(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 565 816**

(51) Int. CI.:

H04L 9/06 (2006.01)
G09C 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.03.2003 E 03755263 (5)**

(97) Fecha y número de publicación de la concesión europea: **24.02.2016 EP 1507247**

(54) Título: **Aparato de conversión de datos y método de conversión de datos**

(30) Prioridad:

23.05.2002 JP 2002148786

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.04.2016

(73) Titular/es:

MITSUBISHI DENKI KABUSHIKI KAISHA (100.0%)
7-3, MARUNOUCHI 2-CHOME CHIYODA-KU
TOKYO 100-8310, JP

(72) Inventor/es:

KASUYA, TOMOMIC;
MATSUI, MITSURUC y
ICHIKAWA, TETSUYAC

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Aparato de conversión de datos y método de conversión de datos

Campo técnico

La presente invención se refiere a un aparato de conversión de datos para cifrado de datos y/o descifrado de datos y un método de los mismos.

Antecedentes de la técnica

Se dará ahora una descripción de la técnica relacionada.

La Fig. 56 es un diagrama que ilustra la configuración y operación de un aparato de conversión de datos relacionado.

Como se muestra en la Fig. 56, el aparato de conversión de datos para cifrado de bloques consta de un generador de claves 20 y un aleatorizador de datos 30.

El generador de claves 20 es una unidad de generación de claves que genera una clave para cifrado/descifrado de datos.

El aleatorizador de datos 30 es una unidad que cifra y descifra datos de entrada.

El generador de claves 20 consta de un generador de claves intermedias 40 y un programador de claves 210. El generador de claves intermedias 40 es una unidad que recibe una clave secreta y genera una clave intermedia (Clave KL) y una clave de salida (Clave KA) basada en la clave secreta recibida. El programador de claves 210 que recibe las claves intermedias (Clave KL) y las claves de salida (Clave KA) generadas en el generador de claves intermedias 40 (Clave KLL, Clave KLH, Clave KAL y Clave KAH) y programa una clave a ser alimentada al aleatorizador de datos 30 entre las claves introducidas. De esta manera, en el generador de claves 20, las claves se generan y programan en el generador de claves intermedias 40 y el programador de claves 210, respectivamente.

El aleatorizador de datos 30, tras la recepción de P (texto plano), realiza una conversión de datos de los datos para cifrado y entonces saca los datos convertidos como C (texto cifrado). Tras la recepción de P (texto cifrado), por otra parte, el aleatorizador de datos 30 realiza una conversión de datos de los datos para descifrado de datos y entonces saca los datos convertidos como C (texto descifrado). El aleatorizador de datos 30 realiza de esta manera el proceso de cifrado de datos y el proceso de descifrado de datos.

En el aleatorizador de datos 30, se conectan en serie un convertidor principal 320 y un subconvertidor 330.

El convertidor principal 320 es una unidad que realiza conversión no lineal. Más particularmente, el convertidor 320 se dota con una función F que realiza conversión de datos no lineal durante una vuelta o múltiples vueltas o una parte de la función F y realiza una conversión no lineal de datos usando la función F o la parte de la función F. La Fig. 57 muestra el convertidor principal 320 que se dota con la función F durante una o más vueltas.

El subconvertidor 330 se dota con al menos una de una unidad de convertidor de datos (FL) que realiza una conversión lineal de datos y una unidad de inversor de datos (FL^{-1}) que realiza una conversión que es inversa a la conversión realizada por la unidad de convertidor de datos y hace una conversión lineal de datos de entrada usando una clave de entrada por medio de la unidad de convertidor de datos (FL) o la unidad de inversor de datos (FL^{-1}).

El selector 310 es un selector que selecciona una señal de entre las señales de entrada del convertidor principal 320, el subconvertidor 330, P (texto plano o texto cifrado) y una clave. El selector 310 mostrado en la Fig. 56 se dota con un selector que selecciona una señal de entre cuatro señales de entrada, que es equivalente a tres selectores 2-1, cada uno de los cuales saca una señal de salida de entre dos señales de entrada.

El registro aritmético 350 es una memoria que mantiene datos que se sacan como el convertidor principal 320, el subconvertidor 330 y C (texto cifrado o texto descifrado) durante un periodo de tiempo predeterminado.

De esta manera, el aleatorizador de datos 30 cifra/descifra los datos de entrada de P (texto plano o texto cifrado) a través de repeticiones de conversión no lineal mediante el convertidor principal 320 y la conversión lineal mediante el subconvertidor 330 varias veces alternativamente y entonces saca C (texto cifrado o texto descifrado).

Se dará ahora una descripción de la configuración interna del convertidor principal 320.

La Fig. 57 muestra la configuración interna del convertidor principal 320. El convertidor principal 320 de la Fig. 57 se compone de seis unidades de función F. Suponiendo aquí que cada una de las unidades de función F se configura con un circuito que se diseña para un proceso de función F de una vuelta, el convertidor principal 320 de la Fig. 57 entonces es para realizar la conversión de datos no lineal basada en la función F durante seis vueltas.

Con respecto al circuito para el proceso de función F de seis vueltas, el convertidor principal 320 se puede dotar con seis circuitos de proceso de función F o de otro modo un único circuito de proceso de función F con repeticiones de seis veces el proceso de función F para terminar logrando el procesamiento de datos basado en la función F seis veces.

En el convertidor principal 320, los datos superiores divididos de datos de entrada se introducen a una unidad de función F 321a en primer lugar. Una clave 1 que se programó por el programador de claves 210 también se introduce a la misma. En la unidad de función F 321a, los datos de entrada superiores se convierte no linealmente mediante el uso de la clave que se mencionó antes. En un circuito EXOR 322a, los datos convertidos no linealmente se someten a una operación XOR con los datos de entrada inferiores. Los datos sacados desde el circuito EXOR 322a se introducen a una unidad de función F 321b. La unidad de función F 321b, como la unidad de función F 321a, realiza la conversión no lineal y los datos convertidos entonces se someten a una operación XOR con los datos introducidos superiores en un circuito EXOR 322b. Los datos sacados desde el circuito EXOR 322b se introduce a una unidad de función F 321c. De esta manera, el mismo proceso que el realizado por la unidad de función F 321a y el circuito EXOR 322a se realiza por la unidad de función F 321b y el circuito EXOR 322b, por la unidad de función F 321c y un circuito EXOR 322c, mediante una unidad de función F 321d y un circuito EXOR 322d, mediante una unidad de función F 321e y un circuito EXOR 322e y mediante una unidad de función F 321f y un circuito EXOR 322f, respectivamente. De esta manera, la conversión no lineal basada en una función F de seis vueltas se realiza (o la conversión no lineal basada en una función F de una vuelta se repite seis veces) de esa manera y entonces se sacan los datos convertidos.

La estructura para el proceso de conversión no lineal antes mencionado se llama estructura FEISTEL, que se caracteriza por que los datos superiores y los datos inferiores se intercambian y sacan recibiendo uno de los datos superiores divididos y datos inferiores divididos, datos de conversión no lineal recibidos, sacando uno de los datos superiores y los datos inferiores convertidos, sometiendo a una operación XOR entre uno de los datos superiores y los datos inferiores sacados y el otro de los datos superiores y los datos inferiores, intercambiando datos sometidos a una operación XOR y el otro de los datos superiores y los datos inferiores que no se introdujeron a la unidad de función F y sacando los datos inferiores y los datos superiores intercambiados.

Las estructuras típicas para aleatorización de datos son la estructura FEISTEL y la estructura SPN (Red de Sustitución-Permutación). El convertidor principal 320 con la estructura SPN se dice que sobresale en el procesamiento paralelo. Con la estructura FEISTEL, el convertidor principal 320 se dice que sobresale en reducción de tamaño de hardware.

Señalar que la estructura SPN, a diferencia de la estructura FEISTEL en la que se dividen los datos de entrada, se estructura de manera que se repite una función F compuesta de una capa S (capa no lineal) y una capa P (capa lineal).

Se dará ahora una descripción de la estructura interna del subconvertidor 330.

La Fig. 58 es un diagrama que ilustra circuitos que componen el subconvertidor 330.

El subconvertidor 330 de la Fig. 58 se dota con una unidad de convertidor de datos 50 y una unidad de inversor de datos 70.

En la unidad de convertidor de datos 50, se realiza una operación AND lógica entre los datos de 32 bits superiores de datos de entrada de 64 bits y una clave 1 en un circuito AND 54, un resultado de la cual se somete entonces a desplazamiento de rotación de un bit a la izquierda. Entonces, en un circuito EXOR 55, una entrada se somete a una operación XOR con los 32 bits inferiores de los datos de entrada, un resultado de la cual se saca como una señal de salida de 32 bits inferior y también se introduce a un circuito OR 57. Entonces, en el circuito OR 57, una entrada se somete a una operación OR lógica con una clave 2, un resultado de la cual entonces se somete a una operación XOR con los datos de 32 bits superiores de los datos de entrada en un circuito EXOR 56, un resultado de la cual se saca como una señal de salida de 32 bits superiores. De esta manera, los datos de entrada de 64 bits se convierten linealmente y entonces se sacan como una señal de salida de 64 bits.

En la unidad de inversor de datos 70, se realiza una operación OR lógica entre los datos de 32 bits inferiores de datos de entrada de 64 bits y una clave 3 en un circuito OR 74, un resultado de la cual entonces se somete a una operación XOR con los 32 bits superiores de los datos de entrada en un circuito EXOR 75, un resultado de la cual se saca como una señal de salida de 32 bits superiores y también se introduce a un circuito AND 77. En el circuito AND 77, se somete una entrada a una operación AND lógica con una clave 4, un resultado de la cual se somete entonces a desplazamiento de rotación de un bit a la izquierda. Entonces, en un circuito EXOR 76, una entrada se somete a una operación XOR con los datos de 32 bits inferiores de los datos de entrada, un resultado de la cual se saca como una señal de salida de 32 bits inferiores. De esta manera, los datos de entrada de 64 bits se convierten linealmente en la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 y entonces se sacan como una señal de salida de 64 bits. Señalar que la clave 1 hasta la clave 4 se alimentan por el programador de claves 210.

La Fig. 59 es un diagrama que muestra un circuito compartido por la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 como un ejemplo del subconvertidor 330.

Con la Fig. 59, cuando se introduce una señal de conmutación para conmutar entre la unidad de convertidor de datos 50 y la unidad de inversor de datos 70, se conmutan la unidad de convertidor de datos 50 y la unidad de inversor de datos 70. Más específicamente, en el circuito compartido de la Fig. 59 cuando se recibe la señal de conmutación, un selector 2-1 99a conmuta entre una señal de entrada A y una señal de entrada E y un selector 2-1 99b conmuta entre una señal de entrada C y una señal de entrada F.

Se dará una descripción del caso en el que el circuito compartido actúa como la unidad de convertidor de datos 50 en primer lugar.

El selector 2-1 99a selecciona la señal de entrada A de entre la señal de entrada E y la señal de entrada A y saca la señal como una señal de salida B. Entonces, en un circuito AND 101, una entrada se somete a una operación AND lógica con la clave 1, un resultado de la cual se somete entonces a desplazamiento de rotación de un bit a la izquierda. Entonces, en un circuito EXOR 91, una entrada se somete a una operación XOR con los 32 bits inferiores de los datos de entrada, un resultado de la cual se saca como una señal de salida de 32 bits inferiores y también se introduce al selector 2-1 99b como la señal de entrada C. El selector 2-1 99b selecciona la señal de entrada C de entre la señal de entrada C y la señal de entrada F y saca la señal C como una señal de salida D. Entonces, en un circuito OR 92, se realiza una operación OR lógica entre la señal de salida D y la clave 2, un resultado de la cual se somete entonces a una operación XOR con los datos de 32 bits superiores de los datos de entrada en un circuito EXOR 93, un resultado de la cual se saca entonces como una señal de salida de 32 bits superiores.

Entonces se dará una descripción del caso en el que el circuito compartido actúa como la unidad de inversión de datos 70.

El selector 2-1 99b selecciona la señal de entrada F de entre la señal de entrada C y la señal de entrada F y saca la señal de entrada F como la señal de salida D. Entonces, el circuito OR 92 realiza una operación OR lógica entre la señal de salida D y la clave 2, un resultado de la cual se somete a una operación XOR con los 32 bits superiores de los datos de entrada en el circuito EXOR 93, un resultado de la cual se saca como una señal de salida de 32 bits superiores y también se introduce al selector 2-1 99a como la señal de entrada E. El selector 2-1 99a selecciona la señal de entrada E de entre la señal de entrada A y la señal de entrada E y saca la señal de entrada E como la señal de salida B. Entonces, en el circuito AND 101, se realiza una operación OR lógica entre la señal de salida B y la clave 1, un resultado de la cual se somete entonces a desplazamiento de rotación de un bit a la izquierda, un resultado de lo cual entonces se somete a una operación XOR con los 32 bits inferiores de los datos de entrada en el circuito EXOR 91, un resultado de la cual se saca como una señal de salida de 32 bits inferiores.

La Fig. 60, en contraste con el aparato de conversión de datos de la Fig. 56, es un diagrama que ilustra un aparato de conversión de datos en el que el convertidor principal 320 se dota con $1/2^x$ ($x \geq 1$) de la función F, que se diseña para procesar la función F durante menos de una vuelta.

En el caso donde el convertidor principal 320 se dote con una función 1/2F, por ejemplo, se puede realizar un proceso de dos ciclos por medio del camino desde el convertidor principal 320 hasta el subconvertidor 330, el selector 310, el registro aritmético 350, entonces de vuelta al convertidor principal 320. Esto permite que sea logrado un proceso de conversión de datos no lineal basada en una función F de una vuelta. Para implementar tal proceso, el aparato de conversión de datos de la Fig. 60, en contraste con el convertidor de la Fig. 56, se añade con el camino desde el registro aritmético 350 al selector 310.

Se dará ahora una descripción de la operación del convertidor principal 320 por medio del camino desde el registro aritmético 350 al selector 310.

La Fig. 61 ilustra la configuración interna del convertidor principal 320.

Como se muestra en la Fig. 61, el convertidor principal 320 se compone de 12 unidades de función F, cada una de las cuales procesa la función F durante menos de una vuelta, por ejemplo, 1/2 de la función F (función 1/2F). El convertidor principal 320 de la Fig. 61 realiza conversión de datos usando una unidad de función F 1321a, una unidad de función F 1321b, un circuito EXOR 1322a y un circuito EXOR 1322b, mientras que el convertidor principal 320 de la Fig. 57 realiza la misma conversión de datos usando la unidad de función F 321a y el circuito EXOR 322a.

Con referencia al convertidor principal 320 de la Fig. 61, se explicará en primer lugar el proceso de primera vuelta. Los datos superiores divididos a partir de los datos de entrada superiores se introducen a la unidad de función F 1321a. Una clave 1H, que se compone de los bits superiores de la clave 1 programada por el programador de claves 210, también se introduce a la unidad de función F 1321a. La unidad de función F 1321a convierte no linealmente los datos superiores usando la clave 1H. Entonces, los datos convertidos se introducen al circuito EXOR 1322a y se someten a una operación XOR con los datos superiores divididos a partir de los datos de entrada inferiores.

Los datos sacados desde el circuito EXOR 1322a se mantienen en el registro aritmético 350 como datos intermedios hasta que se hace un procesamiento de datos en el circuito EXOR 1322b.

Entonces, se explicará un proceso de segunda vuelta. A partir de los datos de entrada superiores, los datos inferiores divididos se introducen a la unidad de función F 1321b. Una clave 1L, que se compone de los bits

inferiores de la clave 1 programada por el programador de claves 210, también se introduce a la unidad de función F 1321b. La unidad de función F 1321b realiza una conversión no lineal de los datos inferiores usando la clave 1L. Entonces, los datos convertidos se introducen al circuito EXOR 1322b.

Ahora, los datos intermedios, que son los datos de salida desde el circuito EXOR 1322a y se mantienen en el registro aritmético 350, van a ser introducidos al circuito EXOR 1322b. Entonces, se necesita el camino desde el registro aritmético 350 al selector 310. Más específicamente, el camino desde el registro aritmético 350 al selector 310 permite introducir los datos intermedios mantenidos en el registro aritmético 350 al selector 310. El selector 310 selecciona los datos intermedios recibidos. Los datos intermedios se introducen entonces al convertidor principal 320 a través del registro aritmético 350 y entonces se someten a una operación XOR con datos de salida desde la unidad de función F 1321b por el circuito EXOR 1322b. Los datos de salida desde el circuito EXOR 1322b se introducen a la función F 1321c.

De esta manera, el mismo proceso que el realizado por la unidad de función F 1321a, el circuito EXOR 1322a, la unidad de función F 1321b y el circuito EXOR 1322b se realiza por una unidad de función F 1321c, un circuito EXOR 1322c, una unidad de función F 1321d y un circuito EXOR 1322d, por una unidad de función F 1321e, un circuito EXOR 1322e, una unidad de función F 1321f y un circuito EXOR 1322f, por una unidad de función F 1321g, un circuito EXOR 1322g, una unidad de función F 1321h y un circuito EXOR 1322h, por una unidad de función F 1321i, un circuito EXOR 1322i, una unidad de función F 1321j y un circuito EXOR 1322j y por una unidad de función F 1321k, un circuito EXOR 1322k, una unidad de función F 1321l y un circuito EXOR 1322l, respectivamente. Después de procesar de esta manera la conversión de datos no lineal de 12 vueltas por las unidades de función F (o repetir 12 veces), se sacan los datos convertidos.

Problema 1.

Con referencia a los aparatos de conversión de datos de la Fig. 56 y la Fig. 60, el generador de claves 20 usa parte del convertidor principal 320 y parte del subconvertidor 330 para generar una clave usada para cifrado/descifrado de datos. El propósito de usar parte del convertidor principal 320 y parte del subconvertidor 330 es reducir el tamaño total del aparato de conversión de datos.

Con esta operación de generación de claves tratada más tarde en detalle, a fin de generar una clave usando de esta manera parte del convertidor principal 320 y parte del subconvertidor 330, se necesita un camino para introducir la clave intermedia (Clave KL) sacada desde el registro de claves KL 240 en el selector 310 como se muestra en la Fig. 56. Este aumento del camino desde el registro de claves KL 240 al selector 310 es una causa que impide que el aparato de conversión de datos se haga más pequeño.

Esto también aumenta el número de señales de entrada al selector 310 por medio del camino desde el registro de claves KL 240 al selector 310, que causa un aumento en el número de selectores que componen el selector 310. Esto es otra causa que impide que el aparato de conversión de datos se haga más pequeño.

Como se mencionó anteriormente, la conversión de datos basada en una función F de una vuelta en dos o más ciclos se acompaña por la necesidad de introducir los datos intermedios mantenidos durante un periodo de tiempo dado en el convertidor principal 320. Este aumento del camino para transferir los datos intermedios desde el registro aritmético 350 al selector 310 aún es otra causa que impide que el aparato de conversión de datos se haga más pequeño.

Adicionalmente, el aumento en el número de señales de entrada al selector 310 por medio del camino desde el registro aritmético 350 al selector 310 causa un aumento en el número de selectores que componen el selector 310. Esto es aún otra causa que impide que el aparato de conversión de datos se haga más pequeño.

Problema 2.

Con referencia a los aleatorizadores de datos 30 de los aparatos de conversión de datos mostrados en la Fig. 56 y la Fig. 60, el convertidor principal 320 y el subconvertidor 330 se conectan en serie. Esto determina la frecuencia de operación únicamente por el camino desde el convertidor principal 320 a través del subconvertidor 330, el selector 310, el registro aritmético 350 entonces de vuelta al convertidor principal 320, lo cual impide que la frecuencia de operación sea mejorada. Por lo tanto, ha sido un deseo aumentar la frecuencia de operación haciendo un camino máximo para procesamiento de datos más corto en el aleatorizador de datos 30, mejorando por ello la velocidad de flujo máximo de manera notable. Adicionalmente, no se proporciona ningún camino que permita a los datos sacados desde el selector 310 y entonces al registro aritmético 350 ir dentro del subconvertidor 330 sin pasar a través del convertidor principal 320. Por lo tanto, no se permite una respuesta flexible a un cambio en la configuración interna del aparato de conversión de datos, lo que provoca poca flexibilidad en la operación en general.

Como se mencionó anteriormente, en el caso donde la conversión de datos basada en la función F de una vuelta se realice en dos o más ciclos, es parte de los datos de entrada (1/2 de los datos de entrada con una función 1/2F) que se convierten en un ciclo. Esto requiere que el camino en el aleatorizador de datos 30 para transferir los datos convertidos de la parte de los datos de entrada al registro aritmético 350 sea mantenido en el mismo y entonces transferir los datos convertidos al subconvertidor 330 después de un periodo de tiempo dado.

O de otro modo, se requiere el camino de transferencia en el convertidor principal 320 para transferir los datos convertidos al subconvertidor 330 pasando a través del convertidor principal 320 después de un periodo de tiempo dado.

Adicionalmente, con el circuito compartido por la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 mostrado en la Fig. 59, el camino A→B→C→D→E→B→C… corresponde a un circuito en bucle. Esto requiere que el circuito compartido diseñado no llegue a ser un circuito de transmisión en una implementación práctica cuando está afectado por el recorrido de la señal causado por diferencias en el retardo de propagación de señales de conmutación, ruido, etc. Otro problema es que las herramientas sintéticas lógicas no son aplicables a tal circuito que tiene un circuito en bucle (circuito en BUCLE DE REALIMENTACIÓN) y por lo tanto la síntesis lógica no se puede lograr eficientemente.

AOKI K ET AL: “THE 128-BITS BLOCK CIPHER CAMELLIA”, ACTAS DEL IEICE SOBRE FUNDAMENTOS DE ELECTRÓNICA, COMUNICACIONES Y CIENCIAS INFORMÁTICAS, SOCIEDAD DE CIENCIAS DE INGENIERÍA, TOKIO, JP, vol. E85-A, nº 1, 1 de enero de 2002 (01-01-2002), páginas 11-24, XP001117312, ISSN: 0916-8508 describen un cifrado de bloque de 128 bits que soporta longitudes de clave de 128, 192, 256 bits. Esta técnica usa una estructura Feistel de 18 vueltas para claves de 128 bits y una estructura Feistel de 24 vueltas para claves de 192 y 256 bits, con blanqueos de entrada/salida adicionales y funciones lógicas llamadas función FL y función FL^{-1} insertadas cada 6 vueltas.

Además, AKASHI SATOH ET AL: “A Compact Rijndael Hardware Architecture with S-Box Optimization”, PROCESAMIENTO Y APLICACIONES PARALELAS Y DISTRIBUIDAS: SEGUNDO SIMPOSIO INTERNACIONAL, ACTAS WA 2004, HONG KONG, CHINA, 13-15 DE DICIEMBRE DE 2004 (EN: APUNTES EN CIENCIAS INFORMÁTICAS), SPRINGER, DE, 1 de enero de 2001 (01-01-2001), páginas 239-254, XP007906471, DOI: DOI: 10.1007/3-540-45682-1 ISBN: 978-3-540-24128-7, describen estructuras hardware compactas y de alta velocidad y métodos de optimización lógica para el algoritmo AES Rijndael. Los caminos de datos de cifrado y descifrado se combinan y se reutilizan todos los componentes aritméticos. Introduciendo un nuevo campo compuesto, también se optimiza la estructura de Caja S.

Es un objeto de la presente invención reducir el tamaño de un aparato de conversión de datos.

Es otro objeto de la presente invención mejorar la frecuencia de operación de un aparato de conversión de datos.

Descripción de la invención

Para resolver los objetos mencionados anteriormente, un aparato de conversión de datos según la presente invención comprende los rasgos de la reivindicación 1 y un método de conversión de datos según la presente invención comprende los rasgos de la reivindicación 11. Las realizaciones preferidas del aparato de conversión de datos se definen en las reivindicaciones dependientes.

Breve descripción de los dibujos

La Fig. 1 es un diagrama que ilustra una configuración de un aparato de conversión de datos según una primera realización.

La Fig. 2 es un diagrama que ilustra una operación de un generador de claves intermedias 40 que genera una clave de salida a partir de una clave intermedia con una clave de 128 bits.

La Fig. 3 es un diagrama que ilustra una configuración interna y operación de un programador de claves 210.

La Fig. 4 es un diagrama que ilustra una operación de un aleatorizador de datos 30 para cifrado/descifrado.

La Fig. 5 es un diagrama que ilustra una configuración interna y operación de una unidad de función F 321.

La Fig. 6 es un diagrama que ilustra una configuración de un aparato de conversión de datos en el que un convertidor principal 320 y un subconvertidor 330 de la Fig. 1 se disponen a la inversa.

La Fig. 7 es un diagrama que ilustra una configuración de un aparato de conversión de datos, en el que el convertidor principal 320 y el subconvertidor 330 se disponen en paralelo.

La Fig. 8 es un diagrama que ilustra una configuración interna de un selector 6-1 KL 220 y un selector 6-1 KA 230 en el generador de claves intermedias 40.

La Fig. 9 es un diagrama que ilustra otra configuración ejemplo del generador de claves intermedias 40.

La Fig. 10 es un diagrama que ilustra una configuración interna del subconvertidor 330 en el que la unidad de convertidor de datos 50 se dota con una función de transferencia de claves.

La Fig. 11 es un diagrama que ilustra una configuración interna del subconvertidor 330 en el que la unidad de inversor de datos 70 se dota con la función de transferencia de claves.

La Fig. 12 es un diagrama que ilustra una configuración interna del subconvertidor 330 en el que la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 se dotan ambas con la función de transferencia de claves.

La Fig. 13 es un diagrama que ilustra una configuración interna del subconvertidor 330 en el que la unidad de convertidor de datos 50 se dota con una función de transferencia de datos según una segunda realización.

La Fig. 14 es un diagrama que ilustra una configuración interna del subconvertidor 330 en el que la unidad de inversor de datos 70 se dota con la función de transferencia de datos.

La Fig. 15 es un diagrama que ilustra una configuración interna del subconvertidor 330 en el que la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 se dotan ambas con la función de transferencia de datos.

La Fig. 16 es un diagrama que ilustra una configuración interna del subconvertidor 330 en el que la unidad de convertidor de datos 50 se dota con la función de transferencia de claves y la función de transferencia de datos y la unidad de inversor de datos 70 se dota con la función de transferencia de claves según una tercera realización.

La Fig. 17 es un diagrama que ilustra una configuración interna del subconvertidor 330 en el que la unidad de inversor de datos 70 se dota con la función de transferencia de claves y la función de transferencia de datos y la unidad de convertidor de datos 50 se dota con la función de transferencia de claves.

La Fig. 18 es un diagrama que ilustra una configuración interna del subconvertidor en el que la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 se dotan ambas con la función de transferencia de claves y la función de transferencia de datos.

La Fig. 19 es un diagrama que ilustra una configuración interna del subconvertidor 330 en el que la unidad de convertidor de datos 50 se dota con la función de transferencia de claves y la función de transferencia de datos.

La Fig. 20 es un diagrama que ilustra una configuración interna del subconvertidor 330 en el que la unidad de inversor de datos 70 se dota con la función de transferencia de claves y la función de transferencia de datos.

La Fig. 21 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 se dota tanto con la función de transferencia de claves como con la función de transferencia de datos y la unidad de inversor de datos 70 se dota con la función de transferencia de datos.

La Fig. 22 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de inversor de datos 70 se dota con la función de transferencia de claves y la función de transferencia de datos y la unidad de convertidor de datos 50 se dota con la función de transferencia de datos.

La Fig. 23 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 se dota con la función de transferencia de datos y la unidad de inversor de datos 70 se dota con la función de transferencia de claves.

La Fig. 24 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 se dota con la función de transferencia de claves y la unidad de inversor de datos 70 se dota con la función de transferencia de datos.

La Fig. 25 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de inversor de datos 70 y la unidad de convertidor de datos 50 se conectan en serie y la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 se dotan ambas con la función de transferencia de datos.

La Fig. 26 muestra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 de la Fig. 25 conmutan la posición de las mismas.

La Fig. 27 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 se conectan en serie y la unidad de convertidor de datos 50 se dota con la función de transferencia de claves y la función de transferencia de datos y la unidad de inversor de datos 70 se dota con la función de transferencia de datos.

La Fig. 28 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 de la Fig. 27 conmutan la posición de las mismas.

La Fig. 29 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 se conectan en serie y la unidad de convertidor de datos 50 se dota con

la función de transferencia de datos y la unidad de inversor de datos 70 se dota con la función de transferencia de claves y la función de transferencia de datos.

La Fig. 30 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 de la Fig. 29 conmutan el orden de las mismas.

La Fig. 31 es un diagrama que ilustra una configuración del subconvertidor 330 en el que una 1/2 unidad de subconvertidor 90 se añade con la función de transferencia de claves y la función de transferencia de datos según una cuarta realización.

La Fig. 32 es un diagrama que ilustra una configuración del subconvertidor en el que la 1/2 unidad de subconvertidor 90 se añade con la función de transferencia de datos.

La Fig. 33 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la 1/2 unidad de subconvertidor 90 se añade con la función de transferencia de claves.

La Fig. 34 es un diagrama que ilustra un proceso de cifrado de datos realizado en un aparato de conversión de datos de CAMELLIA usando una clave de 128 bits.

La Fig. 35 es un diagrama que ilustra un proceso de descifrado de datos realizado en un aparato de conversión de datos de CAMELLIA usando una clave de 128 bits.

La Fig. 36 es un diagrama que ilustra una configuración interna de la función F en un aparato de conversión de datos de CAMELLIA.

La Fig. 37 es un diagrama que ilustra una configuración general y operación según una quinta realización.

La Fig. 38 es un diagrama que ilustra una configuración general y operación según una sexta realización.

La Fig. 39 es un diagrama que ilustra una configuración general y operación según una undécima realización.

La Fig. 40 es un diagrama que ilustra una configuración general y operación según una duodécima realización.

La Fig. 41 es un diagrama que ilustra una configuración general y operación según una décima tercera realización.

La Fig. 42 es un diagrama que ilustra una configuración general y operación según una décima cuarta realización.

La Fig. 43 es un diagrama que ilustra una configuración general y operación según una décima quinta realización.

La Fig. 44 es un diagrama que ilustra una configuración general y operación según una décima sexta realización.

La Fig. 45 es un diagrama que ilustra una configuración general y operación según una décima séptima realización.

La Fig. 46 es un diagrama que ilustra una configuración general y operación según una décima octava realización.

La Fig. 47 es un diagrama que ilustra una configuración general y operación según una séptima realización.

La Fig. 48 es un diagrama que ilustra una configuración general y operación según una octava realización.

La Fig. 49 es un diagrama que ilustra una configuración general y operación según una novena realización.

La Fig. 50 es un diagrama que ilustra una configuración general y operación según una décima realización.

La Fig. 51 es un diagrama que ilustra una configuración general y operación según una décima novena realización.

La Fig. 52 es un diagrama que ilustra una configuración general y operación según una vigésima realización.

La Fig. 53 es un diagrama que ilustra una operación del generador de claves intermedias 40 que genera la clave de salida a partir de la clave intermedia con una clave de 192 o 256 bits.

La Fig. 54 es un diagrama que ilustra un proceso de cifrado de datos realizado en un aparato de conversión de datos de CAMELLIA usando una clave de 192 o 256 bits.

La Fig. 55 es un diagrama que ilustra un proceso de descifrado de datos realizado en un aparato de conversión de datos de CAMELLIA usando una clave de 192 o 256 bits.

La Fig. 56 es un diagrama que ilustra la configuración y operación de un aparato de conversión de datos relacionado.

La Fig. 57 muestra un ejemplo de la configuración interna del convertidor principal 320.

La Fig. 58 es un diagrama que ilustra el circuito que compone el subconvertidor 330.

La Fig. 59 es un diagrama que ilustra un circuito compartido por la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 que componen el subconvertidor 330.

La Fig. 60 muestra otro ejemplo de la configuración y operación del aparato de conversión de datos relacionado.

La Fig. 61 muestra otro ejemplo de la configuración interna del convertidor principal 320.

La Fig. 62 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 se conectan en serie y la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 se dotan ambas con la función de transferencia de claves y la función de transferencia de datos.

La Fig. 63 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 de la Fig. 62 conmutan la posición de las mismas.

La Fig. 64 muestra una configuración interna del convertidor principal 320 de CAMELLIA.

Mejor modo para llevar a cabo la invención

Realización 1.

Se dará una descripción de un aparato de conversión de datos según esta realización.

Aparato de conversión de datos

La Fig. 1 es un diagrama que ilustra una configuración y operación de un aparato de conversión de datos según esta realización.

Esta realización no incluye el “camino para introducir la clave intermedia (Clave KL) que se saca desde el registro de claves KL 240 en el selector 310” ni incluye el “camino para introducir datos que se sacan desde el convertidor principal 320 en el selector 310”, los caminos que se muestran en la Fig. 56 y la Fig. 60. La razón es que un subconvertidor 330 de esta realización se dota con una función de transferencia de claves/datos extra además de su función primaria y original para convertir datos.

Se dará más adelante una descripción de generación de claves y cifrado/descifrado de datos mediante el uso de la función de transferencia de claves/datos del subconvertidor 330. Otros componentes y operaciones son los mismos que los tratados con referencia a la Fig. 56 y la Fig. 60 y, por lo tanto, no se tratarán aquí.

