15. El método de la cláusula 10, en donde el resultado es un valor cifrado.

16. El método de la cláusula 10, en donde el resultado es un valor descifrado.

17. El método de la cláusula 10, en donde la clave y la entrada para un primer ciclo aes se almacenan en un archivo de registro.

18. El método de la cláusula 10, en donde que el archivo de registro incluye una pluralidad de registros de 128 bits.

19. Un artículo que incluye un medio accesible por máquina que tiene información asociada, en donde la información, cuando se accede, da como resultado que una máquina realice: si el número de ciclos aes programables para una instrucción aes es mayor que 1, cargar una clave en registro de clave temporal y antes de realizar cada ciclo aes, generar una clave de ciclo para el ciclo aes en base la clave; y para cada ciclo aes, realizar una secuencia de

operaciones de ciclo aes en una entrada al ciclo aes y la clave de ciclo para que el ciclo aes proporcione una siguiente entrada al siguiente ciclo aes o un resultado para la instrucción aes.

20. El artículo de la cláusula 10, en donde si el número de ciclos aes es igual a 1, antes de realizar la secuencia de operaciones de ciclo aes, cargar una clave de ciclo calculada previamente para el ciclo aes en base a la clave.

21. Un sistema que comprende: una memoria dinámica de acceso aleatorio para almacenar datos e instrucciones; y un procesador acoplado a dicha memoria para ejecutar las instrucciones, el procesador que comprende: una unidad de ejecución para realizar una secuencia de operaciones para una instrucción aes, la secuencia de operaciones para realizar un número programable de ciclos aes, las operaciones para hacer que la unidad de ejecución: si el número de ciclos aes es mayor que 1: cargar una clave en un registro de clave temporal; y antes de realizar cada ciclo aes, generar una clave de ciclo para el ciclo aes en base a la clave; y para cada ciclo aes, realizar una secuencia de operaciones de ciclo aes en una entrada al ciclo aes y la clave de ciclo para que el ciclo aes proporcione una siguiente entrada a un siguiente ciclo aes o un resultado para la instrucción aes.

22. El sistema de la cláusula 22, en donde si el número de ciclos aes es igual a 1, antes de realizar la secuencia de operaciones de ciclo aes, la unidad de ejecución: carga una clave de ciclo calculada previamente para el ciclo aes en base a la clave.

REIVINDICACIONES

1. Un procesador que comprende:
una pluralidad de núcleos;
una caché de instrucciones de nivel 1, L1, para almacenar una pluralidad de instrucciones del estándar de cifrado avanzado, AES, cada instrucción AES tiene un opcode único;
una caché de datos de L1;
lógica de extracción de instrucciones para extraer instrucciones de la caché de instrucciones de L1;
lógica de decodificación para decodificar las instrucciones;
un primer registro de origen para almacenar una clave de ciclo a ser utilizada para un ciclo de una operación de cifrado AES;
un segundo registro de origen para almacenar datos de entrada a ser cifrados mediante el ciclo de la operación de cifrado AES; y
una unidad de ejecución que incluye lógica de ejecución AES para ejecutar al menos una primera instrucción AES de la pluralidad de instrucciones AES para realizar el ciclo de la operación de cifrado AES, el ciclo de la operación de cifrado AES que utiliza la clave de ciclo del primer registro de origen para cifrar los datos de entrada del segundo registro de origen y almacena un resultado del ciclo de la operación de cifrado AES en un primer registro de destino.

2. El procesador (101) de la reivindicación 1, en donde el ciclo de la operación de cifrado AES realizado en respuesta a la primera instrucción AES incluye:
una transformada de sub bytes para realizar una sustitución de bytes en los datos de entrada, la transformada de sub bytes que incluye una caja de sustitución, caja-S, de búsqueda para dar como resultado una primera matriz de datos sustituidos;
una transformada de desplazar filas para desplazar datos de fila en la primera matriz en una cantidad especificada para dar como resultado una segunda matriz;
una transformada de mezclar columnas en la que las columnas de la segunda matriz han de tratarse como polinomios sobre un campo de Galois GF(28) y se multiplican módulo $x^4 + 1$ con un polinomio fijo para generar un resultado de mezclar columnas; y
una transformada de agregar clave de ciclo en la que una función O exclusiva utiliza datos de la clave de ciclo y el resultado de mezclar columnas.