Con esta realización, la clave intermedia (Clave KL) sacada desde el registro de claves KL 240 no se introduce directamente al selector 310 sino que se introduce al subconvertidor 330 a través del programador de claves 210 por medio del camino convencional desde el registro de claves KL 240 al programador de claves 210. El subconvertidor 330, dotado con un “modo de conversión de datos” y un “modo de transferencia de claves/datos”, conmuta al “modo de transferencia de claves/datos” tras la recepción de una clave y transfiere la clave de entrada al selector 310.

Además, según esta realización, los datos que se convierten no linealmente por el convertidor principal 320 no se introducen directamente al selector 310 sino que se introducen al subconvertidor 330 en primer lugar. El subconvertidor 330, tras la recepción de los datos convertidos no linealmente por el convertidor principal 320, conmuta al “modo de transferencia de claves/datos” y transfiere los datos de entrada al selector 310.

Las operaciones de transferencia llevadas a cabo de esta manera por el subconvertidor 330 permiten hacer redundantes los dos caminos mostrados en la Fig. 56 y la Fig. 60.

Señalar que una línea de puntos mostrada en la Fig. 1 indica un “camino para transferir los datos intermedios desde el registro aritmético 350 al selector 310”, que se requiere para introducir en el convertidor principal 320 los datos intermedios mantenidos durante un periodo de tiempo dado, en el caso donde el convertidor principal 320 realiza una conversión de datos basada en función F para una vuelta en dos o más ciclos, como se mencionó anteriormente. Por otra parte, el “camino desde el registro aritmético 350 al selector 310” indicado por la línea de puntos no se requiere en el caso donde el convertidor principal 320 realice una conversión de datos basada en función F para una vuelta en un ciclo. Lo mismo aplica a un camino indicado por una línea de puntos mostrada en la Fig. 6 en una discusión posterior.

Método de generación de claves

Se dará ahora una descripción de una clave intermedia y un método de generación de claves de salida del generador de claves intermedias 40.

La Fig. 2 ilustra una operación del generador de claves intermedias 40 para generar una clave de salida a partir de una clave intermedia.

En primer lugar, se introduce una clave secreta al generador de claves intermedias 40 y se mantiene en el registro de claves KL 240 como la clave intermedia (Clave KL) por medio del selector 6-1 KL 220. La clave secreta mantenida en el registro de claves KL 240 se introduce al convertidor principal 320 como la clave intermedia (Clave KL) por medio del programador de claves 210. En la primera unidad de función F 321a del convertidor principal 320, los bits superiores de la clave intermedia (Clave KL) introducidos se convierten no linealmente mediante el uso de una constante $\Sigma 1$ que se saca desde el programador de claves 210, entonces se somete a una operación XOR con los bits inferiores de la clave intermedia (Clave KL) en el circuito EXOR 322a y entonces se introducen a la unidad de función F 321b. Del mismo modo, en la unidad de función F 321b, una clave sacada desde el circuito EXOR 322a se convierte no linealmente mediante el uso de una constante $\Sigma 2$ que se saca desde el programador de claves 210 y entonces se somete a una operación XOR con los bits inferiores de la clave intermedia (Clave KL) en el circuito EXOR 322b. Entonces, la clave de salida resultante como los bits superiores de la clave y la clave sacada desde el circuito EXOR 322a como los bits inferiores de la clave se sacan al subconvertidor 330.

El subconvertidor 330 recibe estas piezas de datos y se someten a una operación XOR entre los bits superiores y los bits inferiores de la clave por medio de dos operadores OR exclusiva (EXOR) incluidos en la unidad de convertidor de datos 50 y dos operadores OR exclusiva (EXOR) incluidas en la unidad de inversor de datos 70 dentro del subconvertidor 330. Entonces, los datos de salida resultantes se introducen al convertidor principal 320 de nuevo.

El convertidor principal 320 realiza el proceso de conversión de dos etapas que implican la unidad de función F 321a, el circuito EXOR 322a, la unidad de función F 321b y el circuito EXOR 322b en el convertidor principal 320, de la misma manera que la del proceso antes mencionado mediante el uso de la parte del convertidor principal 320, entonces intercambia los bits superiores y los bits inferiores de la clave convertida y saca los intercambiados.

Los datos de salida se introducen al selector 6-1 KA 230 del generador de claves intermedias 40 y se mantienen en el registro de Claves KA 250 como la clave de salida (Clave KA). El generador de claves intermedias 40 genera de esta manera la clave de salida (Clave KA) a partir de la clave intermedia (Clave KL) usando parte del convertidor principal 320 y parte del subconvertidor 330 como componentes que ejecutan cifrado/descifrado de datos. Cuatro claves, que incluyen la clave KLH de los bits superiores y la clave KLL de los bits inferiores de la clave intermedia (Clave KL) generada y la clave KAH de los bits superiores y la clave KAL de los bits inferiores de la clave de salida (Clave KA) generada, se introducen al programador de claves 210 y se usan como una clave para cifrado/descifrado de datos (llamada clave extendida). Entonces, la clave de salida generada de esta manera (Clave KA) y la clave intermedia (Clave KL) se usan para generar otra clave intermedia y otra clave de salida en cada periodo dado mediante el mismo proceso.

Programación de claves

Se dará ahora una descripción de una configuración interna y una operación del programador de claves 210.

La Fig. 3 es un diagrama que ilustra una configuración interna y operación del programador de claves 210.

La clave intermedia (Clave KL) sacada desde el generador de claves intermedias 40 se divide en la Clave KLH de los bits superiores y la Clave KLL de los bits inferiores se introduce a un selector 4-1 216 y un selector 4-1 217. La clave de salida (Clave KA) sacada desde el generador de claves intermedias 40 también se divide en la Clave KAH y la Clave KAL y se introducen al selector 4-1 216 y el selector 4-1 217 del mismo modo. El selector 4-1 216 y el selector 4-1 217 seleccionan una clave de entre las cuatro claves. Entonces, una señal seleccionada por el selector 4-1 216, 217 y una señal obtenida a través de un desplazamiento de rotación a la derecha de un bit de la señal seleccionada se introducen a un selector 2-1 214, 215, respectivamente. La razón de por qué la señal se somete a una rotación a la derecha de un bit es la siguiente. Como se trató anteriormente, el subconvertidor 330 se usa en la generación de la clave de salida (Clave KA) por el generador de claves intermedias 40. En ese caso, la señal se somete a un desplazamiento de rotación de un bit a la izquierda por un desplazador de rotación en el subconvertidor 330. Por lo tanto, suponiendo que la señal se someterá a un desplazamiento de rotación de un bit a la izquierda, la señal se somete a un desplazamiento de rotación de un bit a la derecha por adelantado de manera que no haya ningún efecto del desplazamiento de rotación en el resultado. Por consiguiente, el programador de claves 210 no siempre realiza el desplazamiento de rotación a la derecha de un bit. Depende del número de bits y la dirección de un desplazamiento de rotación lo que el desplazador de rotación del subconvertidor 320 hará para una señal. En otras palabras, el programador de claves 210 va a hacer un desplazamiento de rotación por adelantado para la señal del mismo número de bits que el de la dirección opuesta a la de un desplazamiento de rotación que se hará para la señal por el desplazador de rotación del subconvertidor 330. Por lo tanto, el selector 2-1 214 y el selector 2-1 215, que son para seleccionar una señal relativa a una clave de entre estas dos señales, siempre seleccionan una clave obtenida a través del desplazamiento de rotación por adelantado mediante un número de bits predeterminado y sacan la clave al subconvertidor 330, cuando se saca una clave al subconvertidor 330 para generar la clave de salida (Clave KA).

Las claves sacadas desde el selector 2-1 214 y el selector 2-1 215 se introducen al subconvertidor 330 en el caso donde el subconvertidor 330 se use en la generación de la clave de salida (Clave KA) y se introducen a un selector 2-1 212 en el caso donde el convertidor principal 320 se use en la generación de la clave de salida (Clave KA) y en

el proceso de cifrado/descifrado de datos. Entonces, una clave sometida a un desplazamiento de rotación a la izquierda y derecha de un byte se introduce al selector 2-1 212. La razón de por qué la clave sometida a la clave de desplazamiento de rotación a la izquierda o derecha de un byte se introduce al selector 2-1 212 es que el proceso de cifrado de datos/descifrado de datos requiere esa clave en el caso donde la unidad de función F se compone de partes que procesan la función F de menos de una tal como 1/2, 1/4 y 1/8, que se tratará más adelante en detalle.

El 212 selecciona una clave de entre estas dos claves e introduce una clave seleccionada a un selector 2-1 211. Un selector 8-1 213 recibe las constantes $\Sigma 1$ hasta $\Sigma 4$ divididas en datos superiores y datos inferiores, selecciona una señal de entre estas ocho señales de entrada e introduce una señal seleccionada al selector 2-1 211. El selector 2-1 211 selecciona una señal de entre las dos señales de entrada y saca una señal de selección al convertidor principal 320 como una clave.

Cifrado/Descifrado de datos

Se dará ahora una descripción de cifrado/descifrado de datos realizado por el aleatorizador de datos 30.

La Fig. 4 es un diagrama que ilustra una operación del aleatorizador de datos 30 para cifrado/descifrado.

En primer lugar, se introduce P (texto plano o texto cifrado). Se supone aquí que P (texto plano o texto cifrado) tiene una longitud de 128 bits. Los datos de entrada, P, se introducen a un circuito EXOR 31a y se someten a una operación XOR con una clave secreta (128 bits de longitud) que se introduce a y entonces se saca desde el generador de claves 20 a través del generador de claves intermedias 40 y el programador de claves 210. Señalar que la clave secreta se introduce al generador de claves intermedias 40 en primer lugar, entonces se selecciona por el selector 6-1 KL 220, entonces se mantiene en el registro de claves KL 240 como la clave intermedia (Clave KL) y entonces se introduce al programador de claves 210 como la clave intermedia (Clave KL).

Como CAMELLIA (camellia) diseñado para un proceso de cifrado de bloques con clave común, se usan los operadores OR exclusiva en el subconvertidor 330 para el circuito EXOR 31a y un circuito EXOR 31b. Más particularmente, como se muestra en la Fig. 58, los datos de entrada se dividen en datos superiores de los bits superiores y datos inferiores de los bits inferiores. Entonces, cada pieza de datos divididos y una clave de entrada se someten a una operación XOR en el circuito EXOR 55 y el circuito EXOR 56 de la unidad de convertidor de datos 50 o en el circuito EXOR 75 y el circuito EXOR 76 de la unidad de inversor de datos 70 y se sacan.

Los datos de salida se convierten por el convertidor principal 320 y el subconvertidor 330 mediante el uso de una de las claves extendidas sacadas desde el programador de claves 210. Con la Fig. 4, la conversión de datos se lleva a cabo alternativamente en el orden de: el convertidor principal 320a, un subconvertidor 330a, un convertidor principal 320b, un subconvertidor 330b y un convertidor principal 320c.

Los datos convertidos de esta manera se someten a una operación XOR con una clave sacada a partir del programador de claves 210 en el circuito EXOR 31b del subconvertidor 330 y se sacan como C (texto cifrado o texto descifrado).

Se dará ahora una descripción en detalle de una operación de conversión de datos de CAMELLIA realizada por el convertidor principal 320 y el subconvertidor 330 en el aleatorizador de datos 30 con referencia a la Fig. 1 y la Fig. 4.

Los datos sacados desde el circuito EXOR 31a se dividen en datos superiores y datos inferiores y se introducen al convertidor principal 320a respectivamente. En el convertidor principal 320a, cada pieza de los datos de entrada se convierte no linealmente y los datos superiores y datos inferiores se intercambian como se muestra en la Fig. 4 de manera que los datos inferiores convertidos se tratan como datos superiores y los datos superiores convertidos se tratan como datos inferiores y entonces se introducen al subconvertidor 3301.

En el subconvertidor 330a, los datos de entrada se convierten linealmente. Como se muestra en la Fig. 1, los datos convertidos se introducen al selector 310, entonces se mantienen en el registro aritmético 350 y luego se introducen al convertidor principal 320 (mostrado como el convertidor principal 320b en la Fig. 4).

El convertidor principal 320b y el subconvertidor 330b realizan los mismos procesos que los realizados por el convertidor principal 320a y el subconvertidor 330, respectivamente. El mismo proceso que el realizado por el convertidor principal 320a se repite de nuevo en el convertidor principal 320c. Los datos de salida desde el convertidor principal 320c, que se obtienen a través de la serie de repeticiones, se somete a una operación XOR con datos de claves sacados desde el programador de claves 210 al circuito EXOR 31b y entonces se sacan como C. Con CAMELLIA, se usa un operador lógico exclusivo incluido en el subconvertidor 330 para el 31b como el circuito EXOR 31a. También, con CAMELLIA, la conversión de datos se lleva a cabo usando el mismo convertidor principal 320 para cada uno de los convertidores principales 320a, 320b y 320c y repitiendo el mismo proceso. Alternativamente, no obstante, también es posible que los convertidores principales 320a, 320b y 320c se compongan separadamente de la misma configuración interna. Lo mismo aplica al subconvertidor 330a y el subconvertidor 330b.

Señalar aquí que en el caso donde el convertidor principal 320 se dote con parte para procesar la función F para una vuelta y luego realice una conversión de datos basada en una función F de seis vueltas como se muestra en la Fig. 57, el proceso del convertidor principal 320 se repite seis veces, completando por ello el proceso de la conversión de datos basada en una función F de seis vueltas. Esto, con referencia a la Fig. 1, supone que el convertidor principal 320 completa la conversión de datos basada en una función F de seis vueltas repitiendo el uso del camino en bucle desde el convertidor principal 320 a través del selector 310, el registro aritmético 350, entonces de vuelta al convertidor principal 320 seis veces. Por lo tanto, la técnica relacionada mostrada en la Fig. 56 y la Fig. 60 requiere el "camino para introducir datos que se sacan desde el convertidor principal 320, al selector 310".

No obstante, según esta realización, el subconvertidor 330 tiene una función de transferencia, que se tratará más tarde y por lo tanto los datos sacados desde el convertidor principal 320 se pueden introducir al selector 310 con ser transferidos por el subconvertidor 330. De esta manera, según el aparato de conversión de datos de esta realización, el uso del "camino para introducir datos sacados desde el convertidor principal 320 al selector 310 con ser transferidos por el subconvertidor 330" elimina la necesidad del "camino para introducir datos sacados desde el convertidor principal 320 al selector 310".

Conversión principal – convertidor principal 320.

La configuración interna y la operación del convertidor principal 320 se han tratado anteriormente con referencia a la Fig. 57 y la Fig. 61.

Como se mencionó anteriormente, la estructura para conversión no lineal del convertidor principal 320 caracterizada más adelante se llama Estructura FEISTEL. Específicamente, la estructura para conversión no lineal incluye dividir datos de entrada en datos superiores de los bits superiores y datos inferiores de los bits inferiores, convirtiendo no linealmente uno de los datos superiores y los datos inferiores divididos usando la función F, generando datos a ser introducidos a la función F en base a unos de los datos superiores y los datos inferiores convertidos no linealmente y los otros de los datos superiores y los datos inferiores, dividiendo los datos generados como los datos de entrada en datos superiores y datos inferiores y convirtiendo de nuevo usando la función F y repitiendo los procesos antes mencionados.

Conversión principal – convertidor principal 320 – unidad de función F 321.

Se dará ahora una descripción de una configuración interna y una operación de la unidad de función F 321 incluida en el convertidor principal 320.

La Fig. 5 es un diagrama que ilustra una configuración interna y una operación de una unidad de función F 321.

En primer lugar, los datos de entrada se someten a una operación XOR con una clave extendida en un circuito EXOR 323, entonces se dividen en ocho piezas y se introducen a una función S 324. La clave extendida se define como una clave combinada de la clave de salida (Clave KA) y la clave intermedia (Clave KL), que se generan a partir de la clave secreta por el generador de claves intermedias 40. Con CAMELLIA de una clave secreta de 128 bits de longitud, la clave extendida tiene 256 bits de longitud. La clave intermedia (Clave KL) se divide en una clave KLH de los bits superiores y una clave KLL de los bits inferiores y la clave de salida (Clave KA) también se divide en una clave KAH de los bits superiores y una clave KAL de los bits inferiores. Entonces, una clave programada por el programador de claves 210 de entre las cuatro claves se introduce al circuito EXOR 323. La función S 324 es una función sintetizada (S_1 hasta S_4) de una operación aritmética inversa de GAF (2^8) y una conversión afín y realiza una conversión no lineal en modo byte. Los datos convertidos y luego sacados se introducen a una función P 325, entonces se aleatorizan por la función P 325 realizando una conversión lineal y entonces se sacan.

Se dará ahora una descripción de una operación en un caso que una unidad de función F se compone de un procesamiento de parte para 1/2 de la función F (función 1/2F).

El procesamiento de la parte para 1/2 de la función F en la unidad de función F se compone del circuito EXOR 323, cuatro Cajas S S_4 324e hasta S_1 324h y aproximadamente la mitad de la unidad de función P de la Fig. 5. Con esta configuración, se realiza primero una conversión de datos basada en una 1/2 de la función F para una vuelta. Entonces, se repite el mismo proceso para completar el proceso de función F para una vuelta. En el primer proceso, se usan una clave y datos que se someten al desplazamiento de rotación a la izquierda o derecha de un byte tratado anteriormente en el programador de claves 210. El desplazamiento de rotación a la izquierda o derecha de un byte de la clave y los datos se puede efectuar igual que el del desplazamiento de una caja S en un byte sin cambiar la disposición de las cajas S S_1 hasta S_4. Más específicamente, como se muestra en la Fig. 5, el mismo proceso se puede realizar como la disposición de las cajas S en el orden de S_2, S_3, S_4, S_1 indicado por S_1 324a hasta S_4 324d introduciendo una clave y datos que se someten al desplazamiento de rotación de un byte sin cambiar la disposición de las cajas S S_1, S_2, S_3, S_4 indicadas por S_4 324e hasta S_1 324h.

A través de esas operaciones, el proceso de función F de una vuelta se completa en dos ciclos.

Aparato de conversión de datos con convertidor principal 320 y subconvertidor 330 dispuestos a la inversa.

La Fig. 6 es un diagrama que ilustra una configuración y una operación de un aparato de conversión de datos en el que el convertidor principal 320 y el subconvertidor 330 de la Fig. 1 se disponen a la inversa.

Incluso en el caso donde el aparato de conversión de datos tenga el convertidor principal 320 y el subconvertidor 330 en posición inversa, el subconvertidor 330 usa la función de transferencia para transferir y sacar datos al convertidor principal 320, justo igual que el caso del aparato de conversión de datos mostrado en la Fig. 1. El uso de tal camino permite al convertidor principal 320 completar la conversión de datos basada en una función F de seis vueltas. De esta manera, el "camino para introducir datos sacados desde el subconvertidor 330 al selector 310" se hace redundante.

La clave intermedia (Clave KL) sacada a partir del registro de claves KL 240 no se introduce directamente al selector 310 sino que se introduce al subconvertidor 330 a través del programador de claves 210 mediante el uso del camino desde el registro de claves KL 240 al programador de claves 210. El subconvertidor 330, tras la recepción de una clave, transfiere la clave de entrada al convertidor principal 320 usando la función de transferencia.

La operación de transferencia realizada de esta manera por el subconvertidor 330 permite eliminar la necesidad de los dos caminos del "camino para introducir la clave intermedia (Clave KL) sacada desde el registro de claves KL 240 al selector 310" y dos caminos y el "camino para introducir datos sacados desde el convertidor principal 320 al selector 310" o el "camino para introducir datos sacados desde el subconvertidor 330 al selector 310" mostrados en la Fig. 56 y la Fig. 60.

Aparato de conversión de datos con convertidor principal 320 y subconvertidor 330 dispuestos en paralelo.

La Fig. 7 es un diagrama que ilustra un aparato de conversión de datos que es diferente de los de la Fig. 1 y la Fig. 6 de manera que el convertidor principal 320 y el subconvertidor 330 se disponen en paralelo y hay un selector 340 que selecciona una señal de salida de entre dos señales de entrada.

Otros elementos distintos de los mencionados anteriormente son los mismos que los de la Fig. 1 y la Fig. 6.

El aparato de conversión de datos configurado de esta manera, que tiene el convertidor principal 320 y el subconvertidor 330 en una disposición paralelo, requiere el selector 340 para seleccionar una de las señales sacadas desde el convertidor principal 320 y el subconvertidor 330. Por consiguiente, el convertidor principal 320 y el subconvertidor 330 reciben una señal que se selecciona por el selector 310 de entre una señal seleccionada por el selector 340 y pasa a través del registro aritmético 350 y P (texto plano o texto cifrado).

Por otra parte, la clave intermedia (Clave KL) sacada desde el registro de claves KL 240 no se introduce directamente al selector 310 en el momento de generación de la clave de salida (Clave KA). La clave intermedia (Clave KL) se introduce al subconvertidor 330 a través del programador de claves 210 por medio de un camino desde el registro de claves KL 240 al programador de claves 210. El subconvertidor 330, tras la recepción de la clave, transfiere la clave recibida al convertidor principal 320 por medio de la función de transferencia. De esta manera, se puede eliminar la necesidad del "camino para introducir la clave intermedia sacada desde el registro de claves KL 240 al selector 310".

Además, también se puede eliminar la necesidad de los dos caminos del "camino para introducir datos sacados desde el convertidor principal 320 al selector 310" o el "camino para introducir datos sacados desde el subconvertidor 330 al selector 310".

Configuración interna de generador de claves intermedias 40

Se dará ahora una descripción de una configuración interna del selector 6-1 KL 220 y el selector 6-1 KA 230 en el generador de claves intermedias 40.

La Fig. 8 es un diagrama que ilustra una configuración interna del selector 6-1 KL 220 y el selector 6-1 KA 230 en el generador de claves intermedias 40.

La clave intermedia (Clave KL) que se mantiene en el registro de claves KL 240 en el generador de claves intermedias 40 se saca al programador de claves 210 y también se introduce al selector 6-1 KL 220 de nuevo. El selector 6-1 KL 220 incluye un selector 6-1 221.

En el selector 6-1 KL 220, la clave intermedia (Clave KL) introducida y también cuatro señales obtenidas a través de desplazamientos de rotación de la clave intermedia (Clave KL) mediante cuatro números arbitrarios diferentes se introducen al selector 6-1 221. Las cuatro señales a ser introducidas al mismo se pueden obtener posiblemente a través de desplazamientos de rotación de la clave intermedia en 17 y 15 bits a la izquierda y derecha, respectivamente, lo cual no se muestra en la figura. Las seis señales de la clave intermedia (Clave KL), las cuatro señales sometidas a desplazamientos de rotación y la clave secreta se tratan como seis señales de entrada, el selector 6-1 221 selecciona una señal de salida de entre seis señales de entrada y tiene el registro de claves KL 240 que mantiene la señal de salida seleccionada como una nueva clave intermedia (Clave KL).

El método de generación de una nueva clave de salida (Clave KA) a partir de la clave de salida (Clave KA) es el mismo que la generación de una nueva clave intermedia (Clave KL) a partir de la clave intermedia (Clave KL).

La Fig. 9 es un diagrama que ilustra otra configuración del generador de claves intermedias 40.

La Fig. 9, en contraste con la Fig. 8, muestra la compartición de un selector indicado por un selector 4-1 223. Específicamente, la clave intermedia (Clave KL) sacada desde el registro de claves KL 240 y la clave de salida (Clave KA) sacada desde el registro de claves KA 250 se introducen a un selector 2-1 224. El selector 2-1 224 selecciona una de las dos claves, entonces genera cuatro señales mediante los desplazamientos de rotación de una clave seleccionada mediante cuatro números diferentes y entonces saca las cuatro señales al selector 4-1 223. El selector 4-1 223 selecciona una señal de entre las cuatro señales y entonces saca una señal seleccionada a un selector 3-1 KL 222 o un selector 3-1 KA 232.

El selector 3-1 KL 222 selecciona una clave de entre una clave seleccionada por el selector 4-1 223, la clave secreta y la clave intermedia (Clave KL) que se mantuvo en el registro de Claves KL 240 y el registro de claves KL 240 mantiene una clave seleccionada como una nueva clave intermedia.

De manera similar, el selector 3-1 KA 232 selecciona una clave de entre la clave seleccionada por el selector 4-1 223, la clave de salida (Clave KA) generada y la clave de salida (Clave KA) que se mantuvo en el registro de claves KA 250 y el registro de claves KL 240 mantiene una clave seleccionada como una nueva clave de salida (Clave KA).

En contraste con la configuración mostrada en la Fig. 8 donde se necesitan diez unidades de selectores 2-1, la configuración mostrada en la Fig. 9 solamente necesita ocho unidades de selectores 2-1. Por lo tanto, comparado con el generador de claves intermedias 40 de la configuración mostrada en la Fig. 8, la de la configuración mostrada en la Fig. 9 puede ahorrar dos unidades de selectores 2-1. De esta manera, se puede reducir el tamaño del circuito.

Señalar que la configuración del generador de claves intermedias 40 de la Fig. 8 también es aplicable al aparato de conversión de datos de cada realización de la presente invención. Adicionalmente, la configuración del generador de claves intermedias 40 de la Fig. 9 también es aplicable al aparato de conversión de datos de cada realización de la presente invención.

Aún más, la configuración del generador de claves intermedias 40 de la Fig. 51 en una discusión posterior también es aplicable al aparato de conversión de datos de cada realización de la presente invención.

Conversión subordinada – subconvertidor 330.

Se dará ahora una descripción de una configuración interna y una operación del subconvertidor 330.

Aquí, se dará una descripción del caso donde al menos una de la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 tiene la función de transferencia de claves según esta realización.

Conversión subordinada – subconvertidor 330 – unidad de convertidor de datos 50 con función de transferencia de claves.

La Fig. 10 es un diagrama que ilustra una configuración interna y una operación del subconvertidor 330.

En contraste con la configuración de la unidad de convertidor de datos 50 y la de la unidad de inversión de datos 70 de la técnica relacionada tratada con referencia a la Fig. 58, las de esta realización incluyen una señal de transferencia para transferir una clave o datos y circuitos acompañados con la señal de transferencia, además.

Con la Fig. 10, la unidad de convertidor de datos 50 tiene la función de transferir una clave de entrada.

Específicamente, una señal de transferencia para transferir una clave se introduce al inversor de datos 50. La unidad de convertidor de datos 50, tras la recepción de la señal de transferencia, transfiere la clave recibida basada en la señal de transferencia.

Más específicamente, las señales de transferencia se controlan por un controlador 5. En el caso de transferir una clave, el controlador 5 saca una señal de transferencia de claves FL y una señal de máscara FL. La unidad de convertidor de datos 50 recibe la señal de transferencia de claves FL y la señal de máscara FL sacada desde el controlador 5.

Se darán ahora descripciones concretas de un proceso de transferencia de claves realizado por la unidad de convertidor de datos 50 usando estas señales de transferencia.

En el caso de transferencia de una clave, la señal de transferencia de claves FL se fija a 0 y se introduce a un circuito AND 51. El circuito AND 51 también recibe datos objetivo a ser cifrados/descifrados.

Dado que la señal de transferencia de claves FL es 0, los datos de entrada se inhiben por el circuito AND del circuito AND 51 y se anulan por ello. En otras palabras, cualquiera que sea el valor de datos de entrada que se asigne, los datos de salida del circuito AND 51 llegan a ser cero.

Los bits superiores de los datos asignados a un valor de 0 sacado desde el circuito AND 51 se introducen a un circuito OR 53 y los bits inferiores se introducen al circuito EXOR 55.

Mientras tanto, la señal de máscara FL se introduce a un circuito NOT 52. En el caso de transferencia de una clave, el controlador 5 fija la señal de máscara FL a 0, de manera que la señal de salida desde el circuito NOT 52 llega a ser 1. Por lo tanto, una señal de salida desde el circuito OR 53 que recibe de esta manera señales 0 y 1 llega a ser 1. El circuito AND 54 recibe 1 que es un valor sacado desde el circuito OR 53 y la información de la clave 1, de manera que los datos de salida desde el circuito AND 54 son siempre la clave 1.

La clave 1 sacada desde el circuito AND 54 se somete a un desplazamiento de rotación de un bit a la izquierda y entonces se introduce al circuito EXOR 55. La clave 1 ya se ha sometido a un desplazamiento de rotación a la izquierda de un bit a la derecha por adelantado en el programador de claves 210 como se muestra en la Fig. 3. Por lo tanto, la clave 1 sacada desde el circuito AND 54 puede restaurar su valor original para ser transferido por lo tanto sometido al desplazamiento de rotación de 1 bit a la izquierda.

El circuito EXOR 55 recibe los bits inferiores, asignados a un valor de 0, sacados desde el circuito AND 51, de manera que una operación aritmética del circuito AND 55 saca la clave 1 como está. Estos llegan a ser los bits inferiores de la señal de salida.

De esta manera, la unidad de convertidor de datos 50 puede sacar la clave 1 como está como la señal de salida en base a la señal de transferencia de claves KL y la señal de máscara FL.

Del mismo modo, con la señal de transferencia de claves FL y la señal de máscara FL, la clave 2 se transfiere como está como la señal de salida. La operación se tratará más adelante.

La señal de máscara FL es 0 como se mencionó previamente. Por lo tanto, un circuito AND 58 recibe 0 y la clave 1 sacada desde el circuito EXOR 55 y siempre saca 0.

El circuito OR 57 recibe la clave 2 y 0 y por lo tanto su valor de salida es siempre la clave 2.

La clave 2 se introduce al circuito EXOR 56 donde se somete a una operación XOR con 0 que son los datos superiores sacados por el circuito AND 51, de manera que una salida desde el circuito EXOR 56 es siempre la clave 2. Esta llega a ser los bits superiores de la señal de salida.

De esta manera, se introducen la señal de transferencia de claves FL y la señal de máscara FL y se pueden transferir la clave 1 y la clave 2 como están. Señalar que, aunque el controlador 5 para controlar la señal de transferencia de claves FL y la señal de máscara de claves FL que son ambas la señal de transferencia, no se muestran en las Fig. 11, 12 y 14 hasta 33, las señales de transferencia van a ser controladas por el controlador 5 como el caso mostrado en la Fig. 10.

Conversión subordinada – subconvertidor 330 – unidad de inversor de datos 70 con función de transferencia de claves.

Se dará ahora una descripción del caso donde la unidad de inversión de datos 70 se dota con la función para transferir una clave de entrada.

La Fig. 11 es un diagrama que ilustra el caso donde la unidad de inversor de datos 70 tiene la función de transferencia de claves.

Y el circuito AND 71 recibe una señal de transferencia de claves FL^{-1} y datos.

Como la señal de transferencia de claves FL mencionada anteriormente, la señal de transferencia de claves FL^{-1} mantiene 0 y por lo tanto los datos introducidos al circuito AND 71 se inhiben y de esta manera se anulan, de manera que los datos de salida desde el circuito AND 71 se fijan a 0.

Como la señal de máscara FL mencionada anteriormente, la señal de máscara FL^{-1} es 0 y por lo tanto ambas de las señales introducidas a un circuito AND 73 son 0, de manera que los datos de salida desde el circuito AND 73 se fijan a 0.

El circuito OR 74, que recibe los datos de salida desde el circuito AND 73, 0 y la clave 3, saca la clave 3.

El circuito EXOR 75, que recibe los bits superiores, 0, de los datos de salida, 0, desde el circuito AND 71 y por lo tanto saca la clave 3. Estos llegan a ser los bits superiores de la señal de salida.

Un circuito OR 78, que recibe un valor 1, que es un valor invertido de la señal de máscara FL^{-1} 0 por un circuito NOT 72 y la clave 3 y por lo tanto saca 1. El circuito AND 77, que recibe los datos de salida 1 desde el circuito OR 78 y la clave 4 y por lo tanto saca la clave 4. La clave 4 se somete a un desplazamiento de rotación de un bit a la izquierda y entonces se introduce al circuito EXOR 76. Aquí, de nuevo, la clave 4 ya se ha sometido al desplazamiento de rotación de un bit por adelantado a la derecha por el programador de claves 210 y entonces se introduce a la unidad de inversor de datos 70. Por lo tanto, la clave 4 puede restaurar su valor original sometida de esta manera al desplazamiento de rotación de un bit a la izquierda aquí.

El circuito EXOR 76, que recibe los bits inferiores, 0, de datos de salida desde el circuito AND 71 y la clave 4, saca la clave 4. Estos llegan a ser los bits inferiores de los datos de salida.

De esta manera, la unidad de inversión de datos 70 puede sacar una clave de entrada (clave 3, clave 4) como está tras la recepción de las señales de transferencia, la señal de transferencia de claves FL^{-1} y la señal de máscara FL^{-1}.

Conversión subordinada – subconvertidor 330 – unidad de convertidor de datos 50 y unidad de inversor de datos 70 ambas con la función de transferencia de claves.

Se dará ahora una descripción del caso donde tanto la unidad de convertidor de datos 50 como la unidad de inversor de datos 70 se dotan con la función para transferir una clave de entrada.

La Fig. 12 es un diagrama que ilustra una configuración interna del subconvertidor 330 en el caso donde la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 se dotan con la función de transferencia de claves.

La configuración y operación de la unidad de convertidor de datos 50 es la misma que la de la unidad de convertidor de datos 50 de la Fig. 10 y la configuración y la operación de la unidad de inversor de datos 70 es la misma que la de la unidad de inversor de datos 70 de la Fig. 11 y por lo tanto no se tratará aquí en detalle.

Al menos una de la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 dotada de esta manera con la función de transferencia de claves permite eliminar la necesidad del camino para transferir una clave desde el registro de claves KL 240 al selector 310 mostrado en la Fig. 56 y la Fig. 60, de manera que la clave se puede introducir al subconvertidor 330 desde el registro de claves KL 240 a través del programador de claves 210. Adicionalmente, la señal de transferencia para transferir una clave que se introduce en el subconvertidor 330 permite al subconvertidor 330 transferir la clave al selector 310.

Haciendo posible de esta manera la transferencia de claves usando el camino, se puede reducir un número total de selectores en el aparato de conversión de datos. Más particularmente, según el aparato de conversión de datos de esta realización, la función se comparte generando la clave extendida por el generador de claves intermedias 40 y realizando conversión de datos por el convertidor principal 320 y el subconvertidor 330 como se muestra en la Fig. 2 a fin de implementar un aparato de conversión de datos compacto. Entonces, el uso del “camino para transferir la clave intermedia (Clave KL) desde el registro de claves KL 240 al selector 310 a través del programador de claves 210 por el subconvertidor 330 y entonces al convertidor principal 320 a través del registro aritmético 350” de esta realización puede frenar el aumento en el número de selectores, en lugar del uso del “camino para transferir la clave intermedia (Clave KL) desde el registro de Claves KL 240 al selector 310 y entonces al convertidor principal 320 a través del registro aritmético 350” mostrado en la Fig. 56 y la Fig. 60.

De esta manera frenar el aumento en el número de selectores en el aleatorizador de datos del aparato de conversión de datos para cifrado de bloques y por ello reducir el número total de puertas en los circuitos permite reducir el tamaño de todos los circuitos integrados del circuito y el consumo de potencia. Por lo tanto, el aparato de conversión de datos para el cifrado de bloques de esta realización se puede implementar eficazmente incluso en dispositivos móviles tales como teléfonos celulares para los cuales se desea enérgicamente la reducción de tamaño junto con un consumo de potencia bajo.

Con referencia a la Fig. 10 hasta la Fig. 33, las claves de entrada pueden ser diferentes una de otra o de otro modo las mismas. La señal de transferencia de claves FL y la señal de transferencia de claves FL^{-1} también pueden ser las mismas señales. La señal de máscara FL y la señal de máscara FL^{-1} también pueden ser las mismas señales.

Realización 2.

En esta realización, se dará una descripción del caso donde al menos una de la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 se dota con la función de transferencia de datos.

Conversión subordinada – subconvertidor 330 – unidad de convertidor de datos 50 con función de transferencia de datos.

En esta realización, se dará una descripción del caso donde el subconvertidor 330 se dota con la función de transferencia de datos.

La Fig. 13 es un diagrama que ilustra una configuración interna del subconvertidor 330 en el que la unidad de convertidor de datos 50 se dota con la función de transferencia de datos.

El controlador 5 introduce la señal de transferencia de datos FL a la unidad de convertidor de datos 50 como una señal para transferir datos. Se asigna un valor 0 a la señal de transferencia de datos FL introducida a la unidad de convertidor de datos 50. Esta señal se introduce a un circuito AND 59 y un circuito AND 60.

Un circuito AND 54 recibe los bits superiores de datos de entrada y la clave 1. Los datos de salida desde el circuito AND 54 no están especificados, dependiendo del valor de los datos de entrada. Por otra parte, una señal de salida desde el circuito AND 60 es siempre 0, con independencia del valor de la señal de salida desde el circuito AND 54, incluso con los datos de entrada obtenidos a través de un desplazamiento de rotación de un bit a la izquierda de los datos de salida, debido a que la otra señal de entrada, la señal de transferencia de datos FL, mantiene un valor de 0. Los datos de salida, 0, desde el circuito AND 60 se introducen al circuito EXOR 55, donde los datos de entrada y los bits inferiores se someten a una operación XOR. Dado que la salida desde el circuito AND 60 es 0, los bits inferiores de los datos de entrada se sacan al circuito EXOR 55 como los datos inferiores de la señal de salida.

Mientras tanto, los datos de salida desde el circuito EXOR 55 y una clave se introducen al circuito OR 57 como señales de entrada. Señalar aquí que una señal de salida desde el circuito OR 57 no está especificada, pero la señal de transferencia de datos FL se fija a 0, de manera que una señal de salida desde un circuito AND 59 es 0. En el circuito EXOR 56, los bits superiores de datos de entrada y los datos de salida, 0, desde el circuito AND 59 se someten a una operación XOR. Por lo tanto, los bits superiores de los datos de entrada se sacan como los datos superiores de una señal de salida.

De esta manera, la unidad de convertidor de datos 50, tras la recepción de la señal de transferencia de datos FL como la señal de transferencia, puede recibir datos de salida como están, con independencia de la entrada de la clave.

Señalar que la configuración de la unidad de inversor de datos 70 de la Fig. 13 es la misma que la de la unidad de inversor de datos 70 mostrada en la Fig. 57 y por lo tanto no se tratará aquí en detalle.

Conversión subordinada – subconvertidor 330 – unidad de inversor de datos 70 con función de transferencia de datos.

La Fig. 14 es un diagrama que ilustra una configuración interna del subconvertidor 330 en el que la unidad de inversor de datos 70 tiene la función de transferencia de datos.

La unidad de inversor de datos 70 recibe la señal de transferencia de datos FL^{-1} para transferir datos. En el caso de transferencia de datos, se asigna 0 a la señal de transferencia de datos FL^{-1}, de manera que un circuito AND 79 saca 0 cualquiera que sea el valor que se asigne a una señal de salida desde el circuito OR 74. Por lo tanto, el circuito EXOR 75 saca los bits superiores de datos de entrada como están como los datos superiores de la señal de salida.

La señal de transferencia de datos FL^{-1} se introduce a un circuito AND 80, de manera que una señal de salida desde el circuito AND 80 es 0, con independencia del valor de una señal de salida desde el circuito AND 77. De esta manera, los bits inferiores de datos de entrada se sacan como están en el circuito EXOR 76 como los datos inferiores de la señal de salida.

De esta manera, la unidad de inversor de datos 70 puede transferir datos como están como la señal de salida.

Conversión subordinada – subconvertidor 330 – unidad de convertidor de datos 50 y unidad de inversor de datos 70 ambas con función de transferencia de datos.

La Fig. 15 es un diagrama que ilustra una configuración interna del subconvertidor 330 en el que la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 ambas se dotan con la función de transferencia de datos.

La unidad de convertidor de datos 50 es la misma en configuración que el aparato de conversión de datos de la Fig. 13 y la unidad de inversor de datos 70 es la misma en configuración que la unidad de inversor de datos 70 de la Fig. 14. Por lo tanto, la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 de la Fig. 15 pueden sacar respectivamente datos introducidos como están.

El subconvertidor 330 que tiene de esta manera la función para transferir datos de entrada como están al selector 310 puede eliminar la necesidad del camino para transferir datos de salida desde el convertidor principal 320 al selector 310 mostrado en la Fig. 56.

Como se muestra en la Fig. 60, en el proceso de cifrado/descifrado de datos, en el caso donde el convertidor principal 320 tiene la función F durante menos de una vuelta, los datos intermedios van a ser mantenidos en el registro aritmético 350 durante un periodo de tiempo dado en orden para que el convertidor principal 320 procese la conversión no lineal basada en una función F para una vuelta, que se trató anteriormente. Esto indica que el convertidor principal 320 necesita su propio camino en bucle, que corresponde al camino en bucle de la Fig. 60 para

sacar los datos intermedios sacados desde el convertidor principal 320 al registro aritmético 350 a través del selector 310.

El uso de la función de transferencia de datos del subconvertidor 330 de esta realización, por otra parte, puede eliminar la necesidad del camino en bucle antes mencionado. Más particularmente, los datos intermedios sacados desde el convertidor principal 320 se transfieren por el subconvertidor 330 y se introducen al selector 310. El selector 310 selecciona los datos intermedios recibidos y por ello los datos intermedios se transfieren al convertidor principal 320.

El uso de este camino de datos permite reducir el número de señales de entrada al selector 310, en contraste con el número de señales de entrada al selector 310 mostrado en la Fig. 56 o la Fig. 60. Por lo tanto, el aumento de selectores se puede frenar y de esta manera se puede reducir el número de selectores.

De manera similar, el aparato de conversión de datos de la Fig. 6 y la Fig. 7 se permite que elimine la necesidad del camino desde el convertidor principal 320 al selector 310, permitiendo por ello al dispositivo llegar a ser compacto. Adicionalmente, la reducción en el número de selectores permite lograr un consumo de potencia bajo.

Señalar que la señal de transferencia de datos FL y la señal de transferencia de datos FL^{-1} pueden ser las mismas señales.

Realización 3.

En esta realización, se dará una descripción del caso donde al menos una de la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 se dota con la función de transferencia de claves y la función de transferencia de datos.

Conversión subordinada – subconvertidor 330 – unidad de convertidor de datos 50 con función de transferencia de claves y función de transferencia de datos y unidad de inversor de datos 70 con función de transferencia de claves.

La Fig. 16 es un diagrama que ilustra una configuración interna del subconvertidor 330 en el que la unidad de convertidor de datos 50 se dota con la función de transferencia de claves y la función de transferencia de datos y la unidad de inversor de datos 70 se dota con la función de transferencia de claves.

La configuración y la operación de la unidad de inversor de datos 70 es la misma que las de la unidad de inversor de datos 70 de la Fig. 11 con la función de transferencia de claves y por lo tanto no se tratarán aquí.

La configuración y la operación de la unidad de convertidor de datos 50 corresponden a la combinación de las de la unidad de convertidor de datos 50 de la Fig. 10 con la función de transferencia de claves y las de la unidad de convertidor de datos 50 de la Fig. 13 con la función de transferencia de datos y por lo tanto no se tratarán aquí.

Con la unidad de convertidor de datos 50, la señal de transferencia de claves FL tiene la función de inhibir y de esta manera anular datos de entrada y la señal de máscara FL tiene la función de dejar pasar a través una clave de entrada.

La señal de transferencia de datos FL tiene la función de anular una clave de entrada para permitir pasar a través datos.

Por consiguiente, en el caso donde tanto la señal de transferencia de claves FL como la señal de máscara FL ambas que mantienen 0 como la señal de transferencia para transferir una clave, los datos no se pueden transferir, de manera que la señal de trasferencia de datos FL no puede mantener 0 como una señal de transferencia para transferir datos. De manera similar, en el caso donde la señal de transferencia de datos FL mantiene 0 como la señal de transferencia para transferir datos, no se puede transferir una clave, de manera que la señal de transferencia de claves FL y la señal de máscara FL no puede mantener 0 como la señal de transferencia para transferir una clave.

Entonces, en el caso donde ninguna de la señal de transferencia de claves FL, la señal de máscara FL, la señal de transferencia de datos FL, una señal de transferencia de claves FL^{-1} y una señal de máscara FL^{-1} mantienen 0 como la señal de transferencia, la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 realizan una conversión lineal de datos de entrada, la cual suponen hacer.

En primer lugar, se dará una descripción de una operación de la unidad de convertidor de datos 50 para transferir una clave.

La unidad de convertidor de datos 50 recibe 0 como la señal de transferencia de claves FL y 0 como la señal de máscara FL. Dado que los datos no van a ser transferidos, la señal de transferencia de datos FL permanece sin cambios teniendo 1.

En primer lugar, el circuito AND 51 inhibe y de esta manera anula datos por la señal de transferencia de claves FL. La clave 1 pasa a través del circuito AND 54 directamente, entonces, se somete a un desplazamiento de rotación de un bit a la izquierda y entonces se introduce al circuito AND 60. Dado que la señal de transferencia de datos FL es 1,

la clave 1 pasa a través del circuito AND 60 directamente. En el circuito EXOR 55, la clave 1 se somete a una operación XOR con 0, que es los bits inferiores de datos de salida desde el circuito AND 51. La clave 1 se saca como los datos inferiores de la señal de salida. La clave 2 pasa a través del circuito OR 57 por 0, que se saca desde el circuito AND 58, pasa a través del circuito AND 59 por la señal de transferencia de datos FL, entonces se somete a una operación XOR con 0 que es el bit inferior de los datos de salida sacados desde el circuito AND 51 en el circuito EXOR 56, pasando por ello también a través del circuito XOR 56 y llegan a ser los datos superiores de la señal de salida. La unidad de convertidor de datos 50 puede transferir de esta manera una clave (clave 1, clave 2) como está.

A continuación, se dará ahora una descripción de una operación de la unidad de convertidor de datos 50 para transferir datos.

La señal de entrada de la señal de transferencia de datos FL es 0. La señal de transferencia de claves FL y la señal de máscara FL continúa teniendo 1.

El circuito AND 51 permite pasar a través datos y los bits inferiores de los datos pasados a través se introducen al circuito EXOR 55. El circuito AND 60 recibe 0 de la señal de transferencia de datos FL, de manera que 0 se saca desde el circuito AND 60. Los bits inferiores de los datos introducidos al circuito EXOR 55 pasan a través del circuito EXOR 55 y entonces se sacan como los datos inferiores de la señal de salida.

De manera similar, el circuito AND 59 saca 0 debido a que la señal de transferencia de datos FL es 0. Los bits inferiores de datos introducidos al circuito EXOR 56 pasan a través del circuito EXOR 56 y entonces se sacan como los datos superiores de la señal de salida.

De esta manera, la unidad de convertidor de datos 50 puede transferir los datos como están.

Por lo tanto, la señal de transferencia de claves, tal como la señal de transferencia de claves FL y la señal de transferencia de claves FL^{-1} y la señal de máscara que tiene la señal de máscara FL y la señal de máscara FL^{-1}, trasfieren una clave y la señal de transferencia de datos FL transfiere datos.

Conversión subordinada – subconvertidor 330 – unidad de convertidor de datos 50 con función de transferencia de claves y unidad de inversor de datos 70 con función de transferencia de claves y función de transferencia de datos.

La Fig. 17 es un diagrama que ilustra una configuración interna del subconvertidor 330 en el que la unidad de convertidor de datos 50 se dota con la función de transferencia de claves y la unidad de inversor de datos 70 se dota con la función de transferencia de claves y la función de transferencia de datos.

La configuración y la operación de la unidad de convertidor de datos 50 son las mismas que las del aparato de conversión de datos de la Fig. 10 con la función de transferencia de claves y por lo tanto no se tratarán aquí.

La unidad de inversor de datos 70 opera igual que lo hace la unidad de convertidor de datos 50 de la Fig. 16. De esta manera, la operación de la unidad de inversor de datos 70, tratada anteriormente, no se reiterará aquí en detalle.

Conversión subordinada – subconvertidor 330 – unidad de convertidor de datos 50 y unidad de inversor de datos 70 ambas con función de transferencia de claves y función de transferencia de datos.

La Fig. 18 es un diagrama que ilustra una configuración del subconvertidor en el que la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 se dotan ambas con la función de transferencia de claves y la función de transferencia de datos.

Las operaciones de transferencia realizadas por la unidad de convertidor de datos 50 y la unidad de inversor de datos 70, tratadas anteriormente, no se reiterarán aquí. En esta realización, tanto la unidad de convertidor de datos 50 como la unidad de inversor de datos 70 se dotan con la función de transferencia de claves y la función de transferencia de datos, de manera que se permite al aparato de conversión de datos que realice un proceso sofisticado de transferencia de una clave y datos.

Conversión subordinada – subconvertidor 330 – unidad de convertidor de datos 50 con función de transferencia de claves y función de transferencia de datos.

La Fig. 19 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 se dota con la función de transferencia de claves y la función de transferencia de datos y la unidad de inversor de datos 70 no tiene ninguna de esas funciones de transferencia.

Las operaciones de la unidad de convertidor de datos 50 y la unidad de inversor de datos 70, tratadas anteriormente, no se reiterarán aquí.

Conversión subordinada – subconvertidor 330 –unidad de inversor de datos 70 con función de transferencia de claves y función de transferencia de datos.

La Fig. 20 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de inversor de datos 70 se dota con la función de transferencia de claves y la función de transferencia de datos y la unidad de convertidor de datos 50 no se dota con ninguna de esas funciones de transferencia.

Las operaciones detalladas de la unidad de convertidor de datos 50 y la unidad de inversor de datos 70, tratadas anteriormente, no se reiterarán aquí.

Conversión subordinada – subconvertidor 330 – unidad de convertidor de datos 50 con función de transferencia de claves y función de transferencia de datos y unidad de inversor de datos 70 con función de transferencia de datos.

La Fig. 21 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 se dota tanto con la función de transferencia de claves como la función de trasferencia de datos y la unidad de inversor de datos 70 se dota con la función de transferencia de datos.

Las operaciones de la unidad de convertidor de datos 50 y la unidad de inversor de datos 70, tratadas anteriormente, no se reiterarán aquí.

Conversión subordinada – subconvertidor 330 – unidad de inversor de datos 70 con función de transferencia de claves y función de transferencia de datos y unidad de convertidor de datos 50 con función de transferencia de datos.

La Fig. 22 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 se dota con la función de transferencia de datos y la unidad de inversor de datos 70 se dota con la función de transferencia de claves y la función de transferencia de datos.

Las operaciones de la unidad de convertidor de datos 50 y la unidad de inversor de datos 70, tratadas anteriormente, no se reiterarán aquí.

Conversión subordinada – subconvertidor 330 – unidad de convertidor de datos 50 con función de transferencia de datos y unidad de inversor de datos 70 con función de transferencia de claves.

La Fig. 23 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 se dota con la función de transferencia de datos y la unidad de inversor de datos 70 se dota con la función de transferencia de claves.

Las operaciones respectivas de las mismas, tratadas anteriormente, no se reiterarán aquí.

Conversión subordinada – subconvertidor 330 – unidad de convertidor de datos 50 con función de transferencia de claves y unidad de inversor de datos 70 con función de transferencia de datos.

La Fig. 24 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 se dota con la función de transferencia de claves y la unidad de inversor de datos 70 se dota con la función de transferencia de datos.

Las operaciones respectivas de las mismas, tratadas anteriormente, no se reiterarán aquí.

Conversión subordinada – subconvertidor 330 – unidad de inversor de datos 70 y unidad de convertidor de datos 50 conectadas en serie – unidad de convertidor de datos 50 y unidad de inversor de datos 70 ambas con función de transferencia de datos.

La Fig. 25 es un diagrama que ilustra una configuración en la que la unidad de inversor de datos 70 y la unidad de convertidor de datos 50 se conectan en serie y la unidad de inversor de datos 70 se dota con la función de transferencia de datos y la unidad de convertidor de datos 50 también se dota con la función de transferencia de datos.

Las operaciones internas respectivas de las mismas, tratadas anteriormente, no se reiterarán aquí.

Con la configuración mostrada en la Fig. 25, los datos transferidos por la unidad de inversor de datos 70 se introducen a la unidad de convertidor de datos 50 y entonces se sacan como la señal de salida que se transfiere además por la unidad de convertidor de datos 50.

La unidad de inversor de datos 70 y la unidad de convertidor de datos 50 dispuestas en serie de esta manera y conectadas en serie permiten la conversión de datos lineal no solamente realizada tanto por la unidad de convertidor de datos 50 como la unidad de inversor de datos 70 sino realizada también por la unidad de inversor de datos 70 sola o por la unidad de convertidor de datos 50 sola. Más particularmente, es posible que los datos lineales convertidos por la unidad de inversor de datos 70 se introduzcan a la unidad de convertidor de datos 50, donde los datos recibidos se transfieren sin realizar una conversión lineal. También es posible que la unidad de inversor de datos 70 transfiera datos recibidos a la unidad de convertidor de datos 50 y la unidad de convertidor de datos 50 sola realice una conversión de datos lineal.

Por consiguiente, esta es la configuración que es eficaz para el caso donde los datos vayan a ser convertidos por la unidad de convertidor de datos 50 sola o la unidad de inversor de datos 70 sola. El mismo efecto se puede lograr por los subconvertidores 330 mostrados en la Fig. 26 hasta la Fig. 30 en discusiones posteriores.

Conversión subordinada – subconvertidor 330 – unidad de convertidor de datos 50 y unidad de inversor de datos 70 conectadas en serie – unidad de convertidor de datos 50 y unidad de inversor de datos 70 ambas con función de transferencia de datos.

La Fig. 26 es una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 de la Fig. 25 invierten la posición.

La operación y el efecto de las mismas son los mismos que los del subconvertidor 330 de la Fig. 25 y por lo tanto no se tratarán aquí.

Conversión subordinada – subconvertidor 330 – unidad de convertidor de datos 50 y unidad de inversor de datos 70 conectadas en serie – unidad de convertidor de datos 50 con función de transferencia de claves y función de transferencia de datos y unidad de inversor de datos 70 ambas con función de transferencia de datos.

La Fig. 27 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 de la Fig. 26 se añade con la función de transferencia de claves.

Las configuraciones internas y operaciones de la unidad de convertidor de datos 50 y la unidad de inversor de datos 70, tratadas anteriormente, no se reiterarán aquí.

Conversión subordinada – subconvertidor 330 – unidad de inversor de datos 70 y unidad de convertidor de datos 50 conectadas en serie – unidad de convertidor de datos 50 con función de transferencia de claves y función de transferencia de datos y unidad de inversor de datos 70 ambas con función de transferencia de datos.

La Fig. 28 muestra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 invierten la posición.

Las configuraciones internas y las operaciones de la unidad de convertidor de datos 50 y la unidad de inversor de datos 70, tratadas anteriormente, no se reiterarán aquí.

Conversión subordinada – subconvertidor 330 – unidad de convertidor de datos 50 y unidad de inversor de datos 70 conectadas en serie – unidad de convertidor de datos 50 con función de transferencia de datos y unidad de inversor de datos 70 con función de transferencia de claves y función de transferencia de datos.

La Fig. 29 es un diagrama que ilustra una configuración en la que la unidad de inversor de datos 70 de la Fig. 26 se añade con la función de transferencia de claves.

Las configuraciones y operaciones de la unidad de convertidor de datos 50 y la unidad de inversor de datos 70, tratadas anteriormente, no se reiterarán aquí.

Conversión subordinada – subconvertidor 330 – unidad de inversor de datos 70 y unidad de convertidor de datos 50 conectadas en serie – unidad de convertidor de datos 50 con función de transferencia de datos y unidad de inversor de datos 70 con función de transferencia de claves y función de transferencia de datos.

La Fig. 30 muestra una configuración del subconvertidor 330 en el que la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 de la Fig. 29 invierten la posición.

Las configuraciones internas y las operaciones de las mismas, tratadas anteriormente, no se reiterarán aquí.

De esta manera, la señal de transferencia de claves FL y la señal de transferencia de claves FL^{-1} tienen la función de inhibir y de esta manera anular datos de entrada y la señal de máscara FL y la señal de máscara FL^{-1} tienen la función de permitir pasar a través una clave de entrada.

Entonces, la señal de transferencia de datos FL y la señal de transferencia de datos FL^{-1} tienen la función de anular una clave de entrada para permitir pasar a través datos.

Todas de las seis señales mencionadas anteriormente son señales de transferencia. Tras la no recepción de esas señales de transferencia, la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 realizan la conversión lineal de datos que suponen hacer, como se muestra en la técnica relacionada.

Conversión subordinada – subconvertidor 330 – unidad de convertidor de datos 50 y unidad de inversor de datos 70 conectadas en serie – unidad de convertidor de datos 50 y unidad de inversor de datos 70 ambas con función de transferencia de claves y función de transferencia de datos.

La Fig. 62 incluye la configuración de la unidad de convertidor de datos 50 mostrada en la Fig. 27 y la configuración de la unidad de inversor de datos 70 mostrada en la Fig. 29. Más particularmente, la unidad de convertidor de datos

50 y la unidad de inversor de datos 70 conectadas en serie ambas se dotan con la función de transferencia de claves y la función de transferencia de datos.

Las configuraciones y las operaciones de la unidad de convertidor de datos 50 y la unidad de inversor de datos 70, tratadas anteriormente, no se reiterarán aquí.

Conversión subordinada – subconvertidor 330 – unidad de inversor de datos 70 y unidad de convertidor de datos 50 conectadas en serie – unidad de convertidor de datos 50 y unidad de inversor de datos 70 ambas con función de transferencia de claves y función de transferencia de datos.

La Fig. 63 incluye una configuración del subconvertidor 330 en el cual la unidad de convertidor de datos 50 y unidad de inversor de datos 70 de la Fig. 62 invierten la posición.

Las configuraciones internas y las operaciones de las mismas, tratadas anteriormente, no se reiterarán aquí.

Realización 4.

En esta realización, se dará una descripción de una configuración y una operación de una 1/2 unidad de subconvertidor 90, en la cual la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 se implementan en un circuito compartido, que se dota con la función de transferencia de claves y la función de transferencia de datos.

Conversión subordinada – subconvertidor 330 – 1/2 unidad de subconvertidor 90 con función de transferencia de claves y función de transferencia de datos.

La Fig. 31 es un diagrama que ilustra una configuración del subconvertidor 330 en el que la 1/2 unidad de subconvertidor 90 se añade con la función de transferencia de claves y la función de transferencia de datos.

En contraste con la Fig. 59 explicada en la técnica relacionada, se añaden la señal de transferencia de claves, la señal de máscara y la señal de transferencia de datos. Entonces, en conexión con esas señales de transferencia que se introducen, se proporcionan circuitos adicionales para transferir una clave y datos.

En primer lugar, una señal de conmutación es una señal para conmutar entre la unidad de convertidor de datos 50 y la unidad de inversor de datos 70. En el caso donde la señal A se selecciona por la señal de conmutación de entre la señal A y la señal E introducidas al selector 2-1 99a y entonces se saca como la señal de salida B y la señal C se selecciona por la señal de conmutación de entre la señal C y la señal F introducidas al selector 2-1 99b y entonces se saca como la señal de salida D, la 1/2 unidad de subconvertidor 90 realiza la misma conversión de datos que la realizada por la unidad de convertidor de datos 50.

Por otra parte, en el caso donde el selector 2-1 99a seleccione la señal E como la señal de salida B mediante la señal de conmutación y el selector 2-1 99b seleccione la señal F como la señal de salida B mediante la señal de conmutación, la 1/2 unidad de subconvertidor 90 realiza la misma conversión de datos que la realizada por la unidad de inversor de datos 70.

En el caso donde la 1/2 unidad de subconvertidor 90 funcione como la unidad de convertidor de datos 50 mediante la señal de conmutación, la operación ilustrada en la Fig. 31 es la misma que la realizada por la unidad de convertidor de datos 50 mostrada en la Fig. 18. Específicamente, la señal de transferencia de claves corresponde a la señal de transferencia de claves FL de la Fig. 18, la señal de máscara corresponde a la señal de máscara FL de la Fig. 18 y la señal de transferencia de datos corresponde a la señal de transferencia de datos FL de la Fig. 18.

Más particularmente, cada circuito corresponde como sigue. Un circuito 98 corresponde al circuito AND 51 (Fig. 18). Un circuito 91 corresponde al circuito EXOR 55 (Fig. 18). Un circuito 95 corresponde al circuito AND 60 (Fig. 18). Un circuito 101 corresponde al circuito AND 54 (Fig. 18). Un circuito 94 corresponde al circuito OR 53 (Fig. 18). Un circuito 100 corresponde al circuito NOT 52 (Fig. 18). Un circuito 96 corresponde al circuito AND 58 (Fig. 18). Un circuito 92 corresponde al circuito OR 57 (Fig. 18). Un circuito 97 corresponde al circuito AND 59 (Fig. 18). Un circuito 93 corresponde al circuito EXOR 56 (Fig. 18).

La 1/2 unidad de subconvertidor 90, con tal correspondencia, puede cumplir la función de la unidad de convertidor de datos 50 de la Fig. 18. Mas particularmente, llega a ser posible que la 1/2 unidad de subconvertidor 90 realice una conversión de datos y también transfiera la clave (clave 1, clave 2), tras la recepción de la señal de transferencia de claves, sacando una clave de entrada como la señal de salida. Estas operaciones tratadas anteriormente son las mismas que las de la unidad de convertidor de datos 50 de la Fig. 18 y por lo tanto no se tratarán aquí.

En el caso donde la 1/2 unidad de subconvertidor 90 funcione como la unidad de inversor de datos 70 mediante la señal de conmutación, la operación de la 1/2 unidad de subconvertidor 90 de la Fig. 31 es la misma que la de la unidad de inversor de datos 70 de la Fig. 18. Específicamente, la señal de transferencia de claves corresponde a la señal de transferencia de claves FL^{-1} de la Fig. 18, la señal de máscara corresponde a la señal de máscara FL^{-1} de la Fig. 18 y la señal de transferencia de datos corresponde a la señal de transferencia de datos FL^{-1} de la Fig. 18.

Más particularmente, cada circuito corresponde como sigue. El circuito 98 corresponde al circuito AND 71 (Fig. 18), el circuito 91 corresponde al circuito EXOR 76 (Fig. 18), el circuito 95 corresponde al circuito AND 80 (Fig. 18), el circuito 101 corresponde al circuito AND 77 (Fig. 18), el circuito 94 corresponde al circuito OR 78 (Fig. 18), el circuito 96 corresponde al circuito AND 73 (Fig. 18), el circuito 92 corresponde al circuito OR 74 (Fig. 18), el circuito 97 corresponde al circuito AND 79 (Fig. 18) y el circuito 93 corresponde al circuito EXOR 75 (Fig. 18).

La 1/2 unidad de subconvertidor 90, con tal correspondencia, puede cumplir la función de la unidad de inversor de datos 70 de la Fig. 18. Más particularmente, llega a ser posible que la 1/2 unidad de subconvertidor 90 realice una conversión de datos inversa y también transfiera la clave (clave 3, clave 4), tras la recepción de la señal de transferencia de claves, sacando una clave de entrada como la señal de salida. Esas operaciones tratadas anteriormente son las mismas que las de la unidad de inversor de datos 70 de la Fig. 18 y por lo tanto no se tratarán aquí.

Conversión subordinada – subconvertidor 330 – 1/2 unidad de subconvertidor 90 con función de transferencia de datos.

La Fig. 32 es un diagrama que ilustra una configuración del subconvertidor en la que la 1/2 unidad de subconvertidor 90 se añade con la función de transferencia de datos.

Como el caso de la Fig. 31, la 1/2 unidad de subconvertidor 90 tiene la misma función que la de la unidad de convertidor de datos 50 de la Fig. 13 en el caso donde la señal A se seleccione por el selector 2-1 99a y la señal C se seleccione por el selector 2-1 99b. En este caso, la señal de transferencia de datos corresponde a la señal de transferencia de datos FL.

La 1/2 unidad de subconvertidor 90, por otra parte, tiene la misma función que la de la unidad de inversor de datos 70 de la Fig. 14 en el caso donde la señal E se seleccione por el selector 2-1 99a y la señal F se seleccione por el selector 2-1 99b mediante la señal de conmutación. En este caso, la señal de transferencia de datos corresponde a la señal de transferencia de datos FL^{-1}.

La 1/2 unidad de subconvertidor 90, configurada de esta manera, puede realizar una conversión de datos y también transferir datos sin realizar la conversión de datos sacando datos tras la recepción de la señal de transferencia indicando una transferencia de datos.

Esas operaciones, tratadas anteriormente, no se reiterarán aquí.

Conversión subordinada – subconvertidor 330 – 1/2 unidad de subconvertidor 90 con función de transferencia de claves.

La Fig. 33 es un diagrama que ilustra una configuración del subconvertidor 330 en la que la 1/2 unidad de subconvertidor 90 se añade con la función de transferencia de claves.

Como el caso de la Fig. 31, la 1/2 unidad de subconvertidor 90 funciona igual que la unidad de convertidor de datos 50 de la Fig. 10 en el caso donde la señal A se seleccione por el selector 2-1 99a y la señal C se seleccione por el selector 2-1 99b. En este caso, la señal de transferencia de claves y la señal de máscara corresponden a la señal de transferencia de claves FL y la señal de máscara FL, respectivamente.

La 1/2 unidad de subconvertidor 90, por otra parte, funciona igual que la unidad de inversor de datos 70 de la Fig. 11 en el caso donde la señal E se seleccione por el selector 2-1 99a y la señal F se seleccione por el selector 2-1 99b mediante la señal de conmutación. En este caso, la señal de transferencia de claves y la señal de máscara corresponden a la señal de transferencia de claves FL^{-1} y la señal de máscara FL^{-1}, respectivamente.

La 1/2 unidad de subconvertidor 90 configurada de esta manera puede realizar una conversión de datos y también transferir datos sin realizar la conversión de datos sacando datos tras la recepción de una señal de transferencia indicando una transferencia de datos.

Esas operaciones, tratadas anteriormente, no se reiterarán aquí.

Como se trata en esta realización, la 1/2 unidad de subconvertidor 90 configurada para implementar la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 en el circuito compartido se dotan de esta manera con la función de transferencia de claves y la función de transferencia de datos. Esto permite reducir el tamaño del aparato de conversión de datos sobre todo reduciendo el tamaño del subconvertidor 330 y evitando el aumento de selectores que resulta de la eliminación de la necesidad de los caminos de claves y los caminos de datos logrados como se trató anteriormente.

Con referencia a la primera hasta la cuarta realizaciones, los aparatos de conversión de datos para cifrado de bloques se trataron centrándose en las configuraciones de CAMELLIA. No obstante, los subconvertidores 330 dotados con la función de transferencia tratada anteriormente también son aplicables a cualquier aparato de conversión de datos que realiza cifrado de bloques, tal como CAMELLIA, MISTY, KASUMI.