3. El procesador de la reivindicación 2, en donde la unidad de ejecución ejecuta una segunda instrucción AES para realizar un ciclo final de la operación de cifrado AES, el ciclo final de la operación de cifrado AES utiliza una clave de ciclo correspondiente al ciclo final de una operación de cifrado AES para cifrar unos datos de entrada que han de ser cifrados mediante el ciclo final de la operación de cifrado AES y para almacenar un resultado final cifrado de la operación de cifrado AES en un registro de destino, en donde el ciclo final de la operación de cifrado AES incluye:
una operación de sustitución a ser realizada en los datos de entrada que han de cifrarse en el ciclo final de la operación de cifrado AES, la operación de sustitución utiliza una caja-S para dar como resultado una segunda matriz de datos sustituidos;
una transformada de desplazar filas para desplazar datos de desplazar filas en la segunda matriz en una cantidad especificada para generar un resultado de desplazar filas; y
una transformada de agregar clave de ciclo en la que una función O exclusiva utiliza datos de la clave de ciclo correspondiente al ciclo final de una operación de cifrado AES y el resultados de desplazar filas.

4. El procesador de una cualquiera de las reivindicaciones 1 a 3, en donde el procesador es un procesador de propósito general, en donde la pluralidad de instrucciones AES incluye más de cuatro instrucciones AES y en donde la unidad de ejecución ejecuta microcódigo para ejecutar la primera instrucción AES.

5. Un sistema que comprende:
el procesador de una cualquiera de las reivindicaciones 1-4; y
un dispositivo de almacenamiento acoplado al procesador.

6. El sistema de la reivindicación 5, que comprende además al menos un controlador de interfaz de red acoplado al procesador para procesar paquetes de datos y en donde el dispositivo de almacenamiento se dispone como una matriz redundante de discos independientes, RAID.

7. Un sistema que comprende:
el procesador de una cualquiera de las reivindicaciones 1-4;

un controlador de memoria para acoplar el procesador a una memoria dinámica de acceso aleatorio, DRAM; y

un controlador de entrada/salida, E/S, para acoplar el procesador a uno o más dispositivos.

8. El sistema de la reivindicación 7, en donde el controlador de memoria es un controlador de memoria de gráficos, y en donde el controlador de E/S es un controlador de E/S de almacenamiento.

9. Un procesador que comprende:

una pluralidad de núcleos;

una caché de instrucciones de nivel 1, L1, para almacenar una pluralidad de instrucciones del estándar de cifrado avanzado, AES, cada instrucción AES tiene un código ascendente único;

una caché de datos de L1;

lógica de extracción de instrucciones para extraer instrucciones de la caché de instrucciones de L1;

lógica de decodificación para decodificar las instrucciones;

un primer registro de origen para almacenar una clave de ciclo a ser utilizada para un ciclo de una operación de descifrado AES;

un segundo registro de origen para almacenar datos de entrada a ser descifrados mediante el ciclo de la operación de descifrado AES; y

una unidad de ejecución que incluye lógica de ejecución AES para ejecutar al menos una primera instrucción AES de la pluralidad de instrucciones AES para realizar el ciclo de la operación de descifrado AES, el ciclo de la operación de descifrado AES utiliza la clave de ciclo del primer registro de origen para descifrar los datos de entrada del segundo registro de origen y almacena un resultado del ciclo de la operación de descifrado AES en un primer registro de destino.

10. El procesador (101) de la reivindicación 9, en donde el ciclo de la operación de descifrado AES realizado en respuesta a la primera instrucción AES incluye:

una operación de sustitución a ser realizada en los datos de entrada, la operación de sustitución incluye una búsqueda inversa de caja de sustitución, caja-S;

una operación inversa de desplazar filas;

una operación inversa de mezclar columnas; y

una operación de agregar clave de ciclo en la que una función O exclusiva utiliza datos de la clave de ciclo.