Los aparatos de conversión de datos tratados con referencia a la Fig. 1, Fig. 6 o Fig. 7, pueden tener uno o dos selectores 2-1 que se incluyen en el selector 310.

En comparación con eso, el aparato de conversión de datos de la técnica relacionada tratada anteriormente requiere tres selectores 2-1 a fin de seleccionar una señal de salida de entre cuatro señales como se muestra en la Fig. 56.

Además, en el caso del aparato de conversión de datos que usa la función 1/2F mostrada en la Fig. 60, se requieren cuatro selectores 2-1 a fin de seleccionar una señal de salida de entre cinco señales de entrada.

Consecuentemente, los aparatos de conversión de datos mostrados en la Fig. 1, Fig. 6 o Fig. 7 permiten reducir el número de selectores incluidos en el aleatorizador de datos 30 en comparación con el aparato de conversión de datos de la técnica relacionada.

Además, con referencia al aparato de conversión de datos mostrado en la Fig. 7, el convertidor principal 320 y el subconvertidor 330 se disponen en paralelo y por ello se requiere un selector 340. El selector 340 se compone de un único selector 2-1 que recibe dos señales de salida sacadas desde el convertidor principal 320 y el subconvertidor 330, respectivamente y selecciona una señal de entre las dos señales recibidas. De esta manera, hay dos selectores 2-1 que se requieren para el selector 310 y el selector 340 en la Fig. 7.

Por consiguiente, el aparato de conversión de datos mostrado en la Fig. 7 también permite reducir el número de selectores incluidos en el aleatorizador de datos 30 en comparación con el aparato de conversión de datos de la técnica relacionada.

Realización 5.

En esta realización, se dará una descripción del cifrado de bloque CAMELLIA en el que el convertidor principal 320 y el subconvertidor 330 se disponen en paralelo.

CAMELLIA soporta una longitud de bloque de 128 bits y está disponible para su uso una longitud de clave de 128, 192 o 256 bits.

La estructura de algoritmo es la estructura FEISTEL caracterizada anteriormente. Básicamente, el proceso de cifrado y el proceso de descifrado se pueden implementar en el mismo hardware o software.

La función F es dependiente de la longitud de la clave, es decir, 18 vueltas para una clave de 128 bits (6 vueltas x 3 del convertidor principal 320 de la Fig. 34) y 24 vueltas para una clave de 192 o 256 bits como se muestra en la Fig. 54 y la Fig. 55. La Fig. 54 y la Fig. 55 se tratarán más tarde.

La Fig. 34 es un diagrama que ilustra un proceso de cifrado de CAMELLIA para una clave de 128 bits. Específicamente, la Fig. 34 muestra el caso donde P (texto plano) se somete a una conversión de datos (descifrado de datos) usando el convertidor principal 320 y el subconvertidor 330 y entonces se saca C (texto cifrado). Con la Fig. 34, FL (una función de conversión de datos) y FL^{-1} (una función de conversión inversa de datos) se colocan entre cada función F de seis vueltas.

La Fig. 34 en la izquierda muestra la misma operación que la realizada por el aleatorizador de datos 30 de la Fig. 4. Particularmente, el circuito EXOR 31a y el circuito EXOR 31b de la Fig. 4 corresponden a un circuito EXOR 600 y un circuito EXOR 601 de la Fig. 34, respectivamente y en la práctica, EXOR incluida en el subconvertidor 330 operan el proceso. Se tiene que asumir que todas las claves de entrada mostradas en la Fig. 34 se han programado y sacado desde el programador de claves como se muestra en la Fig. 4.

La Fig. 34 en la derecha muestra un diagrama que es el mismo que el de la Fig. 57.

La Fig. 35 es un diagrama que ilustra un proceso de descifrado de CAMELLIA para una clave de 128 bits.

La Fig. 35 muestra el caso donde C (texto cifrado) se somete a una conversión de datos usando el convertidor principal 320 y el subconvertidor 330 y entonces se saca P (texto descifrado).

Las operaciones mostradas en la Fig. 34 y la Fig. 35, tratadas anteriormente, no se reiterarán aquí.

Se dará ahora una descripción en detalle de un interior de la función F de CAMELLIA.

La Fig. 36 es un diagrama que ilustra una configuración interna de la función F de CAMELLIA.

La función F de CAMELLIA emplea estructura SPN dentro y los datos se procesan básicamente en unidades de ocho bits para datos de entrada (1) hasta datos de entrada (8). La función F de CAMELLIA incluye una función S 324 que se compone de cajas S y conversión lineal mediante OR exclusivas (EXOR) que se llama función P 325.

En la función F 321, al principio, se introducen datos de entrada (1) hasta datos de entrada (8) que tienen respectivamente una longitud de ocho bits, entonces los 64 bits de los datos de entrada se someten a una operación XOR con 64 bits de claves (1) hasta (8) de ocho bits, respectivamente y entonces se sacan. Los datos de salida se

introducen a la función S 324 y entonces se convierten no linealmente de una forma por byte mediante la función S 324 que sintetiza la operación aritmética inversa de GF (2^8) y conversión afín.

Los datos entonces se someten a una conversión lineal basada en OR exclusiva mediante la función P 325. A través de estas operaciones, se aleatorizan los datos y luego se sacan como datos de salida (1) hasta datos de salida (8).

La función de CAMELLIA soporta una anchura de datos de 64 bits. La Fig. 36 muestra dos conjuntos de cajas S S_1 hasta S_4 proporcionadas en la función S 324 (un conjunto de S_1, S_2, S_3 y S_4 de la parte inferior de la Fig. 36 y otro conjunto de S_2, S_3, S_4 y S_1 por encima de ella).

Por lo tanto, como se muestra en la Fig. 36, el proceso también se puede hacer manejando en primer lugar los datos de entrada (1) hasta los datos de entrada (4) para conversión de datos y luego manejando los datos de entrada restantes de los datos de entrada (5) hasta los datos de entrada (8). Con este caso, en la segunda vuelta de conversión de datos, a fin de usar el circuito como está con las cajas S que están dispuestas en el orden de S_1 a S_4, los datos van a ser sometidos al desplazamiento de rotación de un byte por adelantado y entonces se introducen los datos de entrada (5) hasta los datos de entrada (8) que se han sometido al desplazamiento de rotación por adelantado. Esto permite a los datos corresponder a las cajas S S_1 hasta S_4 sin cambiar la estructura de la función S 324.

De esta manera, la función F implementa una conversión de datos no lineal a través de las operaciones de EXOR (OR exclusiva) entre claves y datos de entrada, dos vueltas de operaciones por los cuatro tipos de función S (S_1 hasta S_4) y operaciones por la función P 325. La operación típica de CAMELLIA, incluyendo la función S 324 por las cajas S (circuito aritmético inverso en GF (2^8) + conversión afín) S_1 hasta S_4, la función P 325, la función de conversión de datos (FL) y la función de conversión de datos inversa (FL^{-1}), se pueden implementar mediante una simple combinación de algebras booleanas.

Se dará ahora una descripción en detalle de una configuración general y una operación de CAMELLIA.

La Fig. 37 es un diagrama que ilustra una configuración general y una operación de CAMELLIA.

Con CAMELLIA, si la clave secreta a ser introducida es una clave de 128 bits, la clave se extiende internamente a la clave de 256 bits y la clave extendida como la clave extendida se usa para cifrado/descifrado de datos.

Si la clave secreta a ser introducida es una clave de 192 o 256 bits, la clave se extiende internamente a una clave de 512 bits a ser usada para cifrado/descifrado de datos. El caso de una clave de 192 o 256 bits se tratará más tarde.

En primer lugar, se dará ahora una descripción de un rasgo estructural de CAMELLIA.

El algoritmo entero de CAMELLIA se implementa a través de operaciones repetidas de la misma función F mediante el convertidor principal 320. La función F se configura como se muestra en la Fig. 36.

En el aleatorizador de datos 30, como ilustran el circuito EXOR 31a y el circuito EXOR 31b de la Fig. 4, se realiza una OR exclusiva entre los datos de entrada o de salida y una clave. Esto se llama blanqueo.

También, en el aleatorizador de datos 30, el subconvertidor 330 que incluye conversión de datos (FL) y conversión inversa de datos (FL^{-1}) se coloca entre los convertidores principales 320 incluyendo una función F de seis vueltas. Esto se muestra en la Fig. 34 y la Fig. 35.

Como se mencionó anteriormente, la clave extendida (una clave intermedia + una clave de salida) se genera como se muestra en la Fig. 2.

Esto muestra que el aparato de conversión de datos para implementar el algoritmo CAMELLIA se puede configurar con el subconvertidor 330 que incluye conversión de datos (FL) y conversión de datos inversa (FL^{-1}), la función P 325 y los cuatro tipos de cajas S.

La función P 325 puede llegar a ser más pequeña estando basada por escrito en el método de escritura que se indica en la “Specification of *Camellia* – a 128-bits Block Cipher”.

Específicamente, según la especificación antes mencionada, la función P se puede escribir como sigue.

$z1' = z1 + z3 + z4 + z6 + z7 + z8$

$z2' = z1 + z2 + z4 + z5 + z7 + z8$

$z3' = z1 + z2 + z3 + z5 + z6 + z8$

$z4' = z2 + z3 + z4 + z5 + z6 + z7$

$z5' = z1 + z2 + z6 + z7 + z8$

$z6' = z2 + z3 + z5 + z7 + z8$

$z7' = z3 + z4 + z5 + z6 + z8$

$z8' = z1 + z4 + z5 + z6 + z7$

"+" en las ecuaciones anteriores para calcular z1' hasta z8' indica una operación OR exclusiva.

La z1 hasta z8 son salidas desde S1, S2, S3, S4, S5 (=S2), S6 (=S3), S7 (=S4) y S8 (=S1), respectivamente. Ahora, si z5 hasta z8 se convierte en zz2, zz3, zz4 y zz1, respectivamente, entonces los resultados son los siguientes.

$z1' = z1 + z3 + z4 + zz1 + zz3 + zz4$

$z2' = z1 + z2 + z4 + zz1 + zz2 + zz4$

$z3' = z1 + z2 + z3 + zz1 + zz2 + zz3$

$z4' = z2 + z3 + z4 + zz2 + zz3 + zz4$

$z5' = z1 + z2 + zz1 + zz3 + zz4$

$z6' = z2 + z3 + zz1 + zz2 + zz4$

$z7' = z3 + z4 + zz1 + zz2 + zz3$

$z8' = z1 + z4 + zz2 + zz3 + zz4$

En base a esto, operar en dos relojes, tal como operar S1 hasta S4 para sacar Z1 hasta Z4 y operar S1 hasta S4 para sacar zz1 hasta zz4, etc., permite reducir el circuito de la función P aproximadamente en la mitad de tamaño.

Se dará ahora una descripción de un aparato de conversión de datos para CAMELLIA con referencia a la Fig. 37.

El aparato de conversión de datos para CAMELLIA mostrado en la Fig. 37 incluye el convertidor principal 320 y el subconvertidor 330 dispuestos en paralelo.

El subconvertidor 330 incluye la unidad de convertidor de datos 50 y la unidad de inversor de datos 70.

El convertidor principal 320 tiene la unidad de función F que consta de función 1/2F. En el caso donde el convertidor principal 320 se configura con la función F o menos de una función F, es decir, $1/2^x$ ($x \geq 1$) de la función F, como se ejemplifica con la función 1/2F de la Fig. 61, va a ser mantenido un resultado de salida desde el circuito EXOR 1322a, que es un resultado intermedio del proceso mediante la unidad de función F 1321a y el proceso mediante la unidad de función F 1321b.

En general, si se reduce el número de unidades de la función F instalada y se emplea un método de implementación de una conversión de datos basada en una función F de una vuelta en una pluralidad de veces de arquitectura en bucle, entonces se reduce el tamaño del circuito para la función F. No obstante, se aumentan el número de circuitos de control para controlar el bucle y el número de circuitos tales como selectores para introducir claves a cada función F. De esta manera, hay una relación de compromiso entre el tamaño de circuito para la función F y el tamaño de circuito para control en bucle.

Por lo tanto, en la persecución de la reducción de tamaño de un aparato de conversión de datos para CAMELLIA, se necesita un estudio sobre el número de la función F a ser instalada y el número de repeticiones. Más específicamente, se debería llevar a cabo un estudio cuidadoso sobre si implementar un aparato de conversión de datos para CAMELLIA mediante una única función F instalada en el convertidor principal 320, si reducir el número de cajas S instaladas en la función F y lograr una conversión de datos basada en una función F de una vuelta a través de una operación en varios ciclos, etc. Este es un estudio sobre la relación de compromiso entre la reducción en tamaño del circuito empleando la unidad de función F de menos de una función F y el aumento en el tamaño del circuito empleando el bucle acompañado por el aumento en el número de selectores, etc.

Además con CAMELLIA, como se mencionó anteriormente, como la función para generar la clave de salida (clave KA), se usa parte del convertidor principal 320 en el aleatorizador de datos 30. Por esta razón, también se necesita otro estudio cuidadoso sobre un efecto del aumento de selectores, etc. que se añade para usar la función F del aleatorizador de datos 30.

Como se trató con referencia a la Fig. 36, con la función F de CAMELLIA, los cuatro tipos de cajas S (S_1, S_2, S_3 y S_4) para entrada/salida de 8 bits se usan dos veces cada uno. Entonces, se necesita aquí otro estudio sobre si instalar ocho unidades de las cajas S o instalar cuatro unidades con repetición dos veces o similar.

Según "On Hardware Implementation of 128-bits Block Ciphers (III)" descrita en las Actas del Simposio 2001 sobre Criptografía y Seguridad de la Información, el tamaño del circuito para una única caja S incluye aproximadamente

200 puertas y por lo tanto si el número de cajas S se reduce por cuatro desde 8 a 4, entonces se pueden reducir aproximadamente 800 puertas.

Por otra parte, se requieren al menos 32 unidades de selectores 2-1 (aproximadamente 100 puertas de circuitos NAND) para repeticiones que están en la relación de compromiso.

A partir de este hecho, se espera que el circuito llegue a ser más pequeño con la instalación de cuatro unidades de cajas S con repetición de dos veces en lugar de instalar ocho unidades.

De esta manera, con la unidad de función F 321 del aparato de conversión de datos para CAMELLIA, se puede hacer una conversión de datos una vez con ocho unidades de cajas S instaladas y alternativamente se puede hacer una conversión de datos con cuatro unidades de cajas S instaladas que implican repetición de dos veces de conversión de datos. Se puede usar cualquiera de las dos. No obstante, en vista del tamaño del circuito, es deseable la de repetición de dos veces de conversión de datos.

En el caso de usar el algoritmo CAMELLIA mostrado en la Fig. 37, se puede implementar cifrado/descifrado de datos mediante el ciclo del generador intermedio 40 según esta secuencia.

Los pasos de procesamiento del ciclo del generador de claves intermedias 40 se describirán ahora más adelante.

En primer lugar, en el paso 1, se realiza Blanqueo usando el subconvertidor 330.

Entonces, en el paso 2, se realiza una operación de la mitad de una vuelta de la función F (función 1/2F) usando el convertidor principal 320.

De manera similar, en el paso 3, se realiza una operación para la otra mitad de una vuelta de la función F (función 1/2F) usando el convertidor principal 320.

En el paso 4 hasta el paso 13, el paso 2 y el paso 3 se repiten cinco veces.

En el paso 14, se realiza una operación para la función de conversión de datos (FL) y la función de conversión de datos inversa (FL^{-1}) del subconvertidor 330 para conversión de datos.

Entonces, en el paso 15 hasta el paso 27, se repiten el paso 2 hasta el paso 14.

Entonces, en el paso 28 hasta el paso 39, se repiten el paso 2 hasta el paso 13.

Por último, en el paso 40, se realiza el mismo Blanqueo que el del paso S1.

Señalar aquí que el paso 1 indica que la operación realizada por el circuito EXOR 31a de la Fig. 4 y el paso 40 indica la operación realizada por el circuito EXOR 31b de la Fig. 4. En otras palabras, el circuito EXOR 31a y el circuito EXOR 31b operan usando las EXOR de la unidad de convertidor de datos 50 y la unidad de inversor de datos 70, respectivamente, en el subconvertidor 330.

La configuración y la operación del generador de claves 20 son las mismas que las tratadas anteriormente y por lo tanto no se reiterarán aquí.

En el paso 2 y el paso 3 tratados anteriormente, se realiza una conversión de datos basada en una función F única en dos ciclos mediante el convertidor principal 320. Una operación de este proceso de datos se tratará ahora en detalle con referencia a la Fig. 37 y la Fig. 64.

La Fig. 64 es diferente de la Fig. 61 de manera que se introduce en primer lugar una clave inferior como una clave de entrada y entonces se introduce una clave superior para implementar el proceso.

En primer lugar, se tratará en detalle una operación del paso 1. Los datos de entrada P (texto plano o texto descifrado) se seleccionan por un selector 2-1 311 y dividen en datos superiores y datos inferiores. Los datos superiores se someten a Blanqueo por la unidad de convertidor de datos 50 en el subconvertidor 330 y los datos inferiores se introducen a la unidad de inversor de datos 70 en el subconvertidor 330 y someten de manera similar a Blanqueo. Los datos superiores y los datos inferiores sometidos a Blanqueo se introducen a un selector 2-1 H 341 y un selector 2-1 342 en un selector 2-1 340, respectivamente. Cada pieza de los datos de entrada se selecciona por el selector 2-1 H 341 o el selector 2-1 L 342 y entonces se mantiene en un registro aritmético H 351 o un registro aritmético L 352, respectivamente.

Se tratará ahora una operación del paso 2.

Los bits superiores de los datos superiores mantenidos en el registro aritmético H 351 se introducen a un selector 2-1 312, entonces los bits inferiores de los datos superiores se someten a desplazamiento de rotación de un byte y entonces se introducen al selector 2-1 312. El selector 2-1 312 selecciona los bits inferiores sometidos a desplazamiento de rotación de entre las dos entradas y saca los bits seleccionados al convertidor principal 320. El desplazamiento de rotación para los bits inferiores seleccionados de un byte permite aplicar e introducir

óptimamente los datos de entrada (5) hasta los datos de entrada (8) a las cajas S, como se muestra en la Fig. 36. En el convertidor principal 320, la mitad superior de la primera vuelta de conversión de datos mostrada en al Fig. 64 se realiza por la unidad de función F 321 que tiene una función 1/2F. Señalar aquí que la unidad de función F 321 de la Fig. 37 y las unidades de función F 1321a hasta 1321l de la Fig. 64 con la función 1/2F se configuran igual. Con referencia a una conversión de datos realizada por la unidad de función F 1321a de la Fig. 64, los bits de la mitad inferior de los datos superiores de entrada se convierten usando una clave 1L y entonces se sacan los datos convertidos al circuito EXOR 1322a. El circuito EXOR 1322a recibe datos convertidos sacados por la unidad de función F 1321a y se someten a una operación XOR entre los datos recibidos y los datos inferiores de entrada. En otras palabras, los datos (datos intermedios) sacados desde el convertidor principal 320 se introducen a un selector 3-1 L 342 y entonces se mantienen en un registro aritmético L 352. Al mismo tiempo, los datos superiores de P mantenidos en el registro aritmético H 351 pasan a través del selector 2-1 311 y entonces se transfieren, por medio de la función de transferencia de datos de la unidad de convertidor de datos 50 del subconvertidor 330, por ejemplo y se mantienen en el registro aritmético H 351 de nuevo a través del selector 2-1 H 341 desde el registro aritmético H 351.

A continuación, se dará ahora una descripción de una operación del paso 3.

El procesamiento de datos por la unidad de función F 1321b de la Fig. 64 se implementa en el segundo ciclo de procesamiento por el convertidor principal 320 de la Fig. 37. Específicamente, sin estar sometidos al desplazamiento de rotación de un byte, los bits superiores de los datos superiores introducidos al selector 2-1 312 se seleccionan por el selector 2-1 312 y entonces se sacan al convertidor principal 320. Mediante la aplicación de esta operación, los datos de los bits de la mitad superior de los datos superiores se convierten no linealmente por la unidad de función F 1321b y entonces se sacan al circuito EXOR 1322b. El circuito EXOR 1322b introduce al convertidor principal 320 los datos intermedios que se sacan desde el convertidor principal 320 y se mantienen en el registro aritmético L352 en el primer ciclo, como la otra señal de entrada y por ello los datos intermedios se introducen al circuito EXOR 1322b. Los datos de salida sometidos a una operación XOR en el circuito EXOR 1322b se seleccionan por el selector 2-1 H 341 y entonces se mantienen en el registro aritmético H 351. En esta etapa, los datos superiores de P se están manteniendo en el registro aritmético L 352 a través del selector 3-1 342. Esto significa que los datos superiores y los datos inferiores a ser usados para conversión de datos en la segunda vuelta en el convertidor principal 320 se mantienen en el registro aritmético H 351 y el registro aritmético L 352, respectivamente.

En los pasos 4 hasta 13, se repiten cinco veces los pasos 2 y 3.

Más particularmente, la conversión de datos de segunda vuelta se hace por la unidad de función F 1321c y el circuito EXOR 1322c en un ciclo y por la unidad de función F 1321d y el circuito EXOR 1322d en otro ciclo, el proceso en dos ciclos en total corresponde a los procesos del paso 4 y el paso 5. El proceso de la tercera vuelta a la sexta vuelta se realiza de la misma forma, lo cual corresponde a los procesos de los pasos 6 hasta 13.

Señalar, como se mencionó anteriormente, que las funciones de las unidades de función F 1321a hasta 1321l de la Fig. 64 son las mismas que la función de la unidad de función F 321 de la Fig. 37.

Se dará ahora una descripción de un proceso del paso 14.

Este proceso indica el proceso realizado por el subconvertidor 330 de la Fig. 37.

En primer lugar, los datos superiores y los datos inferiores, que se procesan en el paso 13 y entonces se mantienen en el registro aritmético H 351 y el registro aritmético L 352, respectivamente, se introducen al selector 2-1 311, entonces se seleccionan e introducen a la unidad de convertidor de datos 50 y la unidad de inversión de datos 70, respectivamente.

En la unidad de convertidor de datos 50 y la unidad de inversor de datos 70, los datos de entrada se someten a una conversión lineal. Entonces, los datos convertidos por la unidad de convertidor de datos 50 se introducen al selector 2-1 H 341 y los datos convertidos por la unidad de inversor de datos 70 se introducen al selector 3-1 L 342. Entonces, se seleccionan y mantienen en el registro aritmético H 351 y el registro aritmético L 352, respectivamente.

Los procesos de los pasos 15 hasta 27 corresponden a los procesos del convertidor principal 320 y el subconvertidor 330 de la Fig. 37.

Los procesos de los pasos 28 hasta 39 corresponden al proceso del convertidor principal 320 de la Fig. 37.

En el paso 40, como el paso 1, se realiza Blanqueo usando la EXOR del subconvertidor 330.

A través de esto pasos del generador de claves intermedias 40, llega a ser posible que un texto de cifrado C se saque a través del proceso de cifrado en caso de datos de entrada P que son un texto plano y un texto de descifrado C se saca después del proceso de descifrado por el mismo circuito para el proceso de cifrado, en caso de datos de entrada P que son texto cifrado.

Con el aparato de conversión de datos que usa CAMELLIA de la Fig. 37, la disposición en paralelo del convertidor principal 320 y el subconvertidor 330 permite ahorrar tiempo de ciclo para cada ciclo y mejorar la frecuencia de operación, en contraste con el caso de la disposición en serie de los mismos.

Además, con la disposición en paralelo del convertidor principal 320 y el subconvertidor 330, el camino para introducir una señal al subconvertidor 330 sin la señal que pasa a través del convertidor principal 320 y el camino para introducir una señal al convertidor principal 320 sin la señal que pasa a través del subconvertidor 330 llegan a estar disponibles. Esto permite un ajuste flexible a cambios en la configuración y operación del dispositivo, tal como adición, eliminación, etc. en actividades futuras.

Con el aparato de conversión de datos que usa CAMELLIA en el que se disponen en serie el convertidor principal 320 y el subconvertidor 330, por otra parte, en el caso de realizar la conversión de datos de una vuelta por un proceso de función F en dos o más ciclos, dado que los datos a ser convertidos en un ciclo son parte de los datos de entrada, se necesita el camino en el aleatorizador de datos 30 para mantener datos convertidos de la parte de los datos de entrada en el registro aritmético 350 y transferir los datos convertidos al subconvertidor 330 después de un periodo dado. O, alternativamente, se necesita el camino de transferencia en el convertidor principal 320 para transferir los datos al subconvertidor 330 a través del convertidor principal 320 después del periodo dado.

Según esta realización, no obstante, dado que el convertidor principal 320 y el subconvertidor 330 se disponen en paralelo, se hacen redundantes el camino adicional y la función de transferencia adicional del convertidor principal 320. Esto permite evitar que el tamaño del circuito del dispositivo aumente.

Adicionalmente, en el caso de usar el circuito compartido mostrado en la Fig. 59 en el que se implementan la unidad de convertidor de datos 50 y la unidad de inversor de datos 70, el camino A → B → C → D → E → B → C… llega a ser un circuito en bucle. Por lo tanto, el circuito en bucle no se debería diseñar para llegar a ser un circuito de transmisión cuando está influido por el recorrido de la señal, ruido, etc. causado por la diferencia de retardo de propagación de las señales de conmutación en una implementación LSI práctica del circuito. Otro problema es que las herramientas de síntesis lógica no pueden hacer frente a tal circuito con el circuito en bucle (un circuito de ALIMENTACIÓN EN BUCLE), de manera que no se puede lograr una síntesis lógica eficiente.

A fin de resolver este problema, la unidad de convertidor de datos 50 y la unidad de inversor de datos 70 del subconvertidor 330 se diseñan para estar separados en la Fig. 37. Esto permite al aparato de conversión de datos evitar tal problema relacionado con el recorrido, etc.

Además, como se mencionó anteriormente, el subconvertidor 330 de la Fig. 37 que usa la función de transferencia de claves/datos puede eliminar la necesidad del camino de claves desde el registro de claves KL 240 y el camino de datos desde el convertidor principal 320. Esto puede contribuir a la reducción de tamaño adicional del aparato de conversión de datos para cifrado de bloques de CAMELLIA y lograr un consumo de potencia bajo.

Realización 6.

Se dará ahora una descripción de una sexta realización.

La Fig. 38 es un diagrama de bloques de un aparato de conversión de datos para CAMELLIA de una sexta realización. La Fig. 28 es diferente de la Fig. 37 de manera que el subconvertidor 330 incluye la 1/2 unidad de subconvertidor 9, que implementa la unidad de aparato de conversión de datos 50 y la unidad de inversor de datos 70 en el circuito compartido. Por lo tanto, se hacen redundantes el selector 2-1 215 y el selector 4-1 217 de la Fig. 37.

De esta manera, el aparato de conversión de datos según esta realización no requiere ninguno de los cuatro selectores necesarios para el selector 2-1 215 y el selector 4-1 217 y el camino para introducir una clave sacada desde el selector 2-1 215 al subconvertidor 330. Esto permite simplificar la configuración del programador de claves 210 y además reducir el tamaño por ello del aparato de conversión de datos.

Realización 7.

La Fig. 47 es un diagrama de bloques de un aparato de conversión de datos para CAMELLIA según una séptima realización.

Esta realización es diferente de la del diagrama de bloques de la Fig. 37 de manera que la unidad de función F 321 en el convertidor principal 320 se configura con una función 1/8F. En otras palabras, el convertidor principal 320 de esta realización realiza una conversión de datos basada en una función F de una vuelta en ocho ciclos. Por lo tanto, en contraste con la Fig. 37, el selector 2-1 312 de la Fig. 37 se sustituye por un selector 8-1 315. Otros componentes son los mismos que los de la Fig. 37.

Realización 8.

La Fig. 48 es un diagrama de bloques de un aparato de conversión de datos para CAMELLIA según una octava realización.

Esta realización es diferente de la realización mostrada en la Fig. 47 de manera que 330 se dota con la 1/2 unidad de subconvertidor 90. Por lo tanto, se hacen redundantes el selector 2-1 215 y el selector 4-1 217 mostrados en la Fig. 47.

Realización 9.

Se muestra otra realización en la Fig. 49.

La Fig. 49 es un diagrama de bloques de un aparato de conversión de datos para CAMELLIA según una novena realización.

Esta realización es diferente de la de la Fig. 37 de manera que la unidad de función F 321 en el convertidor principal 320 se configura con una función 1/4F. Por lo tanto, el selector 2-1 312 de la Fig. 37 se sustituye por un selector 4-1 316 en la Fig. 49. El convertidor principal 320 realiza una conversión de datos en cuatro ciclos para realizar una conversión de datos basada en una función F de una vuelta mediante la unidad de función F 321, usando datos de entrada de 16 bits seleccionados por el selector 4-1 316. Otros componentes son los mismos que los de la Fig. 37.

Realización 10.

La Fig. 50 es un diagrama de bloques de un aparato de conversión de datos para CAMELLIA según una décima realización.

Esta realización es diferente de la realización de la Fig. 49 de manera que el subconvertidor 330 se dota con la 1/2 unidad de subconvertidor 90. Por lo tanto, en contraste con el caso de la Fig. 49, se hacen redundantes el selector 2-1 215 y el selector 4-1 217. Otros componentes son los mismos que los de la Fig. 49.

Realización 11.

Se dará ahora una descripción de una undécima realización.

La Fig. 39 es un diagrama de bloques de un aparato de conversión de datos para CAMELLIA según la undécima realización.

La Fig. 39 es diferente de la Fig. 37 de manera que el convertidor principal 320 se configura con la unidad de función F 321 que tiene una única función F. Por lo tanto, el convertidor principal 320 puede realizar el proceso de la función F para una vuelta en un ciclo, lo cual elimina la necesidad del selector 2-1 312 en la Fig. 37. El selector 2-1 212 de la Fig. 37 también se hace redundante y el selector 8-1 213 se sustituye por un selector 4-1 218 que selecciona una constante de entre cuatro constantes.

Realización 12.

Se dará ahora una descripción de una duodécima realización.

La Fig. 40 es un diagrama de bloques de un aparato de conversión de datos para CAMELLIA según la duodécima realización.

En la Fig. 40 se añade un selector 2-1 313. Dado que el subconvertidor 330 se configura con la 1/2 unidad de subconvertidor 90, unos de los datos superiores y los datos inferiores de los datos seleccionados por el selector 2-1 311 van a ser seleccionados. Según esta realización, el proceso mediante el convertidor principal 320 se realiza en un ciclo, de manera que el selector 2-1 312 se hace redundante como la Fig. 39. También, se hacen redundantes el selector 2-1 215 y el selector 4-1 217 de la Fig. 39.

Realización 13.

Se dará ahora una descripción de una décima tercera realización.

La Fig. 41 es un diagrama de bloques de un aparato de conversión de datos para CAMELLIA según la décima tercera realización.

La Fig. 41 es diferente de la Fig. 39 de manera que el convertidor principal 320 no repite el proceso de la unidad de función F 321 seis veces, sino que tiene seis vueltas de la unidad de función F 321 dispuestas en serie proporcionadas en la misma y realiza una conversión de datos. Por lo tanto, hay una señal de salida extra desde el convertidor principal 320 en esta realización. La razón de esto es que los datos de salida de la segunda vuelta de la función F del convertidor principal 320 van a ser introducidos a un selector 3-1 H 343 y un selector 4-1 L 344 y entonces se mantienen en el registro aritmético H 351 y el registro aritmético L 352, respectivamente. Por consiguiente, el selector 3-1 H 343 recibe tres señales y el selector 4-1 L 344 recibe cuatro señales.

Además, se proporcionan cuatro conjuntos de selectores 4-1 500 y selectores 4-1 501 y hay selectores extra para introducir cuatro claves seleccionadas por esos selectores en el convertidor principal 320. Además, el subconvertidor

330 y el convertidor principal 320 reciben claves también desde otros selectores, un selector 4-1 502 y un selector 4-1 503, en el programador de claves 210.

Realización 14.

Se dará ahora una descripción de una décima cuarta realización.

La Fig. 42 es un diagrama de bloques de un aparato de conversión de datos para CAMELLIA según la décima cuarta realización.

La Fig. 42, como la Fig. 41, es diferente de la Fig. 40 de manera que la unidad de función F del convertidor principal 32 se dota con la función F de seis vueltas dispuesta en serie. Por lo tanto, como el caso de la Fig. 41, las señales de entrada del selector 3-1 H 343 y el selector 4-1 L 344 aumentan en número en uno respectivamente, en contraste con la Fig. 40 y se requieren cuatro conjuntos de selectores 4-1 500 y selectores 4-1 501. El subconvertidor 330 y el convertidor principal 320 reciben claves también desde otros selectores en el programador de claves 210, el selector 4-1 502 y el selector 3-1 504. El selector 3-1 504 recibe tres señales de entrada.

Realización 15.

Se muestra otra realización en la Fig. 43.

La Fig. 43 es un diagrama de bloques de un aparato de conversión de datos para CAMELLIA según una décima quinta realización.

Esta realización es diferente de la de la Fig. 41 de manera que el convertidor principal 320 se dota con la unidad de función F 321 que tiene la función F de dos vueltas. Por lo tanto, en contraste con la Fig. 41, el selector 3-1 H 343 y el selector 4-1 L 344 se sustituyen por el selector 2-1 H 341 y el selector 3-1 L 342, respectivamente y se hacen redundantes los cuatro conjuntos de selectores que incluyen los selectores 4-1 500 y los selectores 4-1 501.