11. El procesador de la reivindicación 9 o 10, en donde la unidad de ejecución ejecuta una segunda instrucción AES para realizar un ciclo final de la operación de descifrado AES, el ciclo final de la operación de descifrado AES utiliza una clave de ciclo correspondiente al ciclo final de la operación de descifrado AES para descifrar los datos de entrada a ser descifrados mediante el ciclo final de la operación de descifrado AES y almacena un resultado final de descifrado de la operación de descifrado AES en un registro de destino, en donde el ciclo final de la operación de descifrado AES incluye:

una operación de sustitución a ser realizada en los datos de entrada a ser descifrados mediante el ciclo final de la operación de descifrado AES, la operación de sustitución incluye una búsqueda inversa de caja-S; y

una operación inversa de desplazar filas; y

una operación de agregar clave de ciclo en la que una función O exclusiva utiliza datos de la clave de ciclo correspondiente al ciclo final de la operación de descifrado AES.

12. El procesador de una cualquiera de las reivindicaciones 9 a 11, en donde el procesador es un procesador de propósito general, en donde la pluralidad de instrucciones AES incluye más de cuatro instrucciones AES que comprende cada una un opcode diferente y en donde la unidad de ejecución ejecuta microcódigo para ejecutar la primera instrucción AES.

13. Un sistema que comprende:

el procesador de una cualquiera de las reivindicaciones 9 a 12; y

un dispositivo de almacenamiento acoplado al procesador.

14. El sistema de la reivindicación 13, que comprende además al menos un controlador de interfaz de red acoplado al procesador para procesar paquetes de datos y en donde el dispositivo de almacenamiento se dispone como una matriz redundante de discos independientes, RAID.

15. Un sistema que comprende:

el procesador de una cualquiera de las reivindicaciones 9 a 12;

un controlador de memoria para acoplar el procesador a una memoria dinámica de acceso aleatorio, DRAM; y

un controlador de entrada/salida, E/S, para acoplar el procesador a uno o más dispositivos.

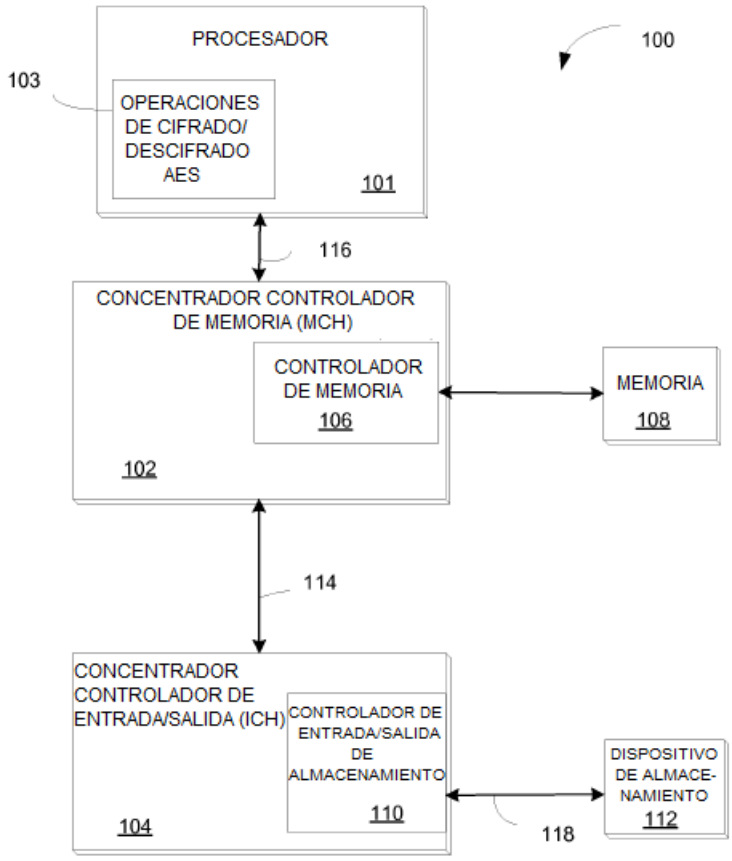
PROCESADOR
100
103
OPERACIONES DE CIFRADO/ DESCIFRADO AES
101
116
CONCENTRADOR CONTROLADOR DE MEMORIA (MCH)
CONTROLADOR DE MEMORIA
106
MEMORIA
108
102
114
CONCENTRADOR CONTROLADOR DE ENTRADA/SALIDA (ICH)
CONTROLADOR DE ENTRADA/SALIDA DE ALMACENAMIENTO
110
DISPOSITIVO DE ALMACE-NAMIENTO
112
104
118