Realización 16.

Se muestra otra realización en la Fig. 44.

La Fig. 44 es un diagrama de bloques de un aparato de conversión de datos para CAMELLIA según una décima sexta realización.

Esta realización es diferente de la realización de la Fig. 42 de manera que la unidad de función F 321 del convertidor principal 320 es la función F de dos vueltas. Por lo tanto, el selector 3-1 H 343 y el selector 4-1 L 344 de la Fig. 42 se sustituyen por el selector 2-1 H 341 y el selector 3-1 L 342, respectivamente y se hacen redundantes los cuatro conjuntos de selectores que incluyen el selector 4-1 500 y el selector 4-1 501.

Realización 17.

La Fig. 45 es un diagrama de bloques de un aparato de conversión de datos para CAMELLIA según una décima séptima realización.

Según esta realización, la unidad de función F 321 del convertidor principal 320 incluye una función F de tres vueltas. Por lo tanto, en contraste con la Fig. 41, se hacen redundantes los cuatro conjuntos de selectores que incluyen el selector 4-1 500 y el selector 4-1 501 y se añade en su lugar un selector 4-1 505. Una señal seleccionada por el selector 4-1 505 se introduce al convertidor principal 320.

Realización 18.

La Fig. 46 es un diagrama de bloques de un aparato de conversión de datos para CAMELLIA según una décima octava realización.

Como la realización mostrada en la Fig. 45, la unidad de función F 321 del convertidor principal 320 incluye la función F de tres vueltas. Esta realización es diferente de la de la Fig. 45 de manera que el subconvertidor 330 incluye la 1/2 unidad de subconvertidor 90. Otros componentes son los mismos que los de la figura.

Realización 19.

La Fig. 51 es un diagrama de bloques de un aparato de conversión de datos para CAMELLIA según una décima novena realización.

En primer lugar, el generador de claves intermedias 40 de esta realización es diferente en configuración del de la Fig. 37. La configuración del generador de claves intermedias 40 de esta realización es equivalente a la del generador de claves intermedias 40 de la Fig. 37, etc. Por lo tanto, el generador de claves intermedias 40 de la Fig. 37, etc. se puede sustituir por el generador de claves intermedias 40 de la Fig. 51.

Se dará ahora una descripción de una configuración del generador de claves intermedias 40 de la Fig. 51.

En primer lugar, un selector 2-1 KL 291 recibe una clave secreta de entrada y una clave intermedia (Clave KL) mantenida en el registro de claves KL 240, selecciona una señal de entre estas dos señales de entrada y mantiene una clave en el registro de claves KL 240. Un selector 2-1 KA 292 recibe una clave de salida generada por el generador de claves intermedias 40 y una clave de salida (Clave KA) mantenida en el registro de claves KA 250. El selector 2-1 KA 292 selecciona una señal de entre esas dos señales de entrada y mantiene una señal seleccionada en el registro de claves KA 250.

Un selector 2-1 227 selecciona una clave de entre la clave intermedia (Clave KL) y la clave de salida (Clave KA) mantenida en y sacada desde el registro de claves KL 240 y el registro de claves KA 250, respectivamente y saca una clave a un selector 8-1 228. En el selector 8-1 228, una clave seleccionada por el selector 2-1 227 se somete a desplazamiento de rotación de ocho tipos de números, 0, 15, 30, 45, 60, 77, 94 y 111, de bits a la izquierda o derecha como se muestra en la Fig. 51. Específicamente, si el número de bits para desplazamiento de rotación es 0, no se desplazan datos. Si el número de bits para desplazamiento de rotación es 15, los datos se someten a desplazamiento de rotación en 15 bits a la izquierda o derecha. Lo mismo aplica a los otros casos. A través de los desplazamientos de rotación de datos de esa manera, se producen ocho señales. Entonces, el selector 8-1 228 selecciona una señal de entre las ocho señales y saca la señal seleccionada.

Esas operaciones permiten al generador de claves intermedias 40 de esta realización configurada de esta manera funcionar igual que el generador de claves intermedias 40 de la Fig. 37. De esta manera, los bits de la mitad superiores de datos sacados a partir del generador de claves intermedias 40 llegan a ser KLH y los bits de la mitad inferiores llegan a ser KLL y esos se introducen a un selector 2-1 510 y un selector 2-1 511, respectivamente, en el programador de claves 210. De esta manera, el selector 4-1 216 y el selector 4-1 217 de la Fig. 37 se puede sustituir por el selector 2-1 510 y el selector 2-1 511, respectivamente, de esta realización.

Por lo tanto, el generador de claves intermedias 40 mostrado en la Fig. 52, como el generador de claves intermedias 40 mostrado en la Fig. 37, requiere diez selectores 2-1. No obstante, el selector 2-1 510 y el selector 2-1 511 solamente requieren dos selectores 2-1. Por consiguiente, el número total de selectores 2-1 requerido para el generador de claves intermedias 40, el selector 2-1 510 y el selector 2-1 511 es 12.

El generador de claves intermedias 40 mostrado en la Fig. 37 requiere diez selectores 2-1 y el selector 4-1 216 y el selector 4-1 217 requieren seis selectores 2-1. Por consiguiente, el número total de selectores 2-1 requerido para el generador de claves intermedias 40, el selector 4-1 216 y el selector 4-1 217 es 16.

De esta manera, el aparato de conversión de datos de esta realización puede reducir el número de selectores 2-1 por cuatro en comparación con el aparato de conversión de datos mostrado en la Fig. 37.

Consecuentemente, esta realización permite lograr reducir el tamaño en base a la reducción en el número de selectores y también lograr un consumo de potencia bajo que acompaña la reducción en el número de puertas resultante de la reducción de selectores.

Señalar que la configuración del generador de claves intermedias 40 tratado en esta realización también es aplicable a las de todas las otras realizaciones de la presente invención.

Realización 20.

La Fig. 52 es un diagrama de bloques de un aparato de conversión de datos para CAMELLIA según una vigésima realización.

Esta realización es diferente de la de la Fig. 51 de manera que el subconvertidor 330 incluye la 1/2 unidad de subconvertidor 90. De esta manera, se hacen redundantes el selector 2-1 215 y el selector 2-1 511 de la Fig. 51 según esta realización. Otros componentes son los mismos que los de la Fig. 51.

Señalar que el número de bits de desplazamiento de rotación referido en la Fig. 51 y la Fig. 52 es sinónimo con el número de bits para desplazamiento de rotación.

Realización 21.

La Fig. 34 y la Fig. 35 tratadas en la cuarta realización muestran el proceso de cifrado/descifrado de CAMELLIA para una clave de 128 bits.

No obstante, las configuraciones de los aparatos de conversión de datos tratadas en todas las realizaciones de la presente invención son aplicables a cualquier aparato de conversión de datos que realice el proceso de cifrado/descifrado de CAMELLIA no solamente para una clave de 128 bits sino también una clave de 192 y 256 bits.

La Fig. 53 es un diagrama que ilustra un proceso de generación de una clave de 192 bits.

Como se trató anteriormente, con una clave de 128 bits, se genera una clave de 256 bits como la clave extendida. Ahora, con una clave secreta de 192 o 256 bits a ser introducida, la longitud de bits de la clave extendida es 512.

Con la Fig. 53, una clave KL y una clave KR son claves intermedias y una clave KA y una clave KB son claves de salida. Entonces, todas las claves KL, KR, KA y KB son de 128 bits y por lo tanto poner las claves juntas genera una clave extendida de 512 bits.

Con una clave secreta de 256 bits a ser introducida, se asignan a la clave KL 128 bits, que son bits de la mitad superiores de la clave secreta de entrada y se asignan a la clave KR los 128 bits inferiores.

La clave KL y la clave KR se someten a una operación XOR, respectivamente y entonces se introducen a una parte del convertidor principal 320 como se muestra en la Fig. 53.

La Fig. 53 corresponde a la Fig. 2 en el lado derecho, que muestra el método de generación de una clave extendida en el caso donde la clave secreta tiene una longitud de 128 bits.

El método de generación de la clave de salida KA a partir de una clave de entrada mostrada en la Fig. 53 en la izquierda es el mismo que el método de generación de la clave de salida KA ilustrada en la Fig. 2, excepto que la clave de entrada se basa en un resultado sometido a una operación XOR con la clave KL o la clave KR. La Fig. 2 no muestra el proceso de generación de la clave de salida KB a partir de la clave KR mostrada en la Fig. 53 en la derecha. Por lo tanto, se describirá ahora el proceso de generación de la clave de salida (clave KB).

Con una clave de 256 bits introducida, los 128 bits inferiores llegan a ser la clave de entrada (clave KR) y se introducen al convertidor principal 320. Los bits superiores de los 128 bits inferiores se convierten no linealmente mediante una constante $\Sigma 5$ usando la unidad de función F 321a en la primera etapa en el convertidor principal 320 y se sacan. Los datos de salida se someten a una operación XOR con los bits inferiores de la clave de entrada (clave KR) en el circuito EXOR 322a y entonces se introducen a la unidad de función F 321b. En la unidad de función F 321b, los datos se someten a otra conversión no lineal mediante una constante $\Sigma 6$ y los datos convertidos entonces se someten a una operación XOR con los bits superiores de la clave de entrada (KR) en el circuito EXOR 322b. Los datos convertidos a través de una operación por el circuito EXOR 322b se sacan como datos superiores de 64 bits de la clave de salida (Clave KB) y los datos resultantes de una operación por el circuito EXOR 322a se sacan como datos inferiores de 64 bits de la clave de salida (Clave KB).

Las claves de salida generadas de esta manera (Clave KA y Clave KB) y las claves de entrada (Clave KL y Clave KR) se transfieren como una clave extendida de 512 bits desde el generador de claves intermedias 40 al programador de claves 210, entonces se programan por el programador de claves 210 y se usan para cifrado/descifrado de datos.

Con una clave secreta de 192 bits, los 128 bits superiores de la clave secreta de entrada llegan a ser la Clave KL. Entonces, los 64 bits inferiores de la clave secreta de entrada llegan a ser los 64 bits superiores de la clave KR. Los 64 bits inferiores de la clave KR son los inversos de los 64 bits superiores de la clave KR que son los 64 bits inferiores de la clave secreta de entrada. Otros métodos de generación de claves son los mismos que el método de generación de la clave secreta de 256 bits y por lo tanto no se tratarán aquí.

La Fig. 54 es un diagrama que ilustra el proceso de cifrado de CAMELLIA para una clave de 192 o 256 bits.

En contraste con la Fig. 34 que ilustra el proceso de cifrado de CAMELLIA para una clave de 128 bits, el número de convertidores principales 320 se aumenta de tres a cuatro y el número de subconvertidores 330 se aumenta de dos a tres. Por lo tanto, el proceso de cifrado para una clave de 192 o 256 bits que usa una función F de 24 vueltas se lleva a cabo para cifrado total. Otros componentes son los mismos que los del caso para una clave de 128 bits mostrada en la Fig. 34 y por lo tanto no se tratarán aquí.

La Fig. 55 es un diagrama que ilustra el proceso de descifrado de CAMELLIA para una clave de 192 o 256 bits.

El proceso de descifrado de CAMELLIA para una clave de 128 bits se trató anteriormente con referencia a la Fig. 35. En contraste con la Fig. 35, el número de convertidores principales 320 se aumenta a cuatro, el número de los subconvertidores 330 se aumenta a tres y se proporciona una función F de 24 vueltas como el caso del proceso de cifrado. Otros componentes son los mismos que los del proceso de descifrado de CAMELLIA para una clave de 128 bits y por lo tanto no se tratarán aquí.

Señalar que los detalles del algoritmo CAMELLIA de cifrado de bloques de claves de 128, 192 o 156 bits se exponen en “128-bit Block Cipher Camellia Algorithm Specification”.

Todas las realizaciones mostradas anteriormente son aplicables a cualquier aparato de conversión de datos para una clave de 128, 192 o 256 bits.

La función de transferencia de claves y datos proporcionada en el subconvertidor 330 se puede aplicar a todas las realizaciones de la presente invención.

Con todas las realizaciones precedentes, las operaciones de los componentes respectivos se asocian unas con otras y por lo tanto las operaciones de los componentes respectivos se pueden sustituir por una secuencia de operaciones basadas en la relación de las operaciones tratadas anteriormente. Con la sustitución, las realizaciones pueden llegar a ser las de un método de la invención.

Además, si los procesos de los componentes respectivos sustituyen las operaciones de los mismos, entonces las realizaciones precedentes pueden llegar a ser realizaciones para programas.

Aún más, si los programas se almacenan en medios de almacenamiento legibles por ordenador que almacenan programas, entonces las realizaciones pueden llegar a ser realizaciones para medios de almacenamiento legibles por ordenador que almacenan programas.

Todas las realizaciones para programas o las realizaciones para almacenamiento legible por ordenador que almacenan programas se pueden implementar por programas operables por ordenador.

Los procesos de las realizaciones respectivas para programas y aquéllos para las realizaciones respectivas para medios de almacenamiento legibles por ordenador son ejecutables por programas, que se almacenan en una memoria. Los programas se leen por una unidad central de proceso (CPU) desde la memoria y se ejecutan para implementar diagramas de flujo por la unidad central de proceso. Señalar que la memoria y la unidad central de proceso no se muestran en las figuras.

También señalar que el software o programa de cada realización se puede implementar por un microprograma almacenado en una ROM (MEMORIA SÓLO DE LECTURA). Alternativamente, cada función de los programas precedentes se puede implementar por una combinación de software, microprograma y hardware.

Aplicabilidad industrial

La restricción del aumento de selectores y la reducción en el número de selectores permiten reducir el tamaño del dispositivo.

También, la reducción en un número global de puertas en circuitos permite lograr un consumo de potencia bajo.

Aún más, se puede mejorar la frecuencia de operación.

El subconvertidor puede transferir datos de entrada o una clave de entrada.

Se permite un ajuste flexible a un cambio en la configuración del aparato.

Se permite que una de la unidad de conversión de datos 50 y la unidad de inversión de datos 70 realice conversión de datos y la otra de la unidad de conversión de datos 50 y la unidad de inversión de datos 70 transfiera datos de entrada o una clave de entrada.

El camino desde el convertidor principal al selector se hace redundante, permitiendo por ello al dispositivo llegar a ser compacto y la reducción en el número de selectores permite lograr un consumo de potencia bajo.

REIVINDICACIONES

1. Un aparato de conversión de datos para recibir una clave y datos y para realizar conversión de datos para uno de cifrado y descifrado de los datos recibidos usando la clave recibida, el aparato de conversión de datos que comprende:

un aleatorizador de datos (30) adaptado para realizar conversión de datos; y

un controlador (5) adaptado para controlar una señal de transferencia que indica uno de la clave y los datos a ser transferidos,

en donde el controlador (5) está adaptado para sacar la señal de transferencia en un caso de transferencia de uno de la clave y los datos y

en donde el aleatorizador de datos (30) incluye,

un subconvertidor (330) adaptado para realizar la conversión de datos para uno de cifrado de datos y descifrado de datos convirtiendo los datos recibidos usando la clave recibida y para transferir al menos uno de la clave recibida y los datos recibidos sin conversión de datos tras la recepción de la señal de transferencia sacada por el controlador (5),

en donde el subconvertidor (330) incluye al menos uno de,

una unidad de convertidor de datos (50) adaptada para realizar conversión de datos lineal y

una unidad de inversor de datos (70) adaptada para realizar una conversión de datos que es inversa a la de la unidad de convertidor de datos (50),

caracterizado por que

al menos una de la unidad de convertidor de datos (50) y la unidad de inversor de datos (70) se adapta para realizar la conversión de datos y para recibir la señal de transferencia sacada desde el controlador (5) y para transferir al menos uno de los datos y la clave sin conversión de datos según la señal de transferencia recibida, cuando el controlador saca la señal de transferencia,

en donde

a) el controlador (5) se adapta para sacar una señal de transferencia de claves y una señal de máscara como las señales de transferencia para transferir la clave recibida y al menos una de la unidad de convertidor de datos (50) y la unidad de inversor de datos (70) se adapta para transferir la clave, tras la recepción de la señal de transferencia de claves y la señal de máscara sacada desde el controlador (5), anulando los datos recibidos según la señal de transferencia de claves recibida y permitiendo a la clave recibida pasar a través según la señal de máscara recibida o

b) el controlador (5) se adapta para sacar una señal de TRANSFERENCIA DE DATOS que es una señal de transferencia de datos como la señal de transferencia para transferir los datos recibidos y al menos una de la unidad de convertidor de datos (50) y la unidad de inversor de datos (70) se adapta para transferir los datos, tras la recepción de la señal de TRANSFERENCIA DE DATOS sacada desde el controlador (5), anulando la clave recibida y permitiendo a los datos recibidos pasar a través según la señal de TRANSFERENCIA DE DATOS recibida.

2. El aparato de conversión de datos según la reivindicación 1, en donde el aleatorizador de datos (30) además incluye,

un convertidor principal (320) adaptado para recibir los datos y para convertir no linealmente los datos recibidos,

en donde el controlador (5) se adapta para sacar la señal de transferencia de datos como la señal de transferencia cuando se transfieren los datos y

en donde el subconvertidor (330) se adapta para recibir la señal de transferencia de datos sacada desde el controlador (5) y los datos convertidos no linealmente por el convertidor principal (320) y para transferir los datos recibidos según la señal de transferencia de datos recibida.

3. El aparato de conversión de datos según la reivindicación 1, que además comprende:

un generador de claves (20) adaptado para generar la clave,

en donde el controlador (5) se adapta para sacar la señal de transferencia de claves como la señal de transferencia en un caso de transferencia de la clave y

en donde el subconvertidor (330) se adapta para recibir la señal de transferencia de claves sacada desde el controlador (5) y la clave generada por el generador de claves (20) y para transferir la clave recibida según la señal de transferencia de claves recibida.

4. El aparato de conversión de datos según la reivindicación 3, en donde el generador de claves (20) además incluye,

un generador de claves intermedias (40), adaptado para recibir una clave secreta y generar una clave intermedia en base a la clave secreta recibida,

en donde el subconvertidor (330) se adapta, tras la recepción de la señal de transferencia de claves sacada desde el controlador (5), para transferir la clave intermedia generada por el generador de claves intermedias (40) al convertidor principal (320) según la señal de transferencia de claves recibida,

en donde el convertidor principal (320) se adapta para repetir la conversión y salida de la clave intermedia transferida por el subconvertidor (330) al menos una vez,

en donde el subconvertidor se adapta para repetir la conversión y salida de la clave intermedia sacada desde el convertidor principal (320) al menos una vez,

en donde al menos uno del convertidor principal (320) y el subconvertidor (330) se adapta para repetir la conversión y salida de la clave intermedia al menos una vez,

en donde el convertidor principal (320) saca la clave intermedia sacada desde al menos uno del convertidor principal (320) y el subconvertidor (330) como una clave de salida y

en donde el generador de claves intermedias (40) se adapta para recibir la clave de salida sacada desde el convertidor principal (320), generando por ello una clave extendida que incluye la clave intermedia y la clave de salida.

5. El aparato de conversión de datos según la reivindicación 4, en donde el generador de claves intermedias (40) incluye,

un selector 6-1 KL (220) adaptado para seleccionar una clave de entre seis claves recibidas y

un registro de claves KL (240) adaptado para mantener la clave seleccionada por el selector 6-1 KL (220) como la clave intermedia,

en donde el selector 6-1 KL (220) se adapta para recibir una clave secreta, para recibir seis claves que incluyen la clave secreta, la clave intermedia mantenida en el registro de claves KL (240) y cuatro claves obtenidas a través de desplazamientos de rotación de la clave intermedia mantenida en el registro de claves KL (240) por cuatro números diferentes y seleccionar una clave de entre las seis claves recibidas,

en donde el registro de claves KL (240) se adapta para mantener una clave seleccionada por el selector 6-1 KL (220) y

en donde el subconvertidor (330) se adapta, tras la recepción de la señal de transferencia de claves sacada desde el controlador (5), para recibir la clave mantenida en el registro de claves KL (240) como la clave intermedia y para transferir la clave intermedia recibida.

6. El aparato de conversión de datos según la reivindicación 4, en donde el generador de claves intermedias (40) incluye,

un selector 4-1 (223) adaptado para seleccionar una clave de entre cuatro claves recibidas,

un selector 3-1 KL (222) adaptado para seleccionar una clave de entre tres claves recibidas y

un registro de claves KL (240) adaptado para mantener una clave seleccionada por el selector 3-1 KL (222) como la clave intermedia,

en donde el selector 4-1 (223) se adapta para recibir cuatro claves obtenidas a través de los desplazamientos de rotación de la clave intermedia mantenida en el registro de claves KL (240) por cuatro números diferentes y para seleccionar una clave de entre las cuatro claves recibidas,

en donde el selector 3-1 KL (222) se adapta para recibir una clave secreta, para recibir tres claves que incluyen la clave secreta, la clave seleccionada por el selector 4-1 (223) y la clave intermedia mantenida en el registro de claves KL (240) y para seleccionar una clave de entre las tres claves recibidas,

en donde el registro de claves KL (240) se adapta para mantener una clave seleccionada por el selector 3-1 KL (222) y

en donde el subconvertidor (330) se adapta, tras la recepción de la señal de transferencia de claves sacada desde el controlador (5), para recibir la clave mantenida en el registro de claves KL (240) como la clave intermedia y para transferir la clave intermedia recibida.

7. El aparato de conversión de datos según la reivindicación 4, en donde el generador de claves (20) además incluye,

un programador de claves (210) adaptado para recibir la clave extendida generada por el generador de claves intermedias (40) y una constante predeterminada y para programar una clave para sacar una de la clave extendida recibida y la constante predeterminada recibida para al menos uno del convertidor principal (320) y el subconvertidor (330) según una condición predeterminada.

8. El aparato de conversión de datos según la reivindicación 1, en donde el subconvertidor (330) incluye,

una 1/2 unidad de subconvertidor (90) adaptada para implementar conversión de datos para conversión de datos lineal e inversión de datos para conversión de datos que es inversa a la conversión de datos lineal en un circuito compartido y

en donde el subconvertidor (330) se adapta para convertir los datos mediante el uso de la 1/2 unidad de subconvertidor (90), recibe la señal de transferencia sacada por el controlador (5) en un caso donde el controlador (5) sacó la señal de transferencia y para transferir al menos uno de la clave y los datos según la señal de transferencia recibida.

9. El aparato de conversión de datos según la reivindicación 1, en donde la unidad de convertidor de datos (50) y la unidad de inversor de datos (70) se disponen en serie y

en donde una de la unidad de convertidor de datos (50) y la unidad de inversor de datos (70) se adapta para recibir uno de los datos convertidos por otra de la unidad de convertidor de datos (50) y la unidad de inversor de datos (70), la clave transferida y los datos transferidos y para realizar una de la conversión de datos, transferencia de claves y transferencia de datos mediante el uso de uno de los datos convertidos, la clave transferida y los datos transferidos que se reciben.

10. El aparato de conversión de datos según la reivindicación 1, en donde el aparato de conversión de datos se adapta para recibir uno de una clave de 128 bits, una clave de 192 bits y una clave de 256 bits y para convertir los datos recibidos usando las claves recibidas.

11. Un método de conversión de datos a ser realizado en un aparato según una de las reivindicaciones 1 a 10, para

recibir una clave y datos y realizar conversión de datos para al menos uno de cifrado de datos y descifrado de datos de los datos recibidos usando la clave recibida, en donde el método de conversión de datos que comprende:

sacar una señal de transferencia que indica una de la clave recibida y los datos recibidos a ser transferidos en un caso de transferencia de la de la clave recibida y los datos recibidos,

realizar la conversión de datos para uno de cifrado de datos y descifrado de datos convirtiendo los datos recibidos usando la clave recibida, la conversión de datos que es una conversión de datos lineal y una conversión inversa a la conversión de datos lineal y

transferir al menos uno de la clave recibida y los datos recibidos sin conversión de datos tras la recepción de la señal de transferencia sacada,

caracterizado por que

a) una señal de transferencia de claves y una señal de máscara se sacan como la señal de transferencia para transferir la clave recibida y

la clave se transfiere tras la recepción de la señal de transferencia de claves y la señal de máscara anulando los datos recibidos según la señal de transferencia de claves recibida y permitiendo a la clave recibida pasar a través según la señal de máscara recibida o

b) una señal de TRANSFERENCIA DE DATOS que es una señal de transferencia de datos se saca como la señal de transferencia para transferir los datos recibidos y

los datos se transfieren tras la recepción de la señal de TRANSFERENCIA DE DATOS anulando la clave recibida y permitiendo a los datos recibidos pasar a través según la señal de TRANSFERENCIA DE DATOS recibida.

12. El aparato de conversión de datos según la reivindicación 1, que además comprende:

un generador de claves (20) adaptado para generar una clave,

en donde el generador de claves (20) además incluye un generador de claves intermedias (40) adaptado para recibir una clave secreta, para generar una clave intermedia basada en la clave secreta recibida y para generar una clave de salida basada en la clave intermedia generada usando el convertidor principal (320) y el subconvertidor (330).

13. El aparato de conversión de datos según la reivindicación 12, en donde el generador de claves intermedias (40) incluye,

un selector 6-1 KL (220) adaptado para recibir seis claves y seleccionar una clave de entre las seis claves recibidas,

un registro de claves KL (240) adaptado para mantener la clave seleccionada por el selector 6-1 KL (220) como la clave intermedia,

un selector 6-1 KA (230) adaptado para seleccionar una clave de entre seis claves y

un registro de claves KA (250) adaptado para mantener la clave seleccionada por el selector 6-1 KA (230) como la clave de salida,

en donde el selector 6-1 KL (220) se adapta para recibir una clave secreta, para recibir seis claves que incluyen la clave secreta, la clave intermedia mantenida en el registro de claves KL (240) y cuatro claves obtenidas a través de desplazamientos de rotación de la clave intermedia mantenida en el registro de claves KL (240) por cuatro números diferentes y seleccionar una clave de entre las seis claves recibidas,

en donde el registro de claves KL (240) se adapta para mantener una clave seleccionada por el selector 6-1 KL, como una clave intermedia,

en donde el selector 6-1 KA (230) se adapta para recibir una clave de salida generada usando el convertidor principal (320) y el subconvertidor (330), para recibir seis claves que incluyen la clave de salida recibida, la clave de salida mantenida en el registro de claves KA (250) y cuatro claves obtenidas a través de desplazamientos de rotación de la clave de salida mantenida en el registro de claves KA (250) por cuatro números diferentes y para seleccionar una clave de entre las seis claves recibidas y

en donde el registro de claves KA (250) se adapta para mantener la clave seleccionada por el selector 6-1 KA (230) como una clave de salida.

14. El aparato de conversión de datos según la reivindicación 12, en donde el generador de claves intermedias (40) incluye,

un selector 2-1 (224) que se adapta para seleccionar una clave de entre dos claves,

un selector 4-1 (223) que se adapta para seleccionar una clave de entre cuatro claves,

un selector 3-1 KL (222) que se adapta para seleccionar una clave de entre tres claves,

un registro de claves KL (240) que se adapta para mantener la clave seleccionada por el selector 3-1 KL (222) como una clave intermedia,

un selector 3-1 KA (232) que se adapta para seleccionar una clave de entre tres claves y

un registro de claves KA (250) que se adapta para mantener la clave seleccionada por el selector 3-1 KA (232) como una clave de salida,

en donde el selector 2-1 (224) se adapta para seleccionar una clave de entre la clave intermedia mantenida en el registro de claves KL (240) y la clave de salida mantenida en el registro de claves KA (250),

en donde el selector 4-1 (223) se adapta para recibir cuatro claves obtenidas a través de desplazamientos de rotación de la clave seleccionada por el selector 2-1 (224) por cuatro números diferentes y seleccionar una clave de entre las cuatro claves recibidas,

en donde el selector 3-1 KL (222) se adapta para recibir una clave secreta, para recibir tres claves que incluyen la clave secreta, la clave seleccionada por el selector 4-1 (223) y la clave intermedia mantenida en el registro de claves KL (240) y para seleccionar una clave de entre las tres claves,

en donde el registro de claves KL (240) se adapta para mantener la clave seleccionada por el selector 3-1 KL (222) como una clave intermedia,

en donde el selector 3-1 KA (232) se adapta para recibir una clave de salida generada usando el convertidor principal (320) y el subconvertidor (330), para recibir tres claves que incluyen la clave de salida recibida, la clave seleccionada por el selector 4-1 (223) y la clave de salida mantenida en el registro de claves KA (250) y para seleccionar una clave de entre las tres claves y

en donde el registro de claves KA 8250) se adapta para mantener una clave seleccionada por el selector 3-1 KA (232) como una clave de salida.

15. El aparato de conversión de datos según la reivindicación 12, en donde el generador de claves intermedias (40) incluye,

un selector 2-1 KL (291) que se adapta para seleccionar una clave de entre dos claves,

un registro de claves KL (240) que se adapta para mantener la clave seleccionada por el selector 2-1 KL (291),

un selector 2-1 KA (250) que se adapta para seleccionar una clave de entre dos claves,

un registro de claves KA (250) que se adapta para mantener la clave seleccionada por el selector 2-1 KA (292),

un selector 2-1 (227) que se adapta para seleccionar una clave de entre dos claves y

un selector 8-1 (228) que se adapta para seleccionar una clave de entre ocho claves,

en donde el selector 2-1 KL (291) se adapta para recibir una clave secreta y seleccionar una clave de entre la clave secreta recibida y la clave mantenida en el registro de claves KL (240),

en donde el selector 2-1 KA (292) se adapta para recibir una clave de salida generada usando el convertidor principal (320) y el subconvertidor (330) y para seleccionar una clave de entre la clave de salida recibida y la clave mantenida en el registro de claves KA (250),

en donde el selector 2-1 (227) se adapta para seleccionar una clave de entre dos claves seleccionadas por el selector 2-1 KL (291) y el selector 2-1 KA (292) y

en donde el selector 8-1 (228) se adapta para recibir ocho claves obtenidas a través de desplazamientos de rotación de la clave seleccionada por el selector 2-1 (227) por ocho números diferentes y para seleccionar una clave de entre las ocho claves recibidas.

Fig. 1

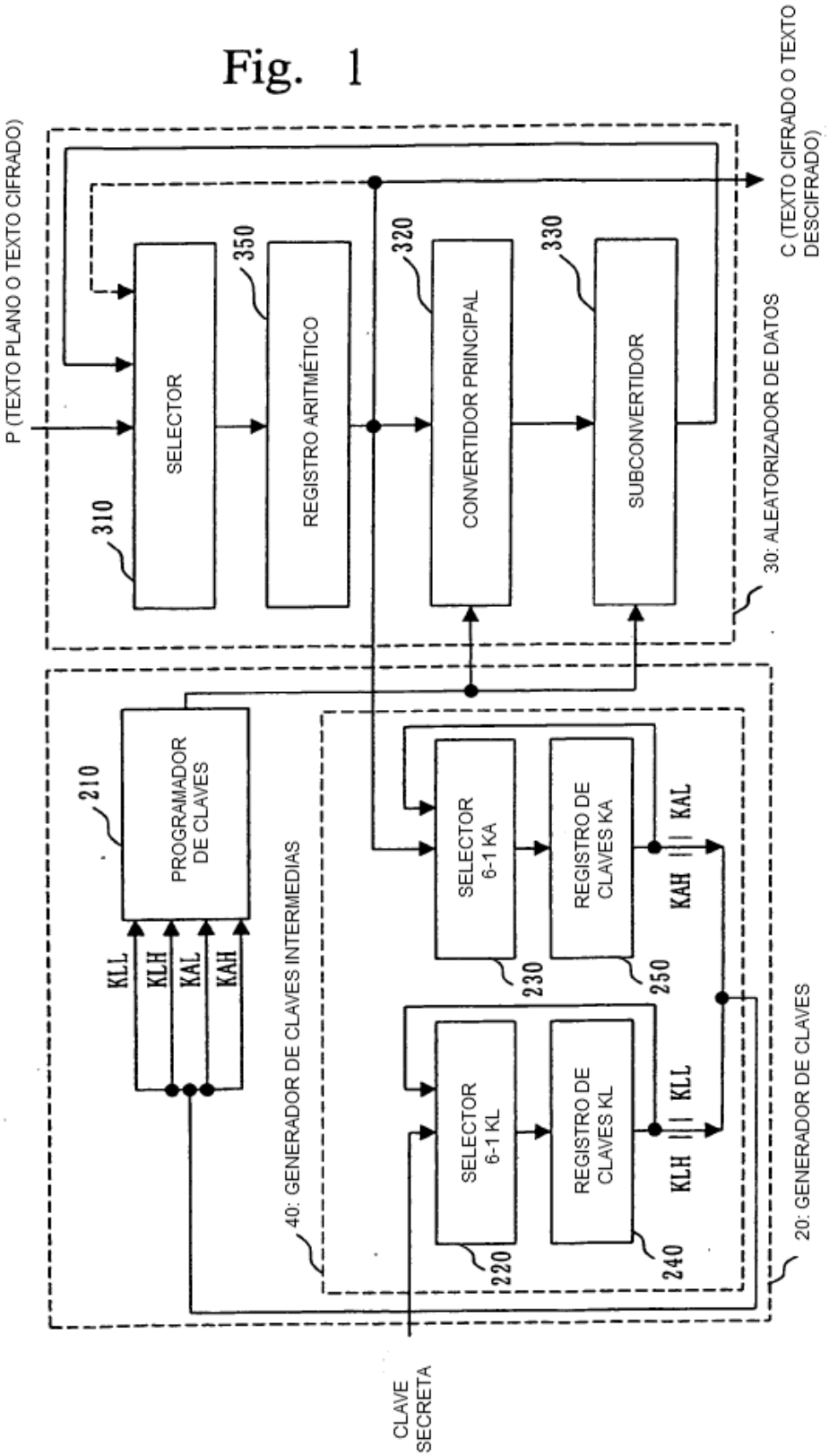

P (TEXTO PLANO O TEXTO CIFRADO)
C (TEXTO CIFRADO O TEXTO DESCIFRADO)
30: ALEATORIZADOR DE DATOS
SELECTOR
310
REGISTRO ARITMÉTICO
350
CONVERTIDOR PRINCIPAL
320
SUBCONVERTIDOR
330
20: GENERADOR DE CLAVES
40: GENERADOR DE CLAVES INTERMEDIAS
PROGRAMADOR DE CLAVES
210
KLL
KLH
KAL
KAH
SELECTOR 6-1 KA
230
REGISTRO DE CLAVES KA
250
SELECTOR 6-1 KL
220
REGISTRO DE CLAVES KL
240
CLAVE SECRETA

Fig. 2

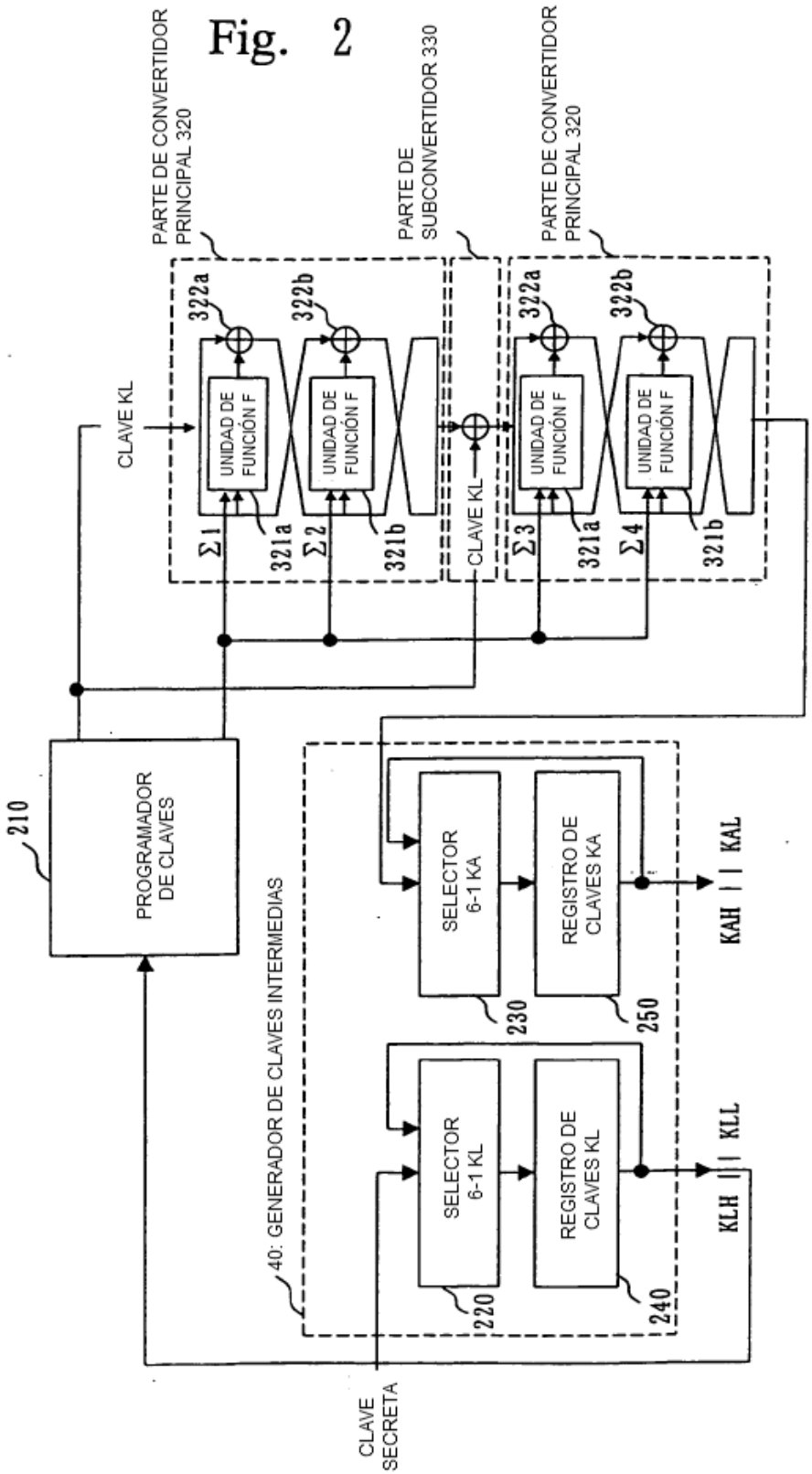

PARTE DE CONVERTIDOR PRINCIPAL 320
PARTE DE SUBCONVERTIDOR 330
PARTE DE CONVERTIDOR PRINCIPAL 320
CLAVE KL
322a
322b
UNIDAD DE FUNCIÓN F
Σ1
Σ2
Σ3
Σ4
321a
321b
CLAVE KL
210
PROGRAMADOR DE CLAVES
40: GENERADOR DE CLAVES INTERMEDIAS
SELECTOR 6-1 KA
REGISTRO DE CLAVES KA
230
250
KAH || KAL
SELECTOR 6-1 KL
REGISTRO DE CLAVES KL
220
240
KLH || KLL
CLAVE SECRETA

Fig. 3

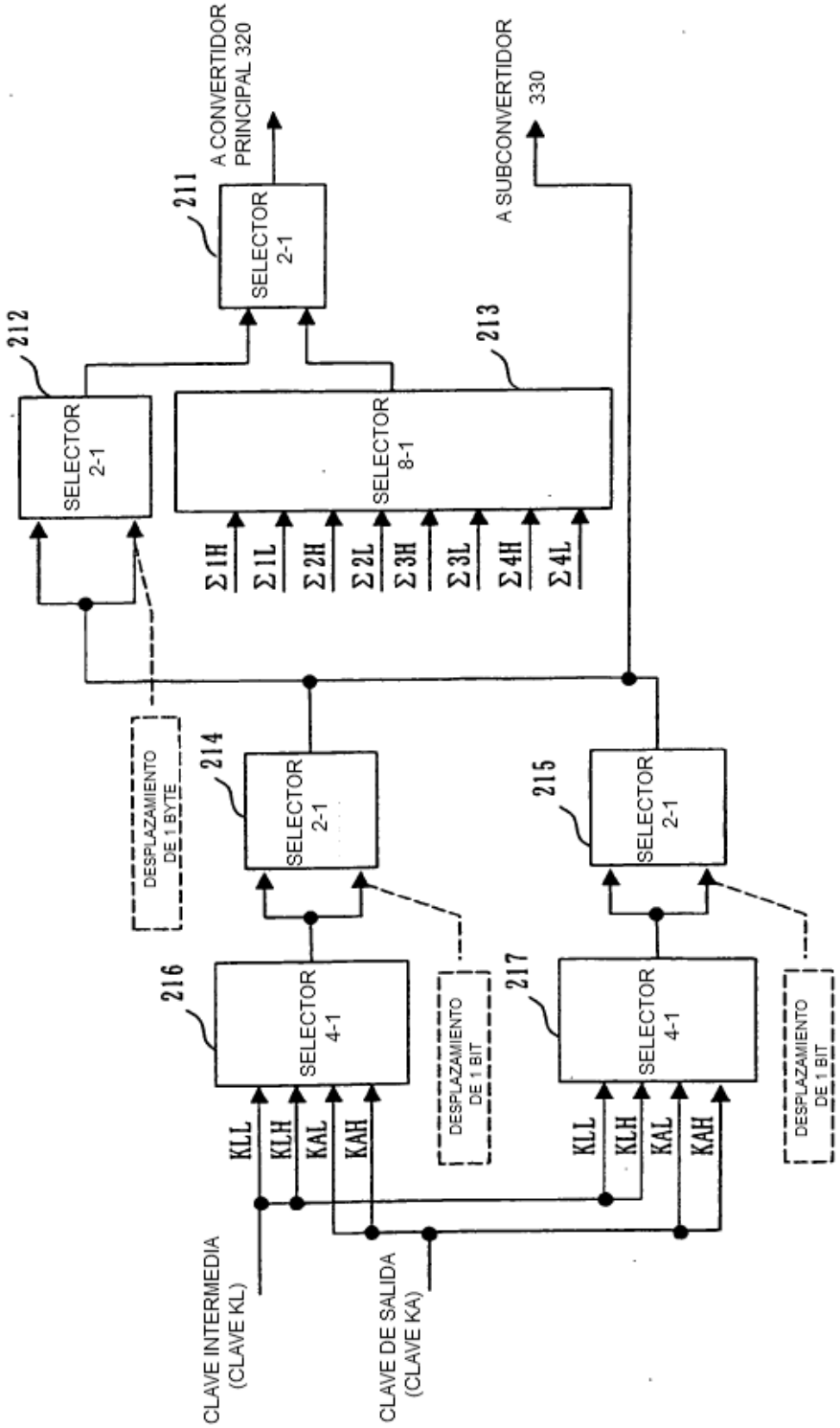

A CONVERTIDOR PRINCIPAL 320
A SUBCONVERTIDOR 330
211
SELECTOR 2-1
212
SELECTOR 2-1
213
SELECTOR 8-1
Σ1H
Σ1L
Σ2H
Σ2L
Σ3H
Σ3L
Σ4H
Σ4L
DESPLAZAMIENTO DE 1 BYTE
214
SELECTOR 2-1
215
SELECTOR 2-1
216
SELECTOR 4-1
217
SELECTOR 4-1
DESPLAZAMIENTO DE 1 BIT
DESPLAZAMIENTO DE 1 BIT
KLL
KLH
KAL
KAH
KLL
KLH
KAL
KAH
CLAVE INTERMEDIA (CLAVE KL)
CLAVE DE SALIDA (CLAVE KA)

Fig. 4

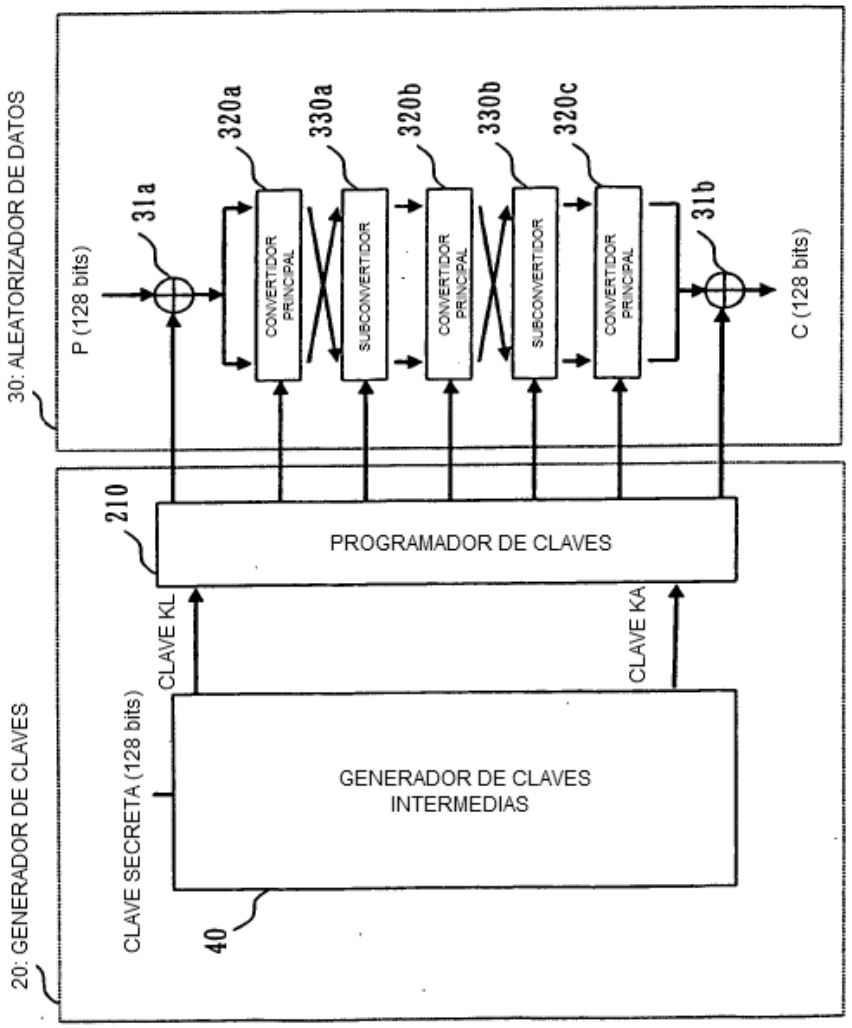

30: ALEATORIZADOR DE DATOS
P (128 bits)
31a
320a
330a
320b
330b
320c
CONVERTIDOR PRINCIPAL
SUBCONVERTIDOR
CONVERTIDOR PRINCIPAL
SUBCONVERTIDOR
CONVERTIDOR PRINCIPAL
31b
C (128 bits)
210
PROGRAMADOR DE CLAVES
CLAVE KL
CLAVE KA
20: GENERADOR DE CLAVES
CLAVE SECRETA (128 bits)
GENERADOR DE CLAVES INTERMEDIAS
40

Fig. 5

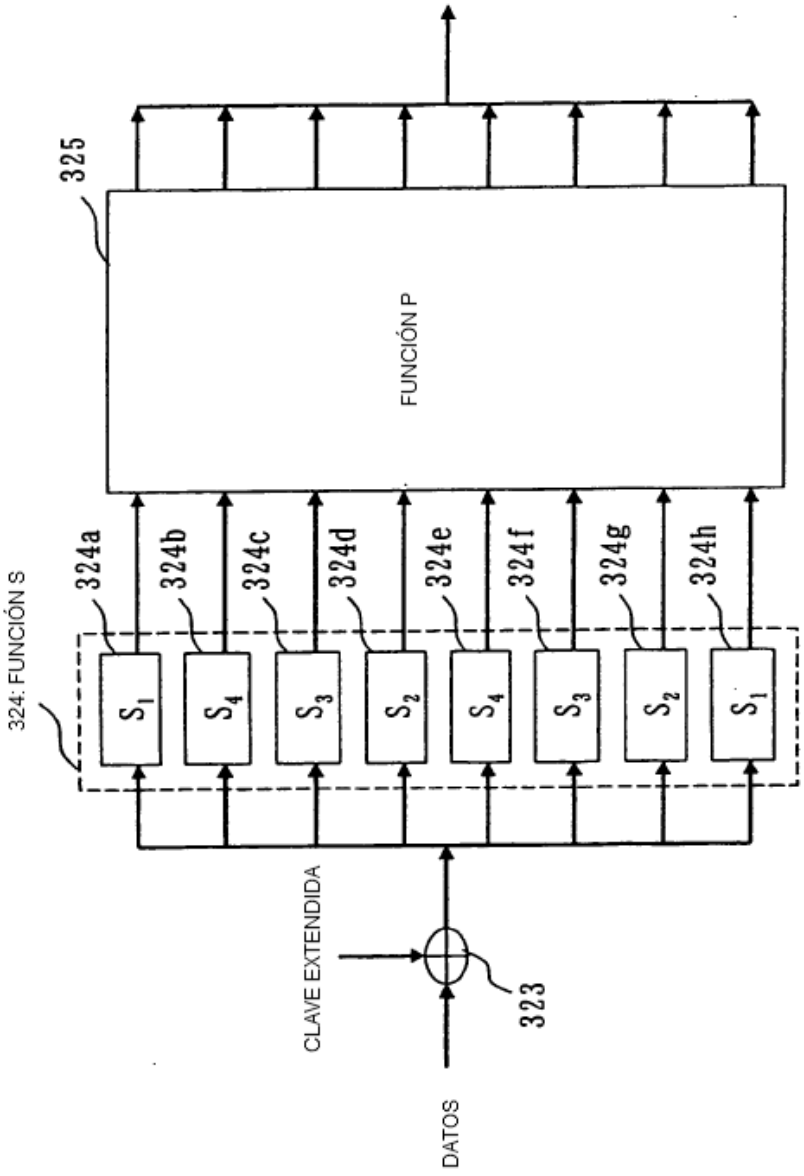

325
FUNCIÓN P
324a
324b
324c
324d
324e
324f
324g
324h
324: FUNCIÓN S
S1
S4
S3
S2
S4
S3
S2
S1
CLAVE EXTENDIDA
323
DATOS

Fig. 6

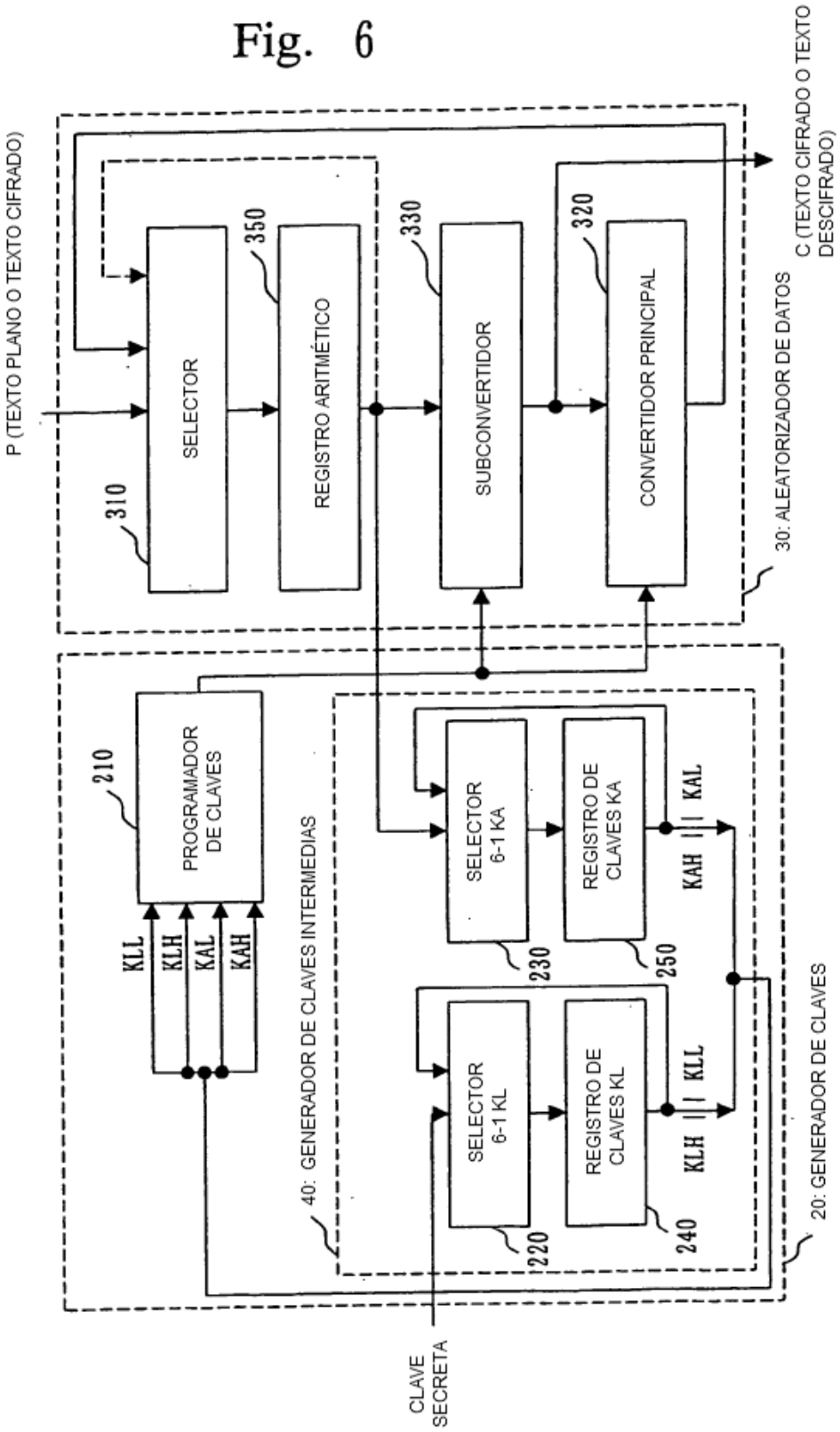

P (TEXTO PLANO O TEXTO CIFRADO)
C (TEXTO CIFRADO O TEXTO DESCIFRADO)
30: ALEATORIZADOR DE DATOS
SELECTOR
REGISTRO ARITMÉTICO
SUBCONVERTIDOR
CONVERTIDOR PRINCIPAL
310
350
330
320
20: GENERADOR DE CLAVES
40: GENERADOR DE CLAVES INTERMEDIAS
PROGRAMADOR DE CLAVES
210
KLL
KLH
KAL
KAH
SELECTOR 6-1 KA
REGISTRO DE CLAVES KA
SELECTOR 6-1 KL
REGISTRO DE CLAVES KL
230
250
220
240
CLAVE SECRETA

Fig. 7

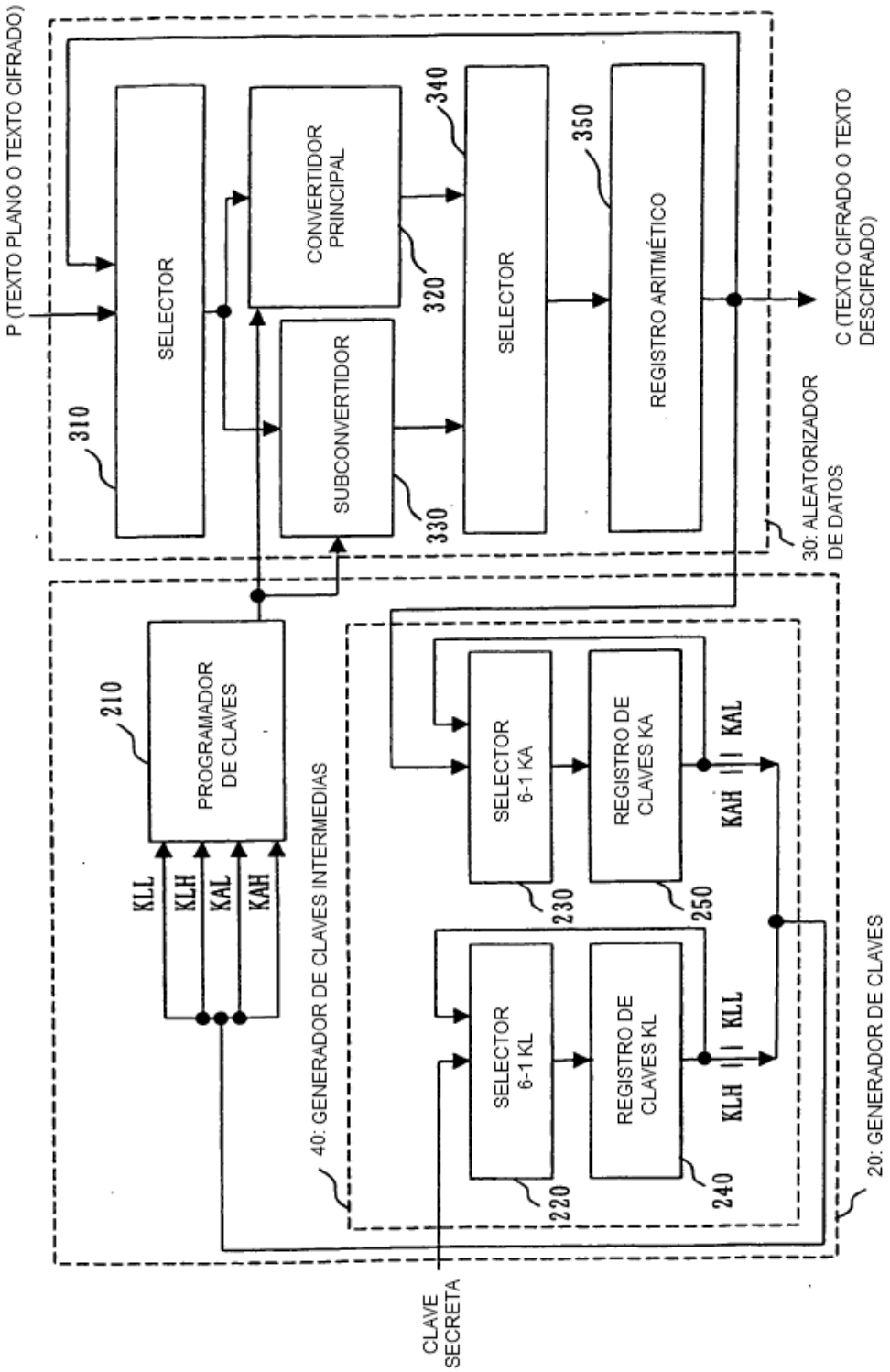

P (TEXTO PLANO O TEXTO CIFRADO)
SELECTOR
310
CONVERTIDOR PRINCIPAL
320
SUBCONVERTIDOR
330
340
SELECTOR
350
REGISTRO ARITMÉTICO
C (TEXTO CIFRADO O TEXTO DESCIFRADO)
30: ALEATORIZADOR DE DATOS
PROGRAMADOR DE CLAVES
210
KLL
KLH
KAL
KAH
40: GENERADOR DE CLAVES INTERMEDIAS
SELECTOR 6-1 KA
230
REGISTRO DE CLAVES KA
250
KAL
KAH
SELECTOR 6-1 KL
220
REGISTRO DE CLAVES KL
240
KLL
KLH
20: GENERADOR DE CLAVES
CLAVE SECRETA

Fig. 8

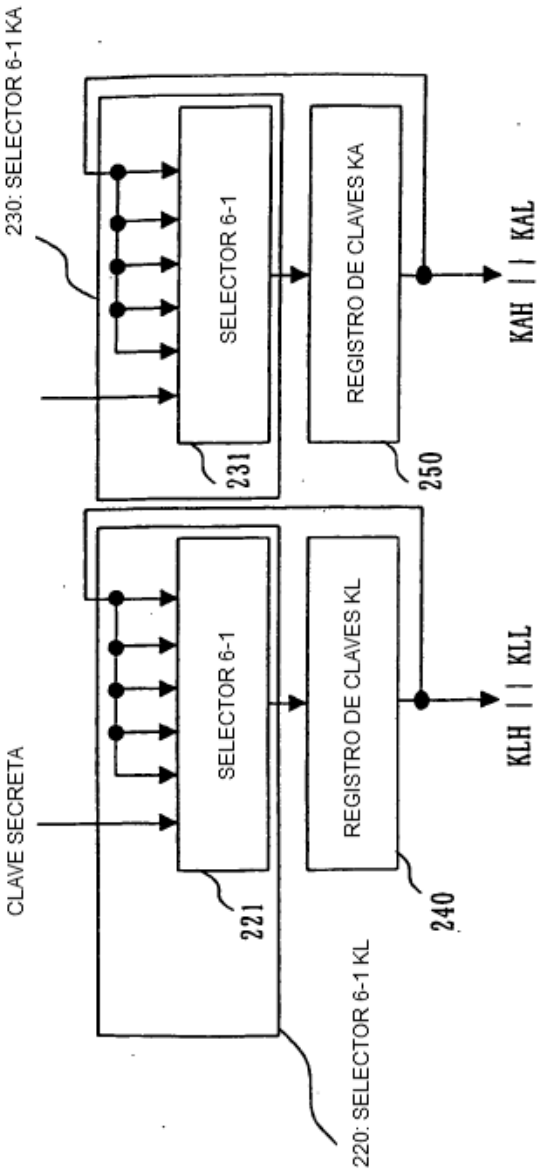

230: SELECTOR 6-1 KA
SELECTOR 6-1
231
REGISTRO DE CLAVES KA
250
KAH || KAL
CLAVE SECRETA
SELECTOR 6-1
221
REGISTRO DE CLAVES KL
240
KLH || KLL
220: SELECTOR 6-1 KL

Fig. 9

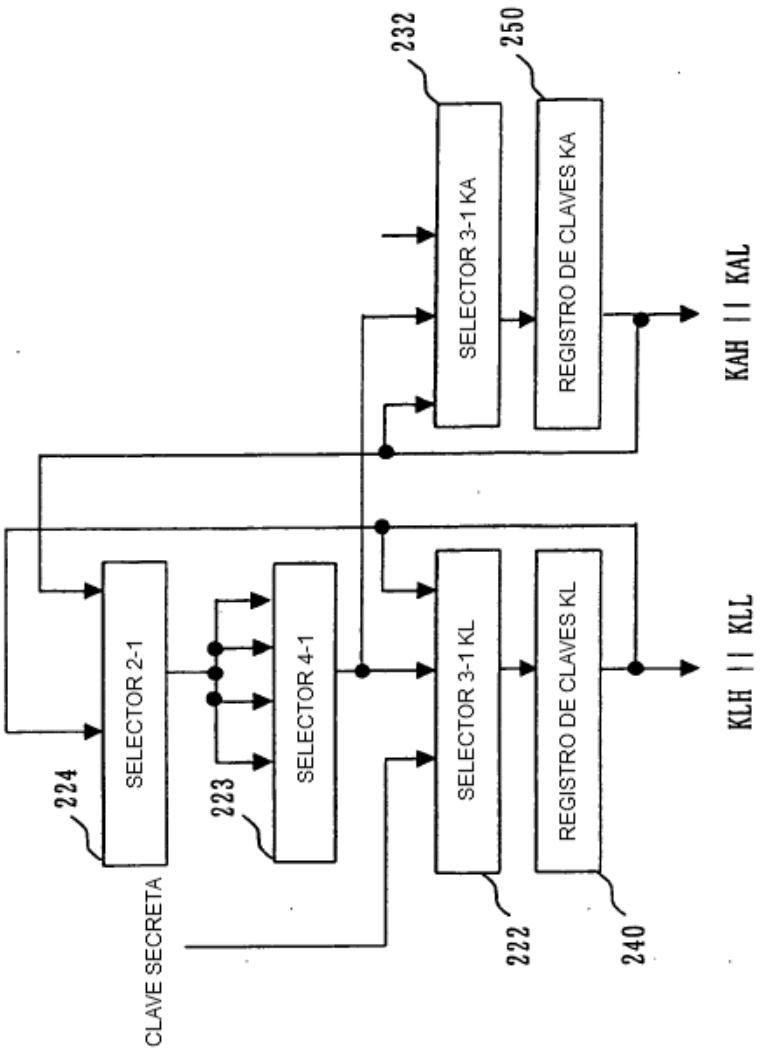

232
250
SELECTOR 3-1 KA
REGISTRO DE CLAVES KA
KAH || KAL
SELECTOR 2-1
SELECTOR 4-1
SELECTOR 3-1 KL
REGISTRO DE CLAVES KL
KLH || KLL
224
223
222
240
CLAVE SECRETA

Fig. 10

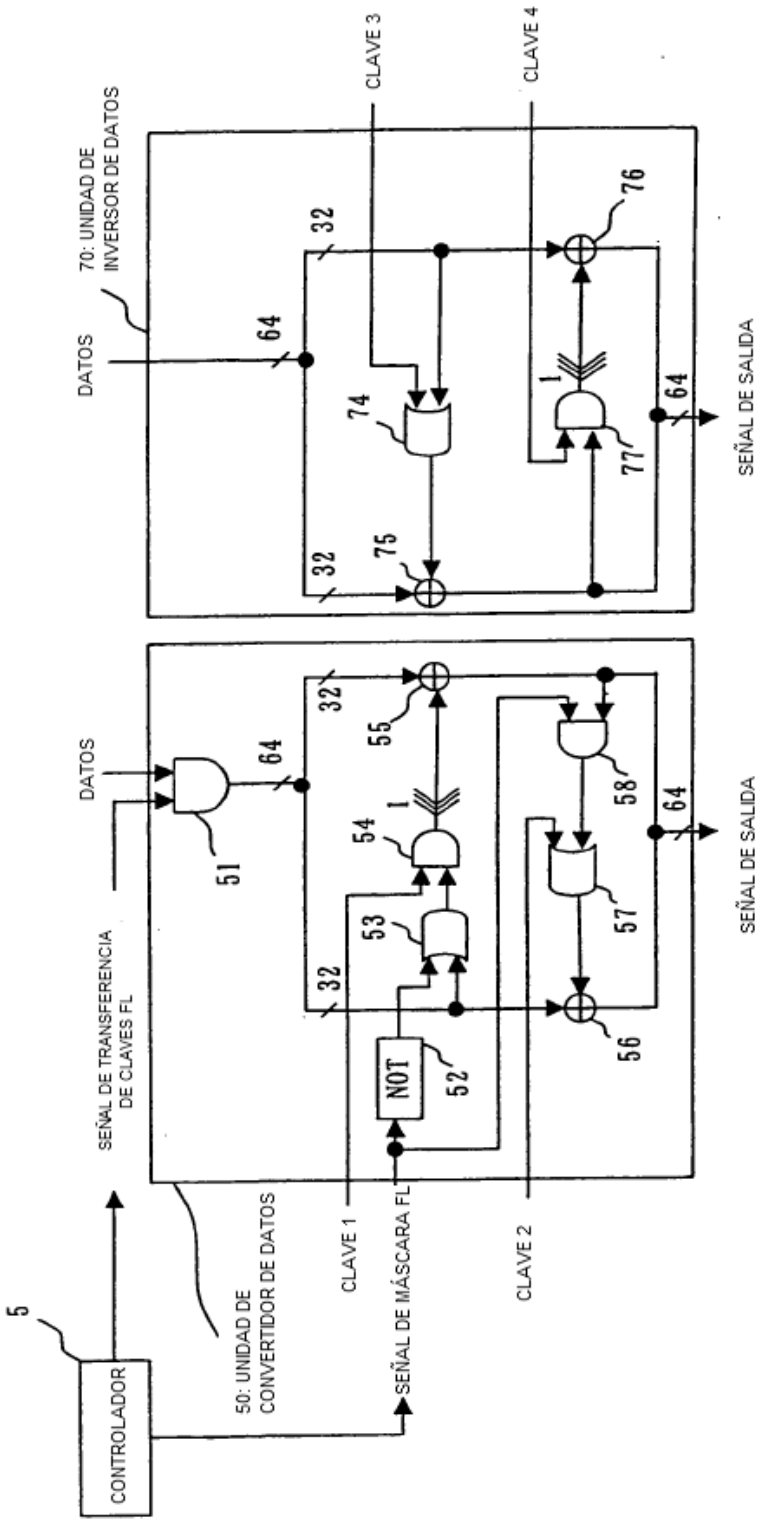

5
CONTROLADOR
50: UNIDAD DE CONVERTIDOR DE DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL
SEÑAL DE MÁSCARA FL
CLAVE 1
CLAVE 2
CLAVE 3
CLAVE 4
70: UNIDAD DE INVERSOR DE DATOS
DATOS
SEÑAL DE SALIDA
NOT
51
52
53
54
55
56
57
58
74
75
76
77
64
32
1