FIG. 1

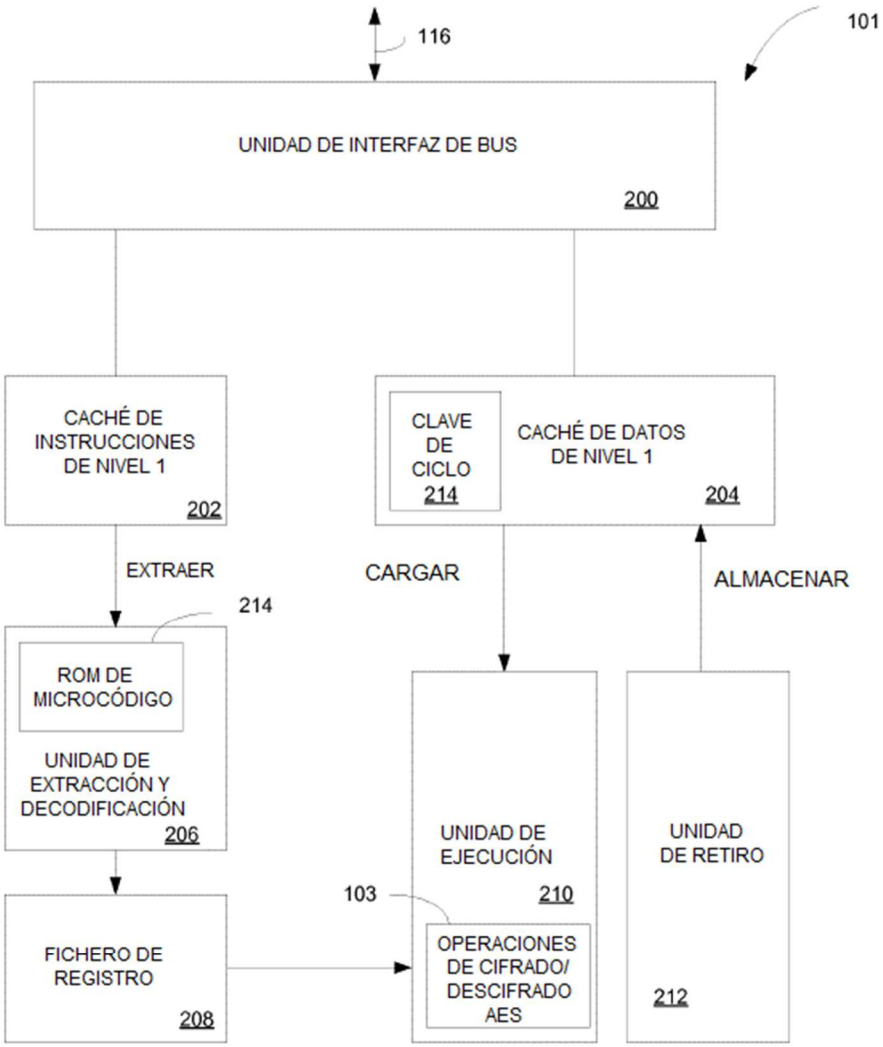
116
101
UNIDAD DE INTERFAZ DE BUS
200
CACHÉ DE INSTRUCCIONES DE NIVEL 1
202
CLAVE DE CICLO
214
CACHÉ DE DATOS DE NIVEL 1
204
EXTRAER
CARGAR
ALMACENAR
214
ROM DE MICROCÓDIGO
UNIDAD DE EXTRACCIÓN Y DECODIFICACIÓN
206
UNIDAD DE EJECUCIÓN
210
UNIDAD DE RETIRO
212
103
OPERACIONES DE CIFRADO/ DESCIFRADO AES
FICHERO DE REGISTRO
208