Fig. 11

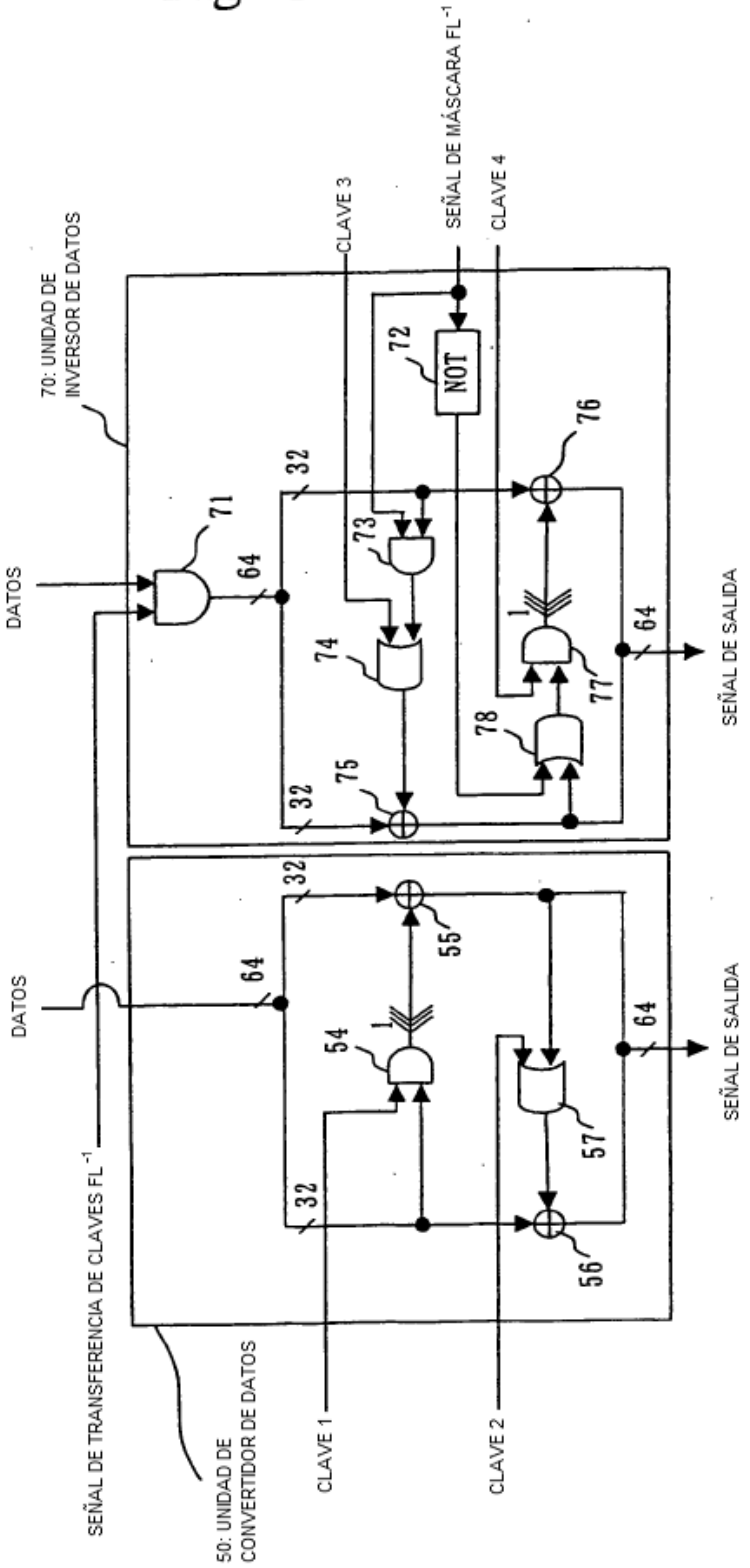

70: UNIDAD DE INVERSOR DE DATOS
CLAVE 3
SEÑAL DE MÁSCARA FL-1
CLAVE 4
NOT
72
76
32
71
73
DATOS
64
74
1
64
SEÑAL DE SALIDA
77
78
75
32
32
55
64
DATOS
54
1
64
SEÑAL DE SALIDA
57
32
56
SEÑAL DE TRANSFERENCIA DE CLAVES FL-1
50: UNIDAD DE CONVERTIDOR DE DATOS
CLAVE 1
CLAVE 2

Fig. 12

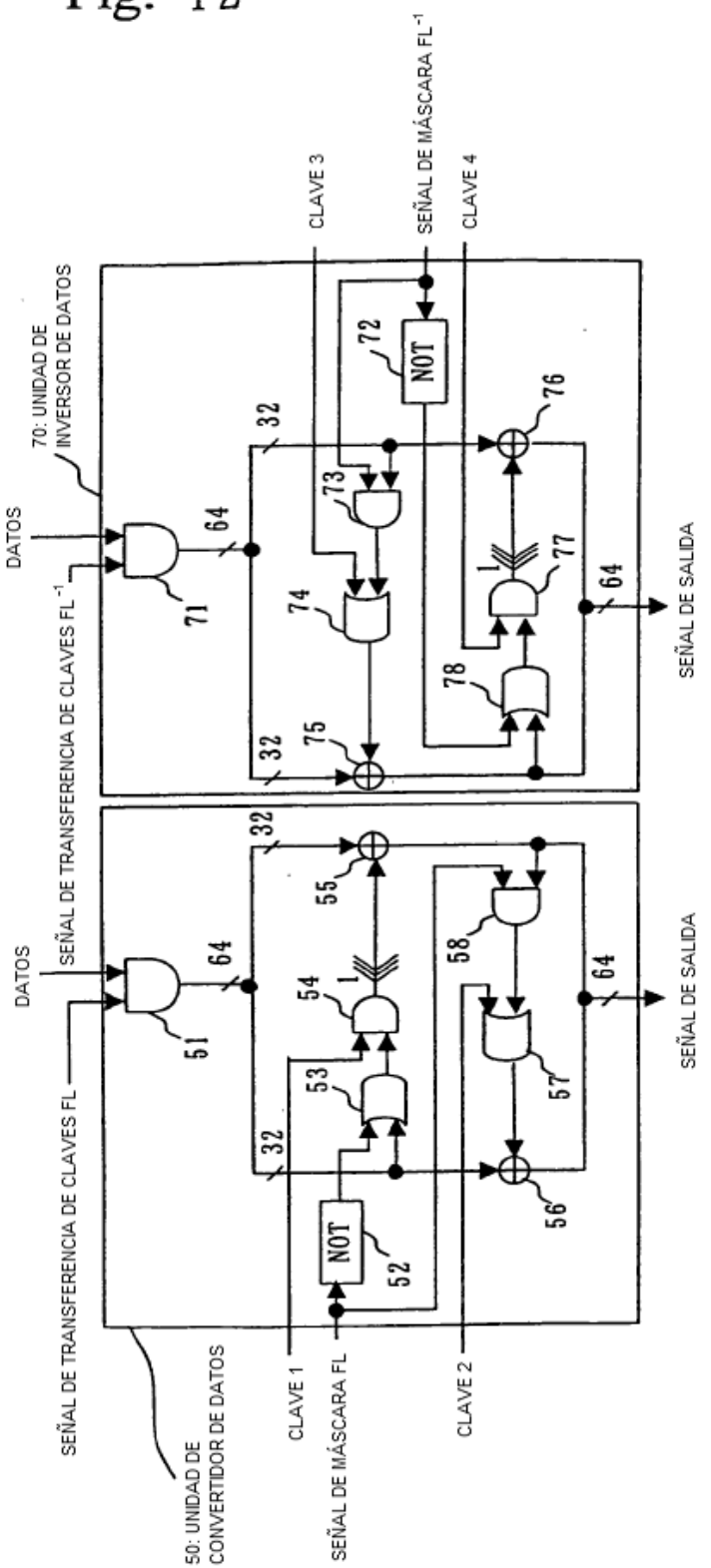

70: UNIDAD DE INVERSOR DE DATOS
DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL -1
CLAVE 3
SEÑAL DE MÁSCARA FL -1
CLAVE 4
NOT
SEÑAL DE SALIDA
SEÑAL DE TRANSFERENCIA DE CLAVES FL
50: UNIDAD DE CONVERTIDOR DE DATOS
CLAVE 1
SEÑAL DE MÁSCARA FL
CLAVE 2
NOT
SEÑAL DE SALIDA

Fig. 13

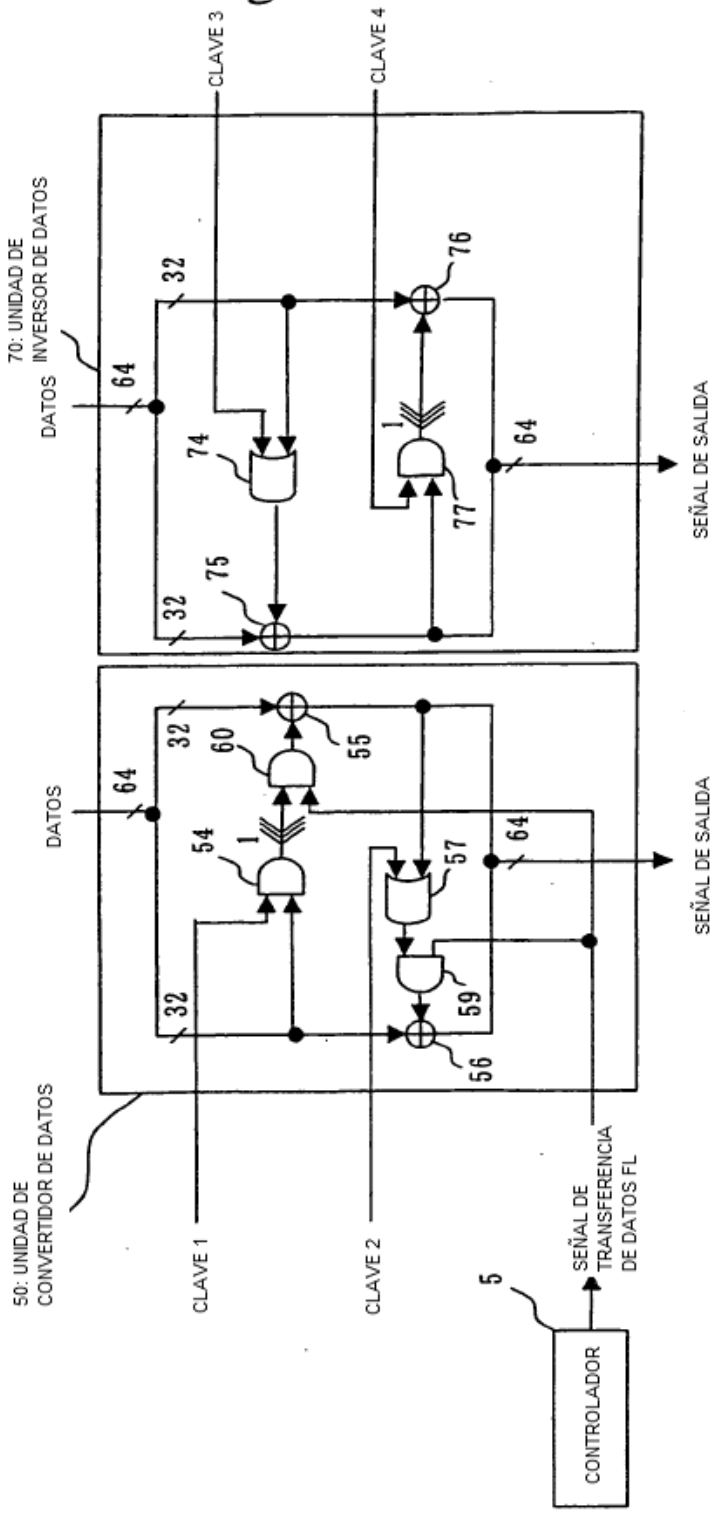

CLAVE 3
CLAVE 4
70: UNIDAD DE INVERSOR DE DATOS
DATOS
64
32
76
74
75
77
SEÑAL DE SALIDA
DATOS
64
32
60
55
54
57
59
56
SEÑAL DE SALIDA
50: UNIDAD DE CONVERTIDOR DE DATOS
CLAVE 1
CLAVE 2
SEÑAL DE TRANSFERENCIA DE DATOS FL
5
CONTROLADOR

Fig. 14

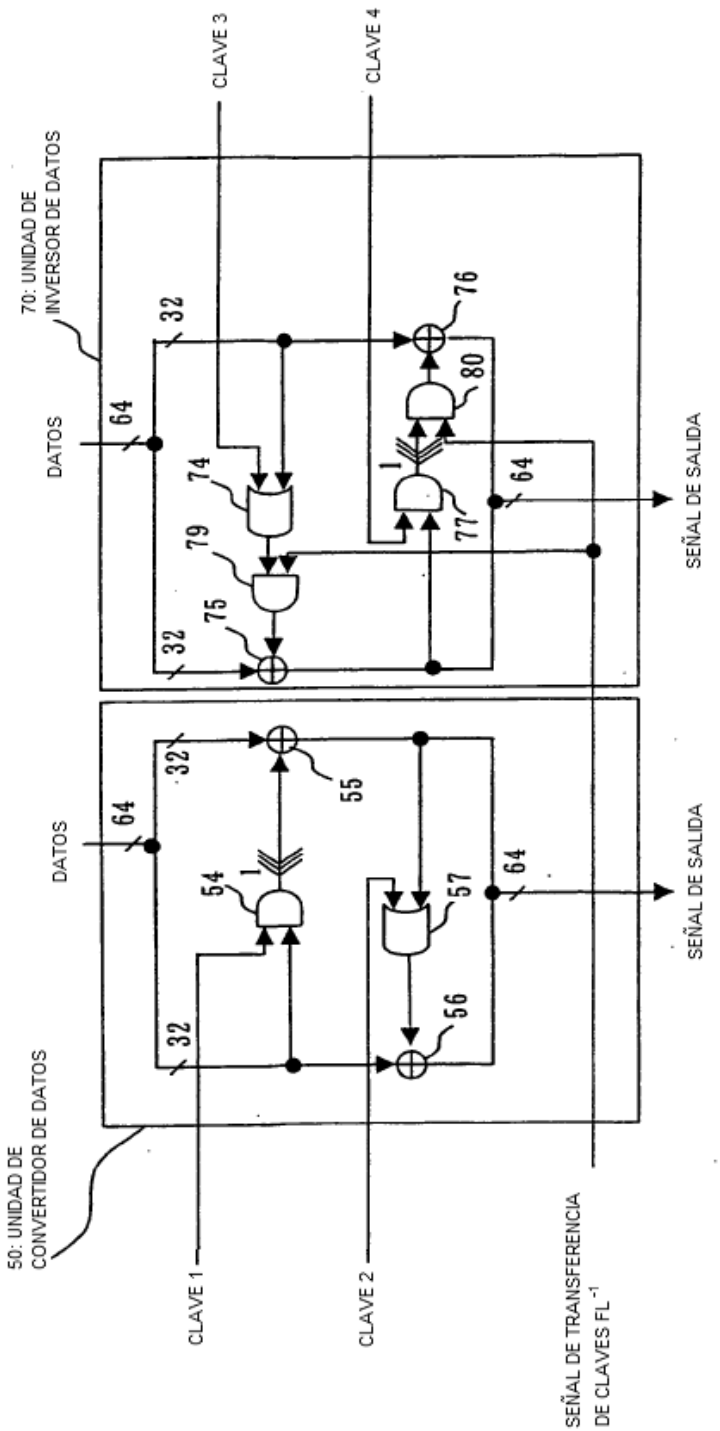

70: UNIDAD DE INVERSOR DE DATOS
CLAVE 3
CLAVE 4
DATOS
64
32
74
79
75
76
80
77
SEÑAL DE SALIDA
50: UNIDAD DE CONVERTIDOR DE DATOS
55
54
57
56
CLAVE 1
CLAVE 2
SEÑAL DE TRANSFERENCIA DE CLAVES FL -1

Fig. 15

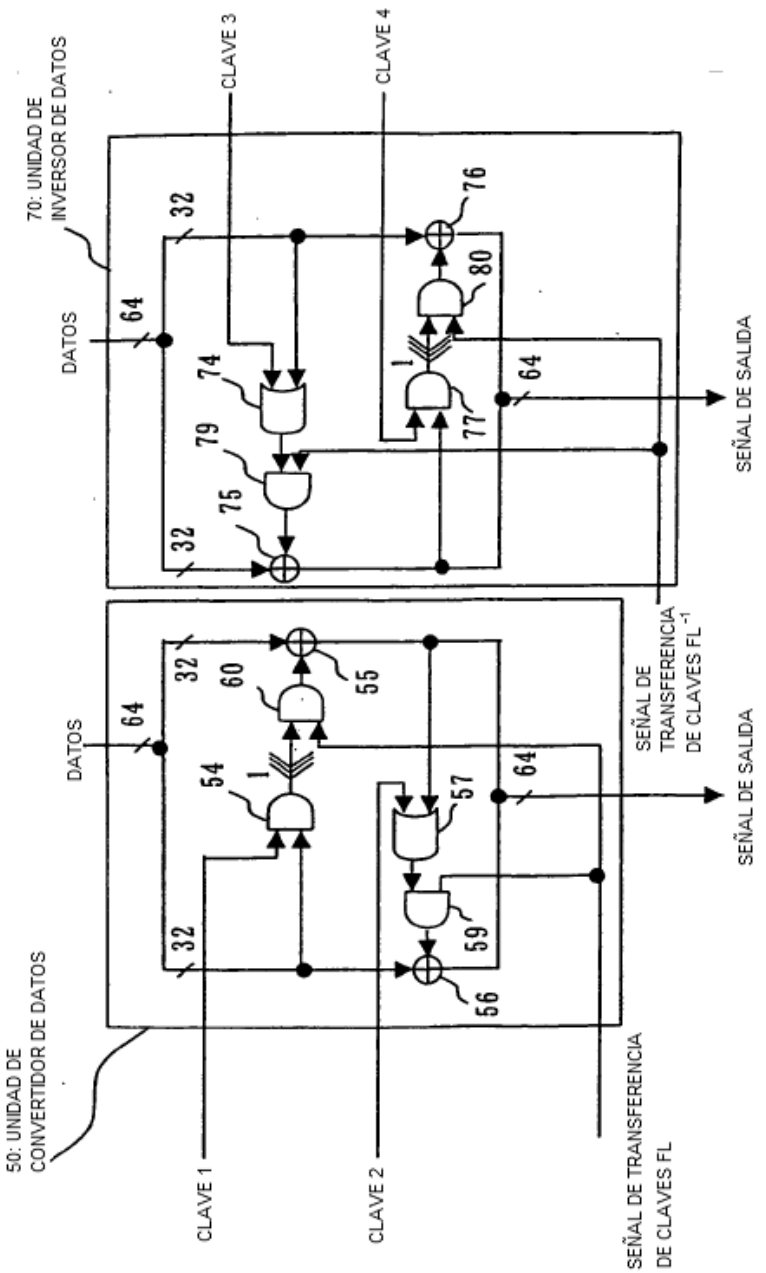

70: UNIDAD DE INVERSOR DE DATOS
CLAVE 3
CLAVE 4
DATOS
64
32
74
79
75
76
80
77
SEÑAL DE SALIDA
SEÑAL DE TRANSFERENCIA DE CLAVES FL-1
50: UNIDAD DE CONVERTIDOR DE DATOS
60
55
54
57
59
56
CLAVE 1
CLAVE 2
SEÑAL DE TRANSFERENCIA DE CLAVES FL

Fig. 16

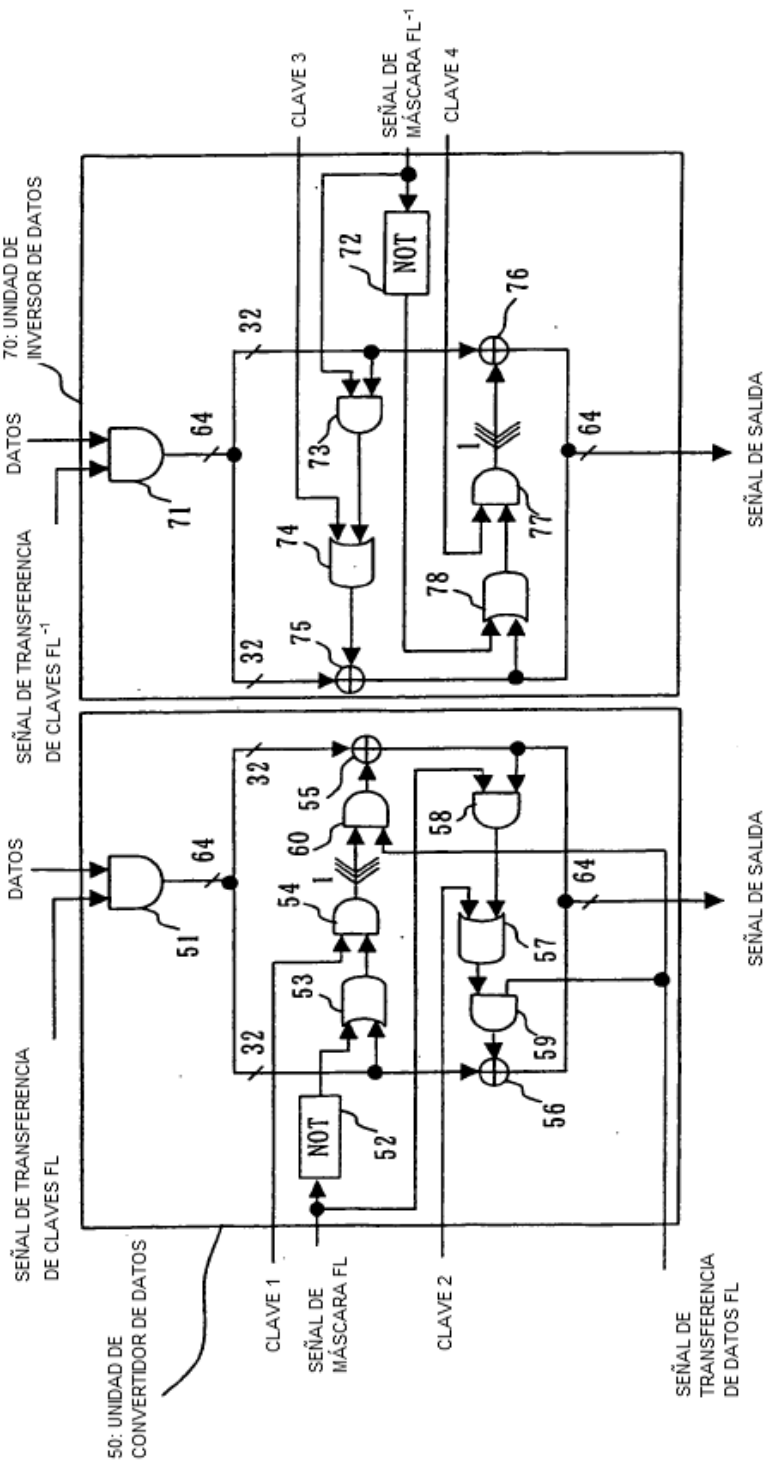

70: UNIDAD DE INVERSOR DE DATOS
DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL-1
CLAVE 3
SEÑAL DE MÁSCARA FL-1
CLAVE 4
NOT
SEÑAL DE SALIDA
50: UNIDAD DE CONVERTIDOR DE DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL
CLAVE 1
SEÑAL DE MÁSCARA FL
CLAVE 2
SEÑAL DE TRANSFERENCIA DE DATOS FL

Fig. 17

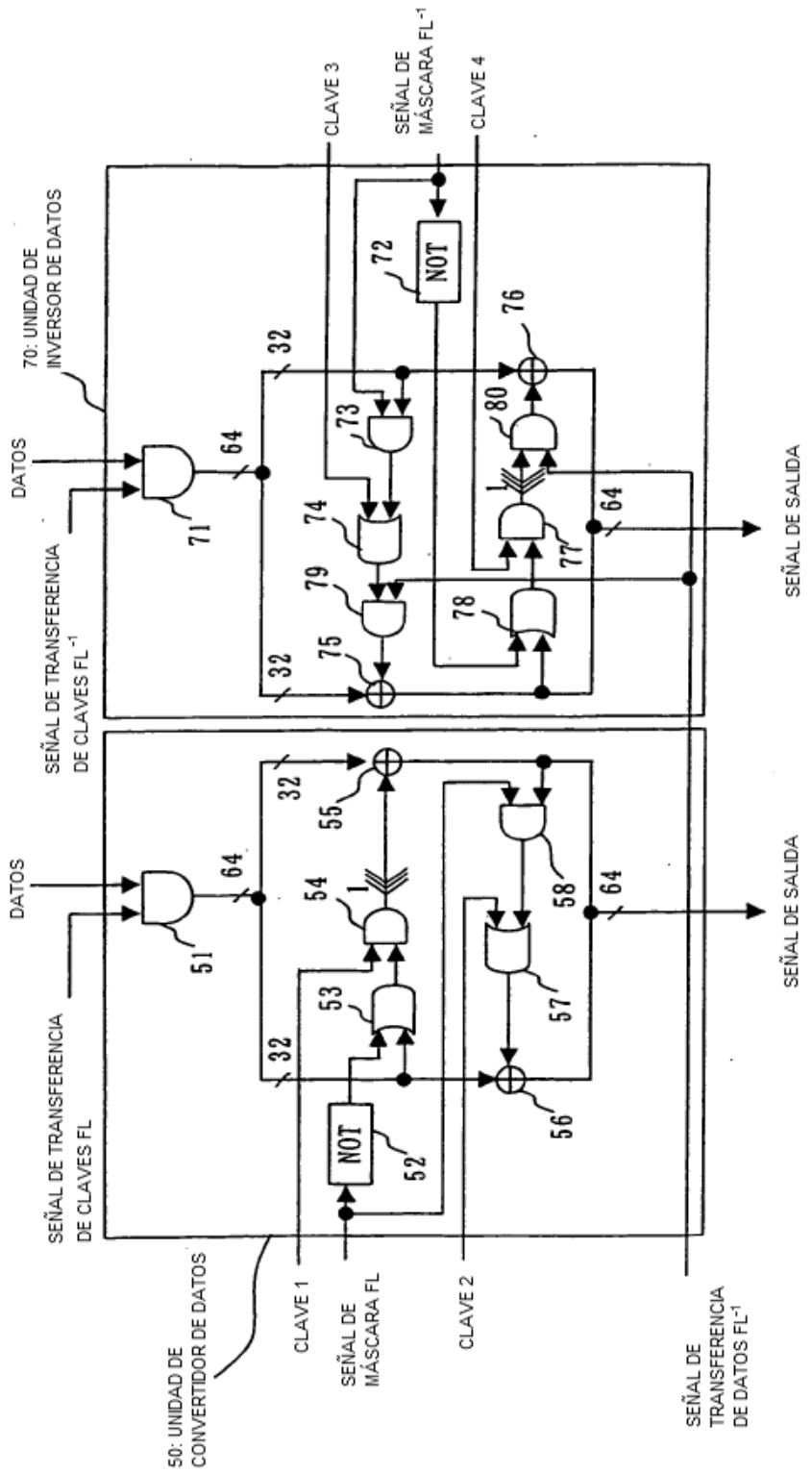

70: UNIDAD DE INVERSOR DE DATOS
DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL-1
CLAVE 3
SEÑAL DE MÁSCARA FL-1
CLAVE 4
NOT
SEÑAL DE SALIDA
50: UNIDAD DE CONVERTIDOR DE DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL
CLAVE 1
SEÑAL DE MÁSCARA FL
CLAVE 2
SEÑAL DE TRANSFERENCIA DE DATOS FL-1

Fig. 18

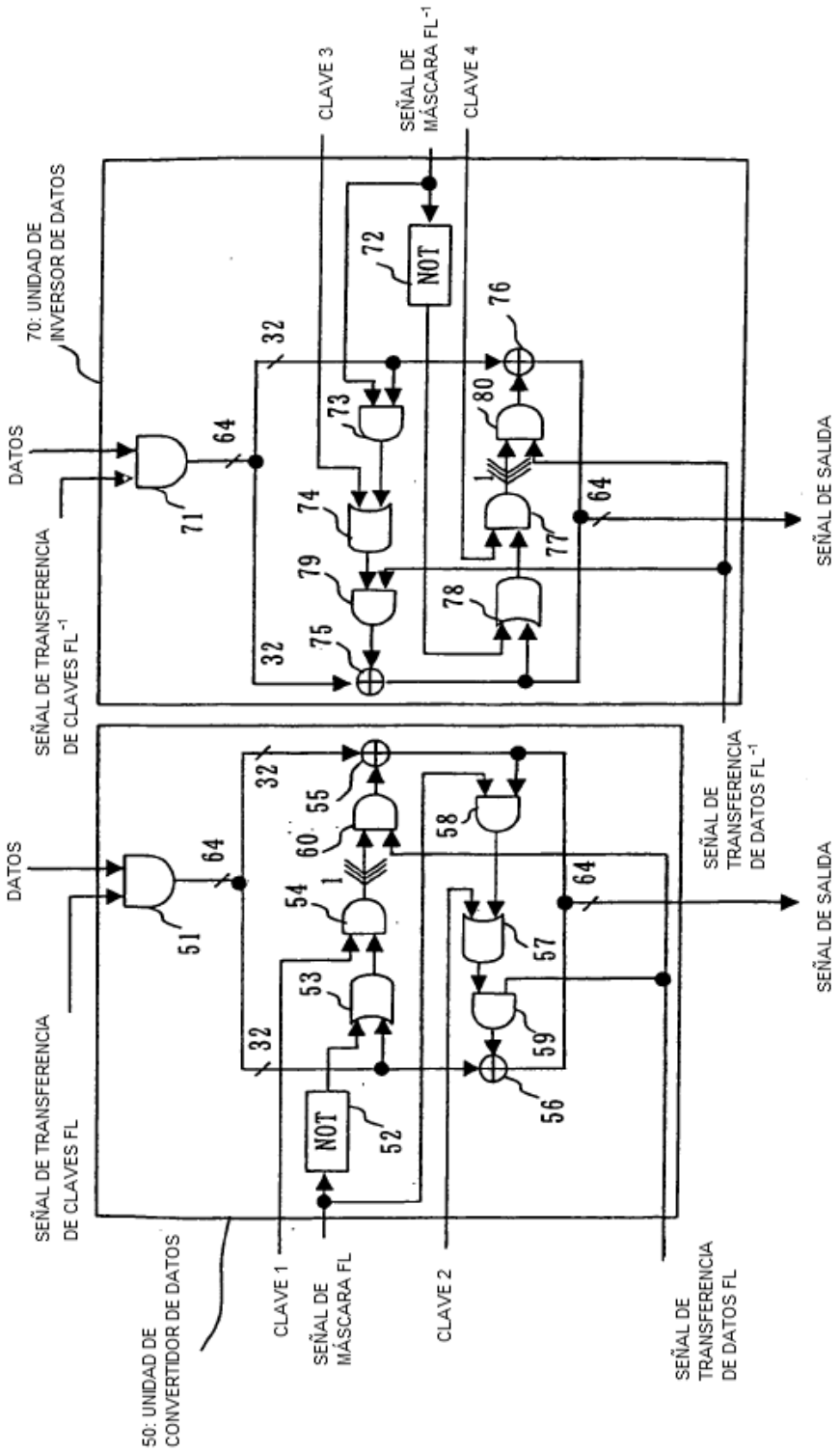

70: UNIDAD DE INVERSOR DE DATOS
DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL^{-1}
CLAVE 3
SEÑAL DE MÁSCARA FL^{-1}
CLAVE 4
SEÑAL DE SALIDA
SEÑAL DE TRANSFERENCIA DE DATOS FL^{-1}
50: UNIDAD DE CONVERTIDOR DE DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL
CLAVE 1
SEÑAL DE MÁSCARA FL
CLAVE 2
SEÑAL DE TRANSFERENCIA DE DATOS FL
NOT
1
32
64