FIG. 2

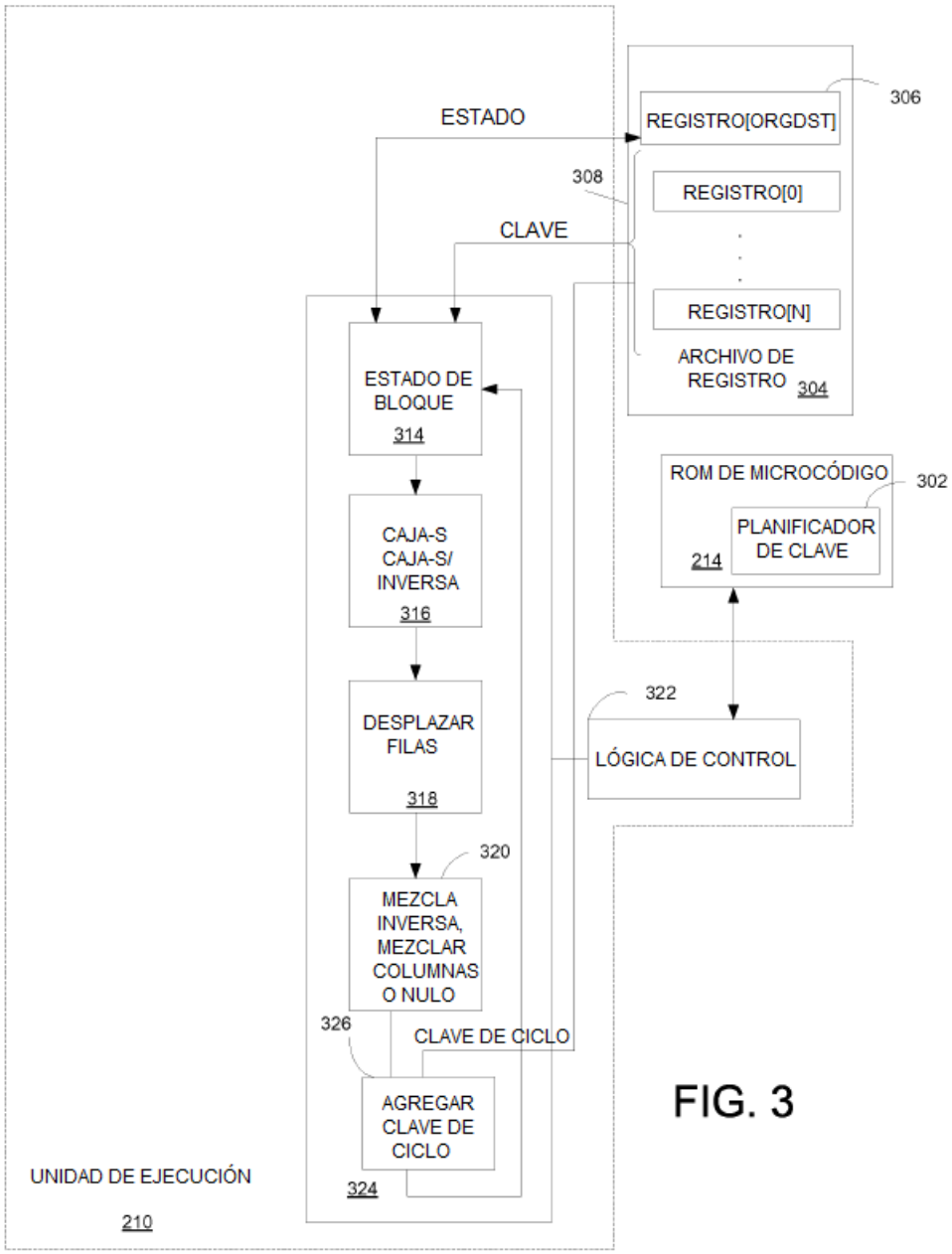
ESTADO
306
REGISTRO[ORGDST]
308
REGISTRO[0]
CLAVE
REGISTRO[N]
ARCHIVO DE REGISTRO 304
ESTADO DE BLOQUE 314
ROM DE MICROCÓDIGO
302
PLANIFICADOR DE CLAVE
214
CAJA-S CAJA-S/ INVERSA 316
DESPLAZAR FILAS 318
322
LÓGICA DE CONTROL
320
MEZCLA INVERSA, MEZCLAR COLUMNAS O NULO
326
CLAVE DE CICLO
AGREGAR CLAVE DE CICLO
324
UNIDAD DE EJECUCIÓN
210

FIG. 3

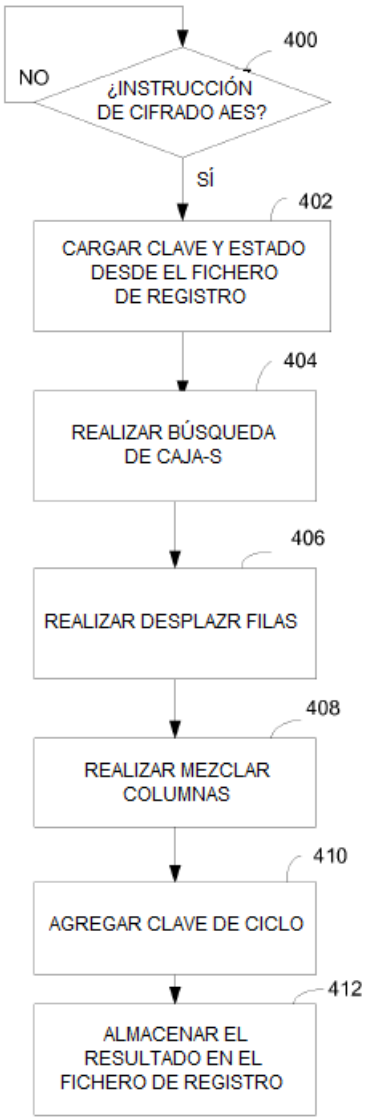
400
NO
¿INSTRUCCIÓN DE CIFRADO AES?
SÍ
402
CARGAR CLAVE Y ESTADO DESDE EL FICHERO DE REGISTRO
404
REALIZAR BÚSQUEDA DE CAJA-S
406
REALIZAR DESPLAZR FILAS
408
REALIZAR MEZCLAR COLUMNAS
410
AGREGAR CLAVE DE CICLO
412
ALMACENAR EL RESULTADO EN EL FICHERO DE REGISTRO

FIG. 4

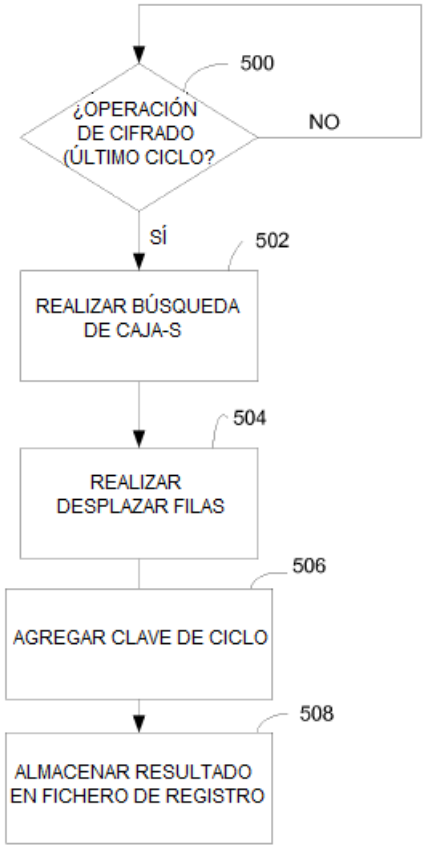
500
¿OPERACIÓN DE CIFRADO ¿ÚLTIMO CICLO?
NO
SÍ
502
REALIZAR BÚSQUEDA DE CAJA-S
504
REALIZAR DESPLAZAR FILAS
506
AGREGAR CLAVE DE CICLO
508
ALMACENAR RESULTADO EN FICHERO DE REGISTRO

FIG. 5

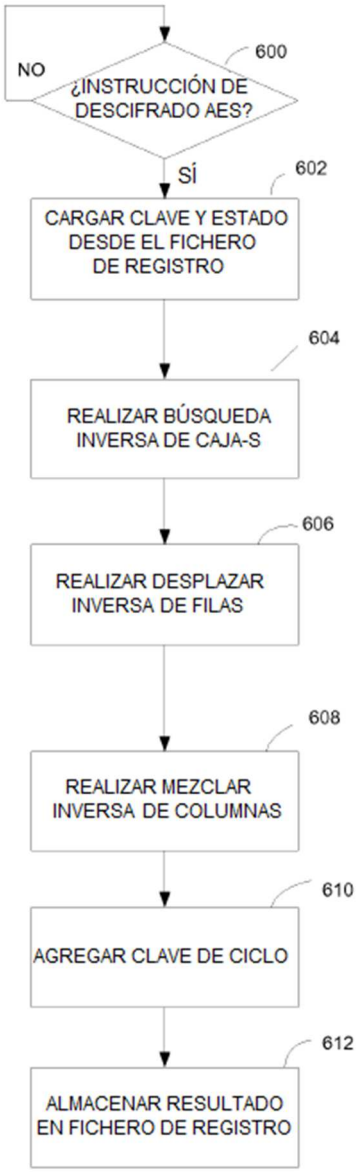
NO
600
¿INSTRUCCIÓN DE DESCIFRADO AES?
SÍ
602
CARGAR CLAVE Y ESTADO DESDE EL FICHERO DE REGISTRO
604
REALIZAR BÚSQUEDA INVERSA DE CAJA-S
606
REALIZAR DESPLAZAR INVERSA DE FILAS
608
REALIZAR MEZCLAR INVERSA DE COLUMNAS
610
AGREGAR CLAVE DE CICLO
612
ALMACENAR RESULTADO EN FICHERO DE REGISTRO

FIG. 6

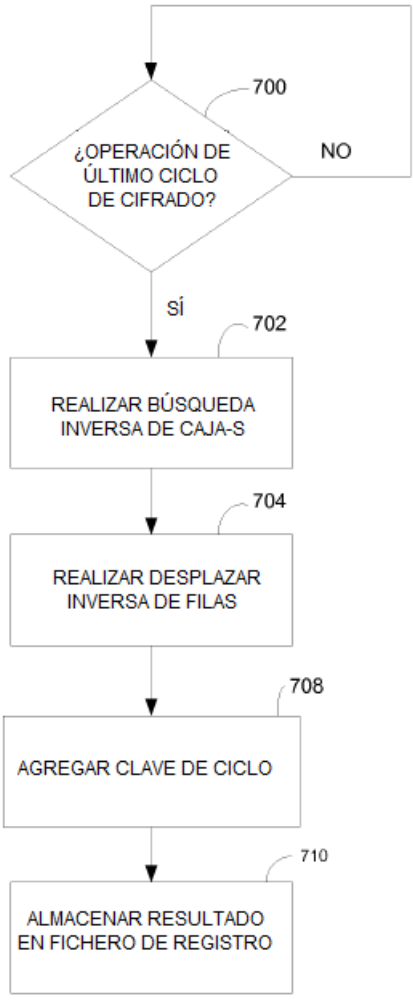
700
¿OPERACIÓN DE ÚLTIMO CICLO DE CIFRADO?
NO
SÍ
702
REALIZAR BÚSQUEDA INVERSA DE CAJA-S
704
REALIZAR DESPLAZAR INVERSA DE FILAS
708
AGREGAR CLAVE DE CICLO
710
ALMACENAR RESULTADO EN FICHERO DE REGISTRO

FIG. 7

dest:= aes_key_round(origen2, origen1), key_select_modifier																
PUERTOS						BANDERAS DE ENTERO						BANDERAS DE COMA FLOTANTE				
0	1	2	3	4	5	O	S	Z	A	P	C	Pre C	C3	C2	C1	C0
-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-

UNIDAD DE EJECUCIÓN	UNIDAD AES
EVENTOS DE ENTERO	-
EVENTOS DE OPERACIONES PREVIAS	N/D
EVENTOS DE OPERACIONES POSTERIORES	N/D

FIG. 8