Fig. 19

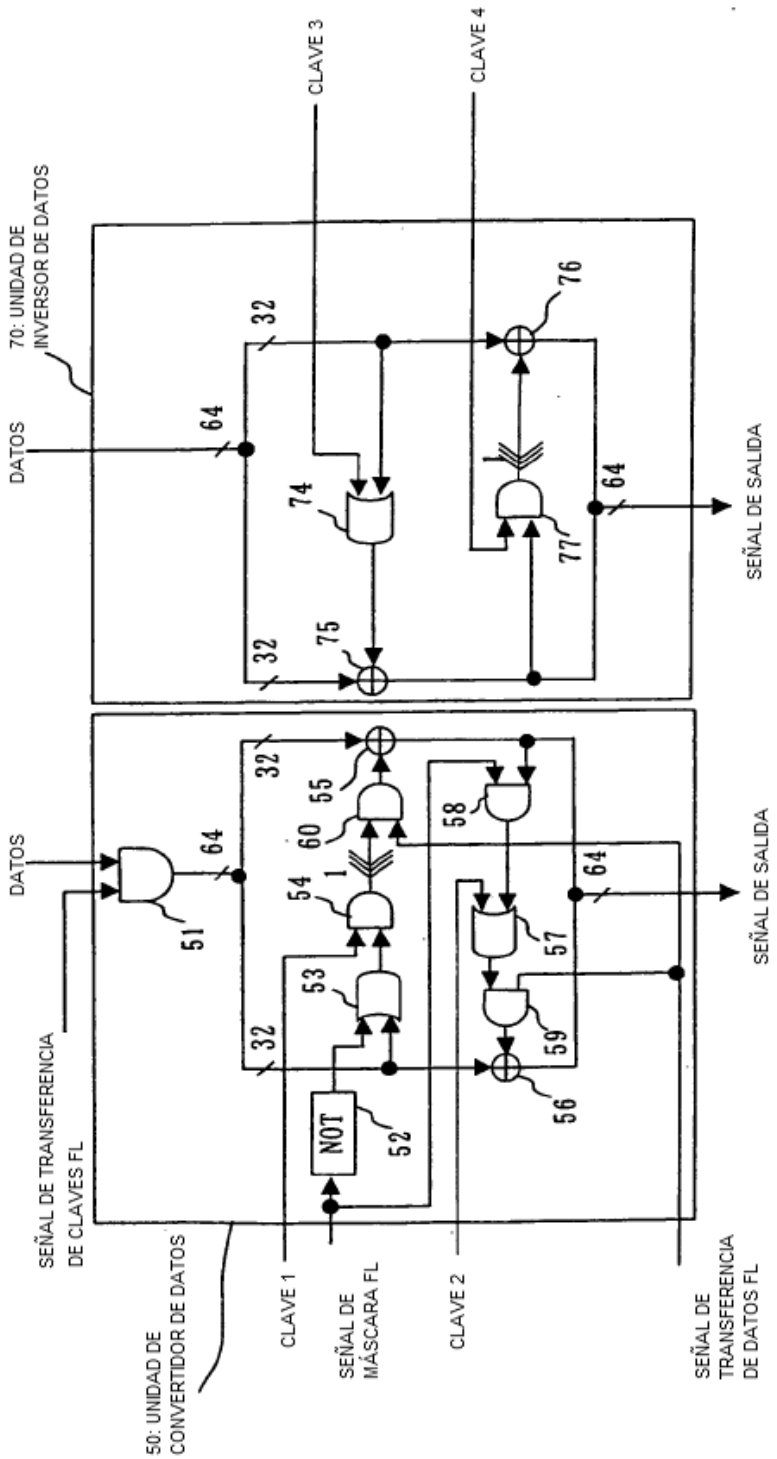

70: UNIDAD DE INVERSOR DE DATOS
DATOS
64
32
CLAVE 3
CLAVE 4
76
74
75
77
64
SEÑAL DE SALIDA
50: UNIDAD DE CONVERTIDOR DE DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL
DATOS
51
64
32
55
60
58
54
1
53
57
59
56
52
NOT
64
SEÑAL DE SALIDA
CLAVE 1
SEÑAL DE MÁSCARA FL
CLAVE 2
SEÑAL DE TRANSFERENCIA DE DATOS FL

Fig. 20

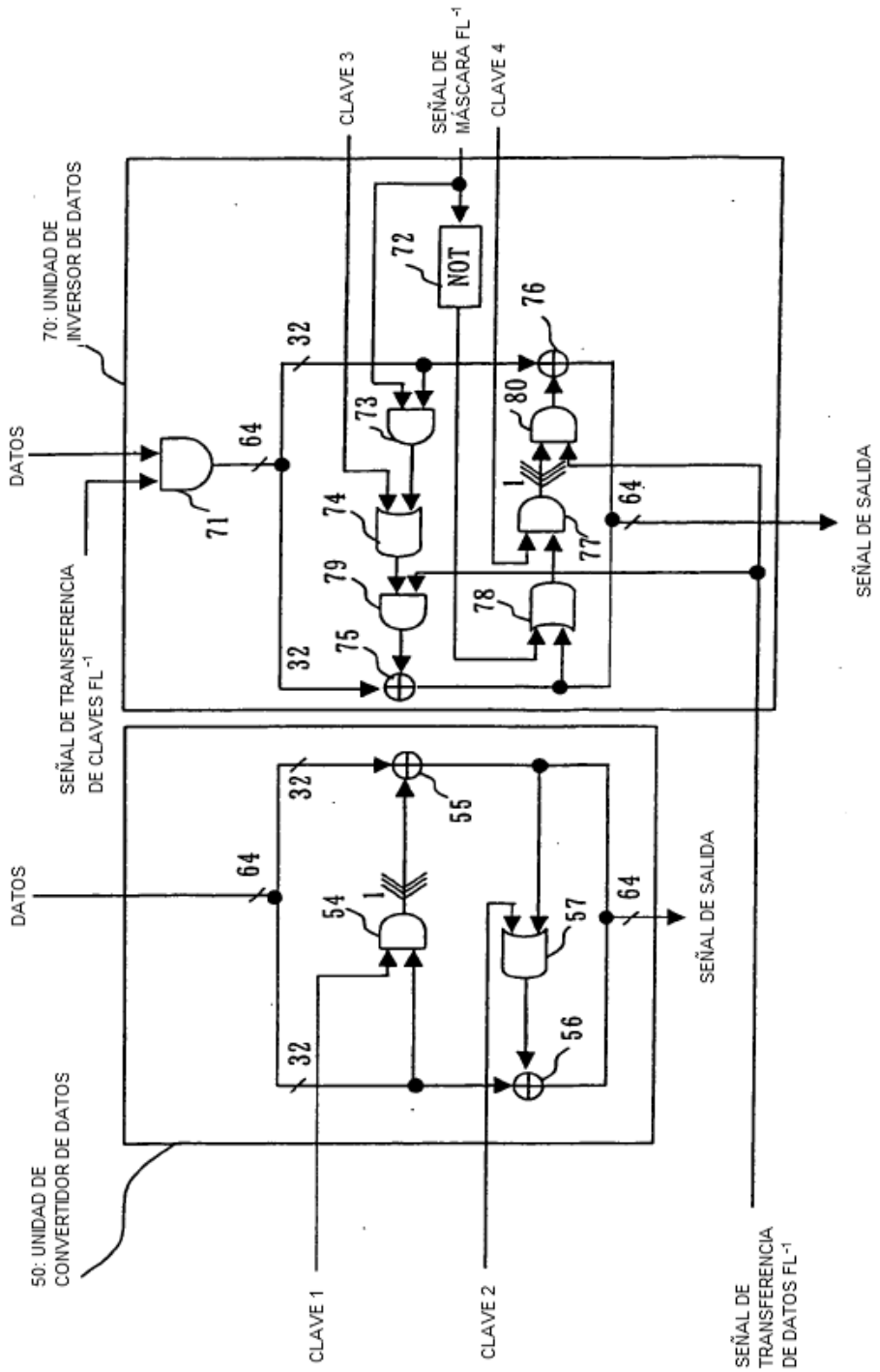

70: UNIDAD DE INVERSOR DE DATOS
DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL-1
CLAVE 3
SEÑAL DE MÁSCARA FL-1
CLAVE 4
NOT
SEÑAL DE SALIDA
50: UNIDAD DE CONVERTIDOR DE DATOS
DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL-1
SEÑAL DE SALIDA
CLAVE 1
CLAVE 2
SEÑAL DE TRANSFERENCIA DE DATOS FL-1

Fig. 21

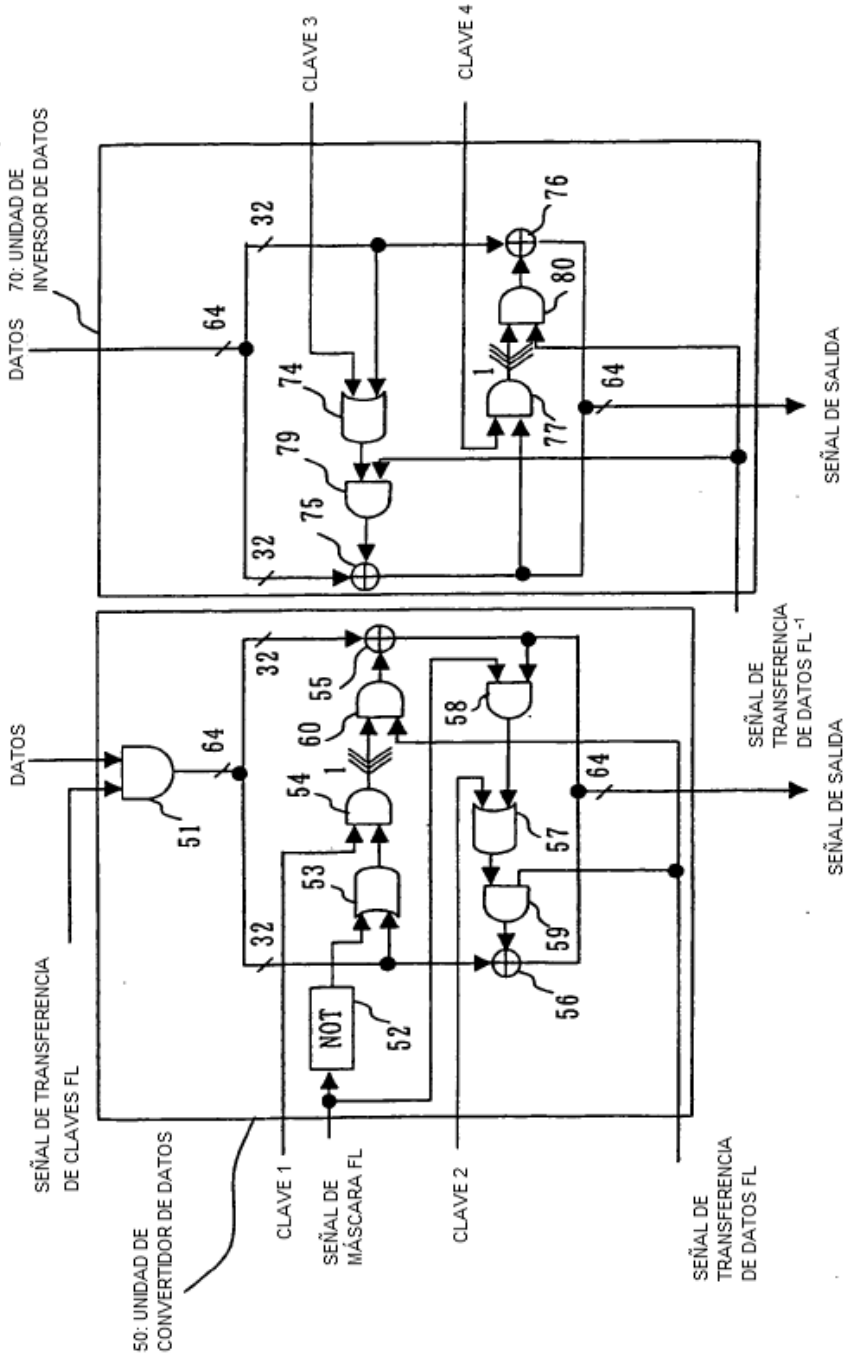

DATOS
70: UNIDAD DE INVERSOR DE DATOS
CLAVE 3
CLAVE 4
SEÑAL DE SALIDA
SEÑAL DE TRANSFERENCIA DE DATOS FL -1
SEÑAL DE TRANSFERENCIA DE CLAVES FL
50: UNIDAD DE CONVERTIDOR DE DATOS
CLAVE 1
SEÑAL DE MÁSCARA FL
CLAVE 2
SEÑAL DE TRANSFERENCIA DE DATOS FL
NOT

Fig. 22

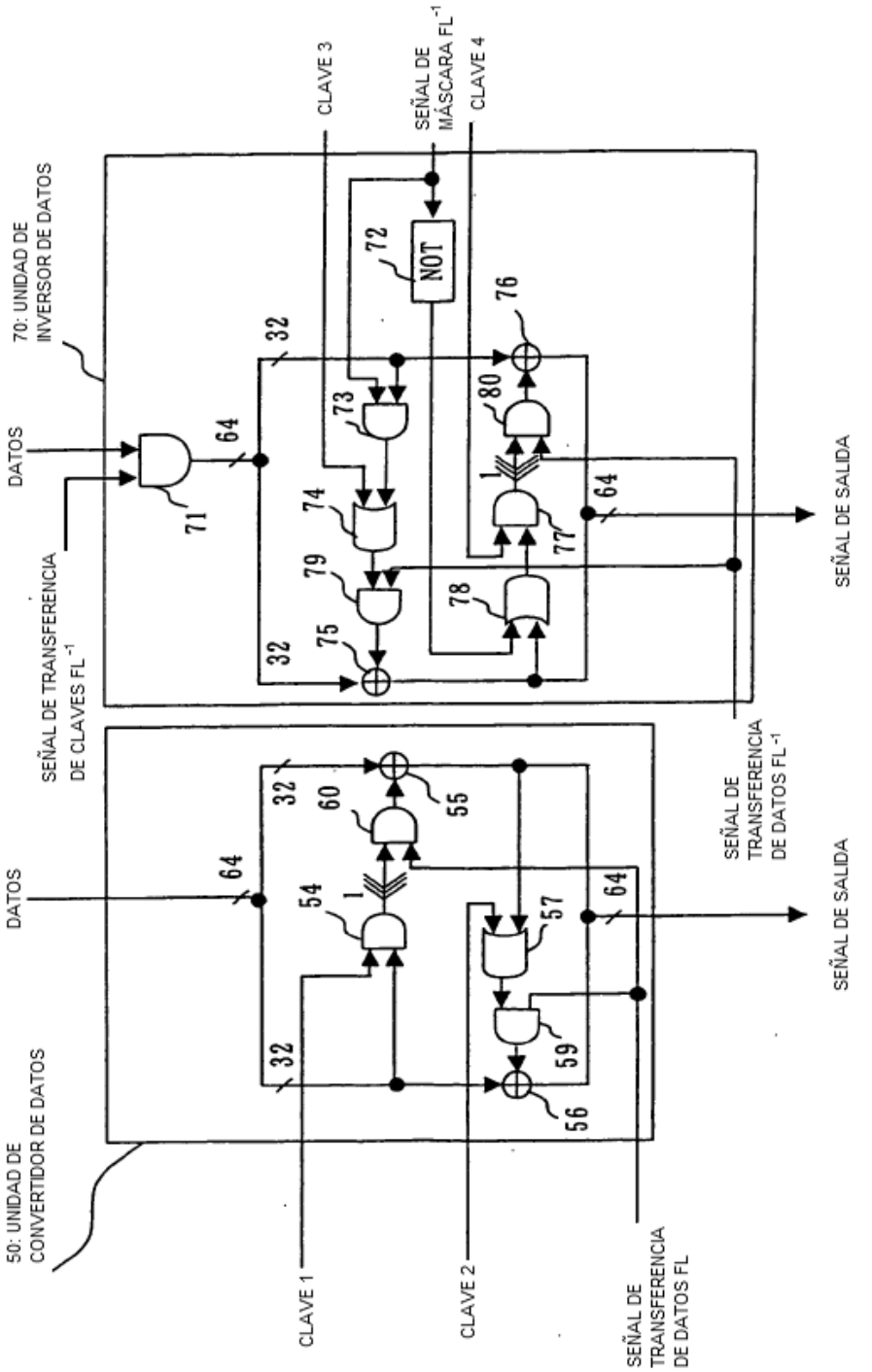

70: UNIDAD DE INVERSOR DE DATOS
50: UNIDAD DE CONVERTIDOR DE DATOS
DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL-1
SEÑAL DE MÁSCARA FL-1
CLAVE 3
CLAVE 4
CLAVE 1
CLAVE 2
SEÑAL DE TRANSFERENCIA DE DATOS FL
SEÑAL DE TRANSFERENCIA DE DATOS FL-1
SEÑAL DE SALIDA
NOT
71
72
73
74
75
76
77
78
79
80
54
55
56
57
59
60
64
32
1

Fig. 23

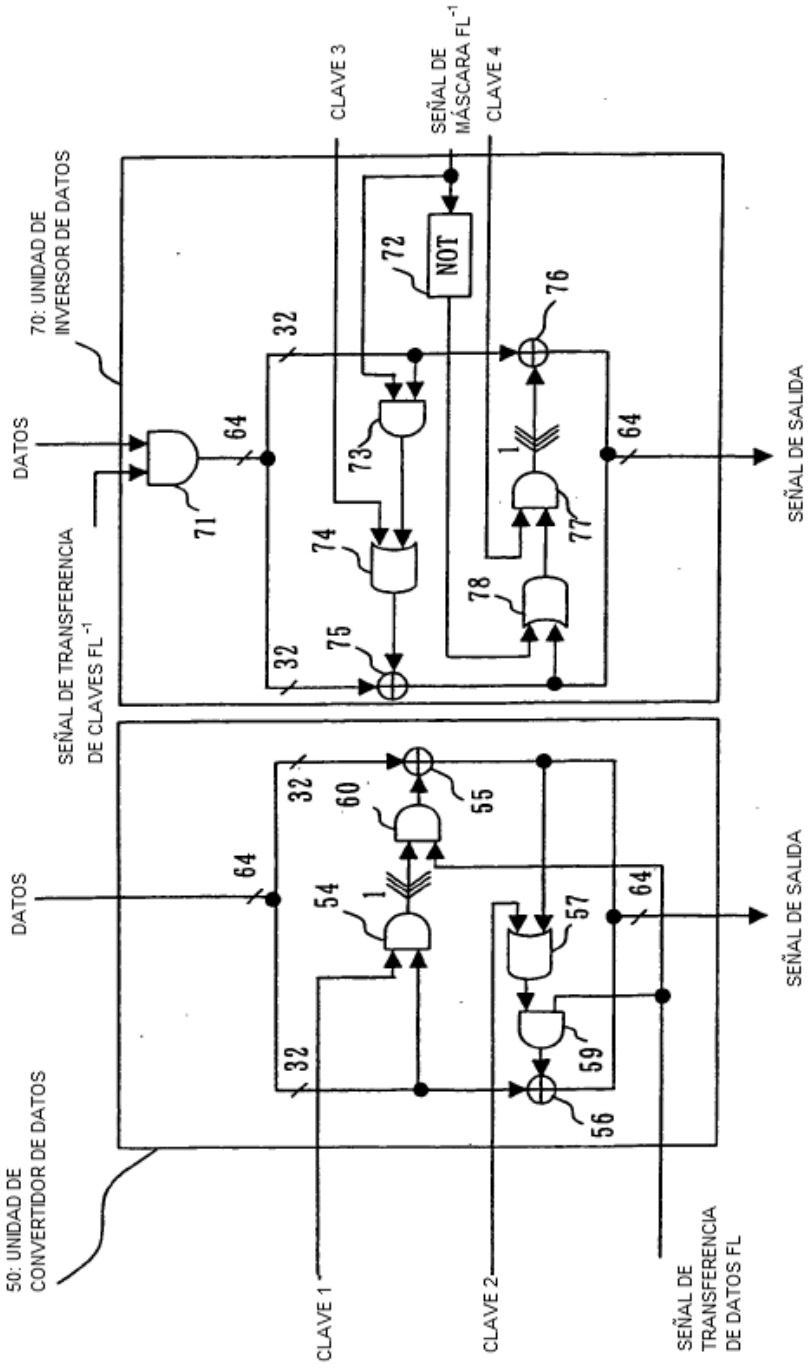

50: UNIDAD DE CONVERTIDOR DE DATOS
70: UNIDAD DE INVERSOR DE DATOS
DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL-1
SEÑAL DE MÁSCARA FL-1
CLAVE 1
CLAVE 2
CLAVE 3
CLAVE 4
SEÑAL DE TRANSFERENCIA DE DATOS FL
SEÑAL DE SALIDA
NOT
64
32
1

Fig. 24

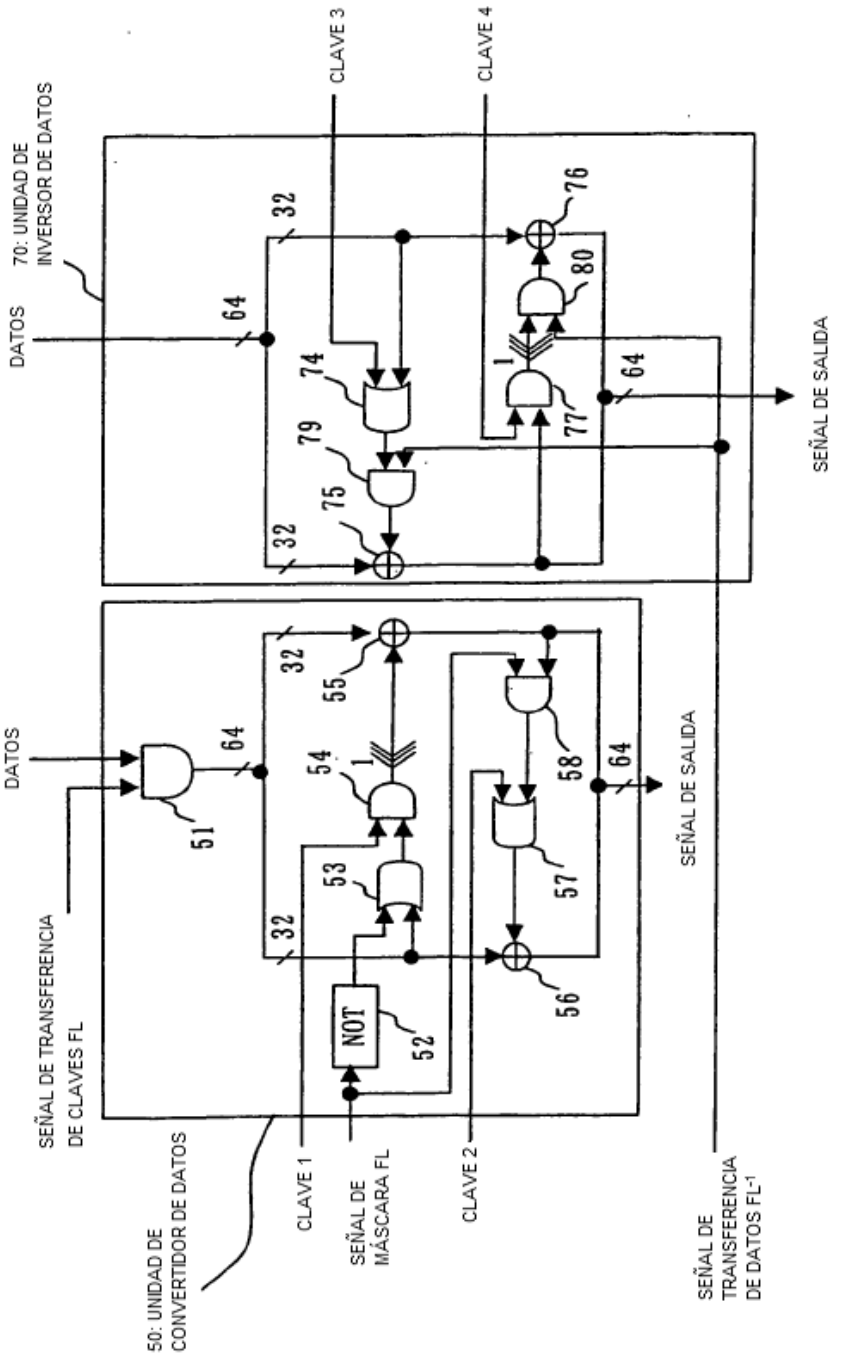

70: UNIDAD DE INVERSOR DE DATOS
DATOS
CLAVE 3
CLAVE 4
SEÑAL DE SALIDA
SEÑAL DE TRANSFERENCIA DE CLAVES FL
50: UNIDAD DE CONVERTIDOR DE DATOS
CLAVE 1
SEÑAL DE MÁSCARA FL
CLAVE 2
SEÑAL DE TRANSFERENCIA DE DATOS FL-1
NOT

Fig. 25

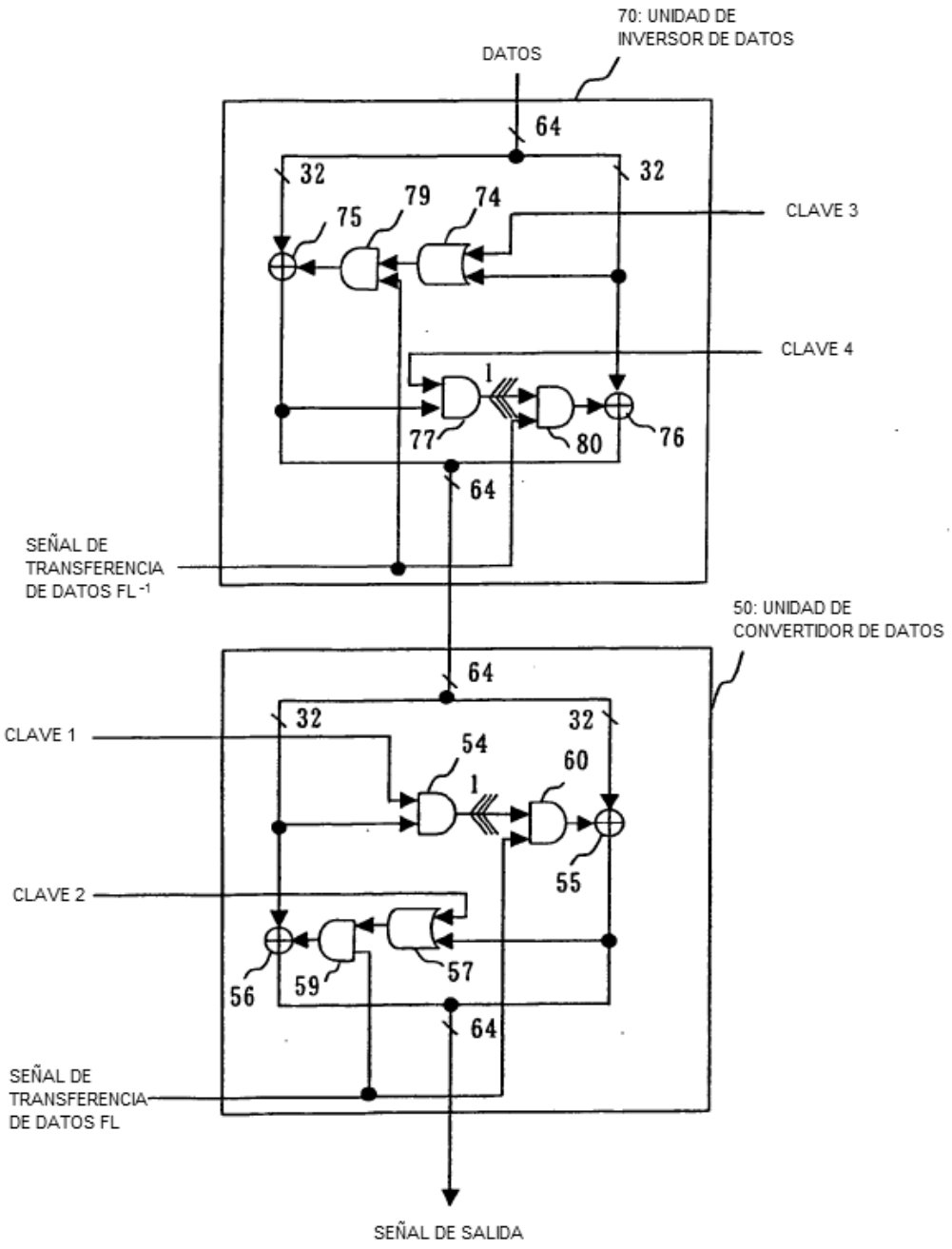

70: UNIDAD DE INVERSOR DE DATOS
DATOS
64
32
32
75
79
74
CLAVE 3
CLAVE 4
1
77
80
76
64
SEÑAL DE TRANSFERENCIA DE DATOS FL-1
50: UNIDAD DE CONVERTIDOR DE DATOS
64
CLAVE 1
32
32
54
60
1
55
CLAVE 2
56
59
57
64
SEÑAL DE TRANSFERENCIA DE DATOS FL
SEÑAL DE SALIDA

Fig. 26

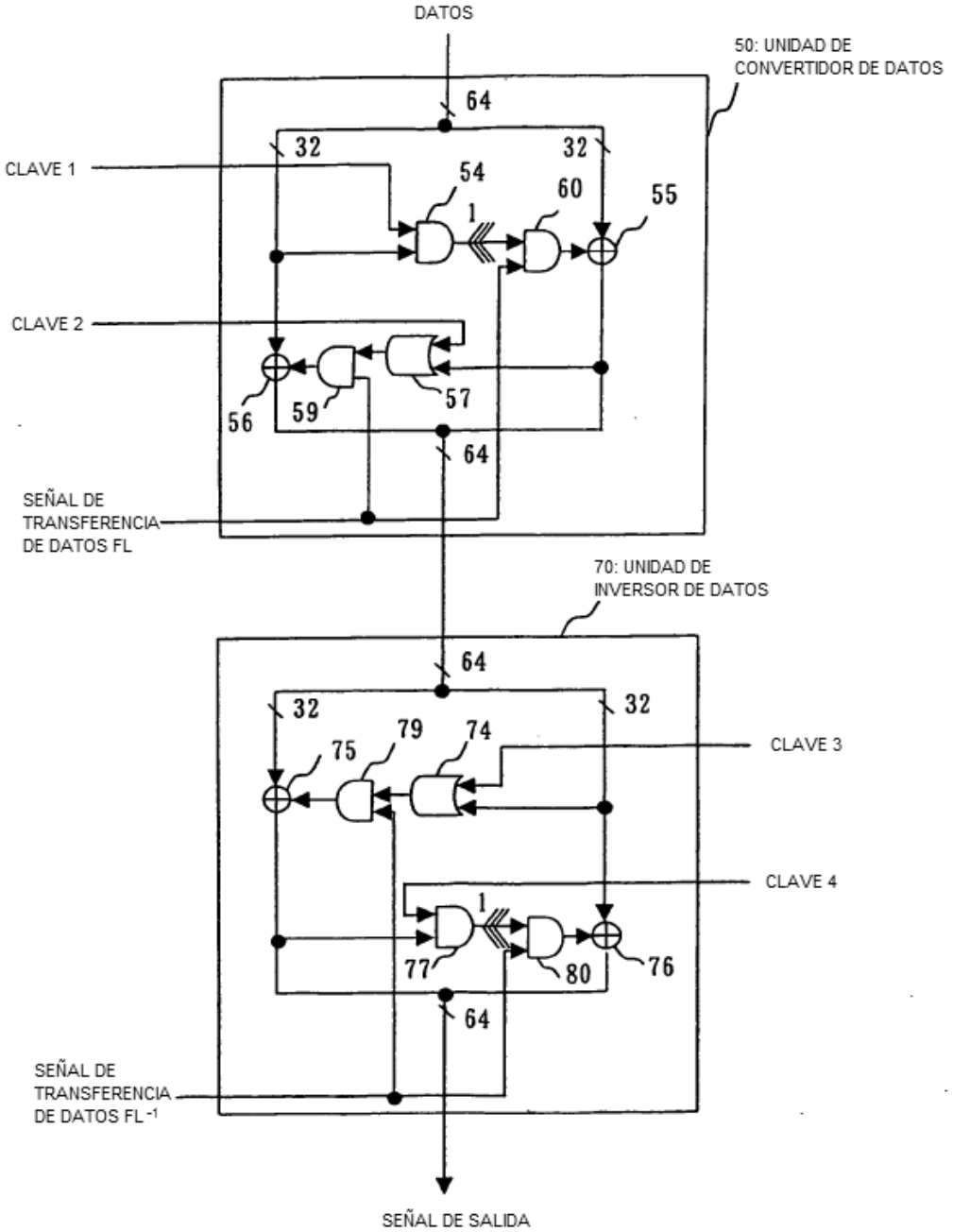

DATOS
50: UNIDAD DE CONVERTIDOR DE DATOS
64
32
32
CLAVE 1
54
60
55
1
CLAVE 2
56
59
57
64
SEÑAL DE TRANSFERENCIA DE DATOS FL
70: UNIDAD DE INVERSOR DE DATOS
64
32
32
75
79
74
CLAVE 3
CLAVE 4
1
77
80
76
64
SEÑAL DE TRANSFERENCIA DE DATOS FL-1
SEÑAL DE SALIDA

Fig. 27

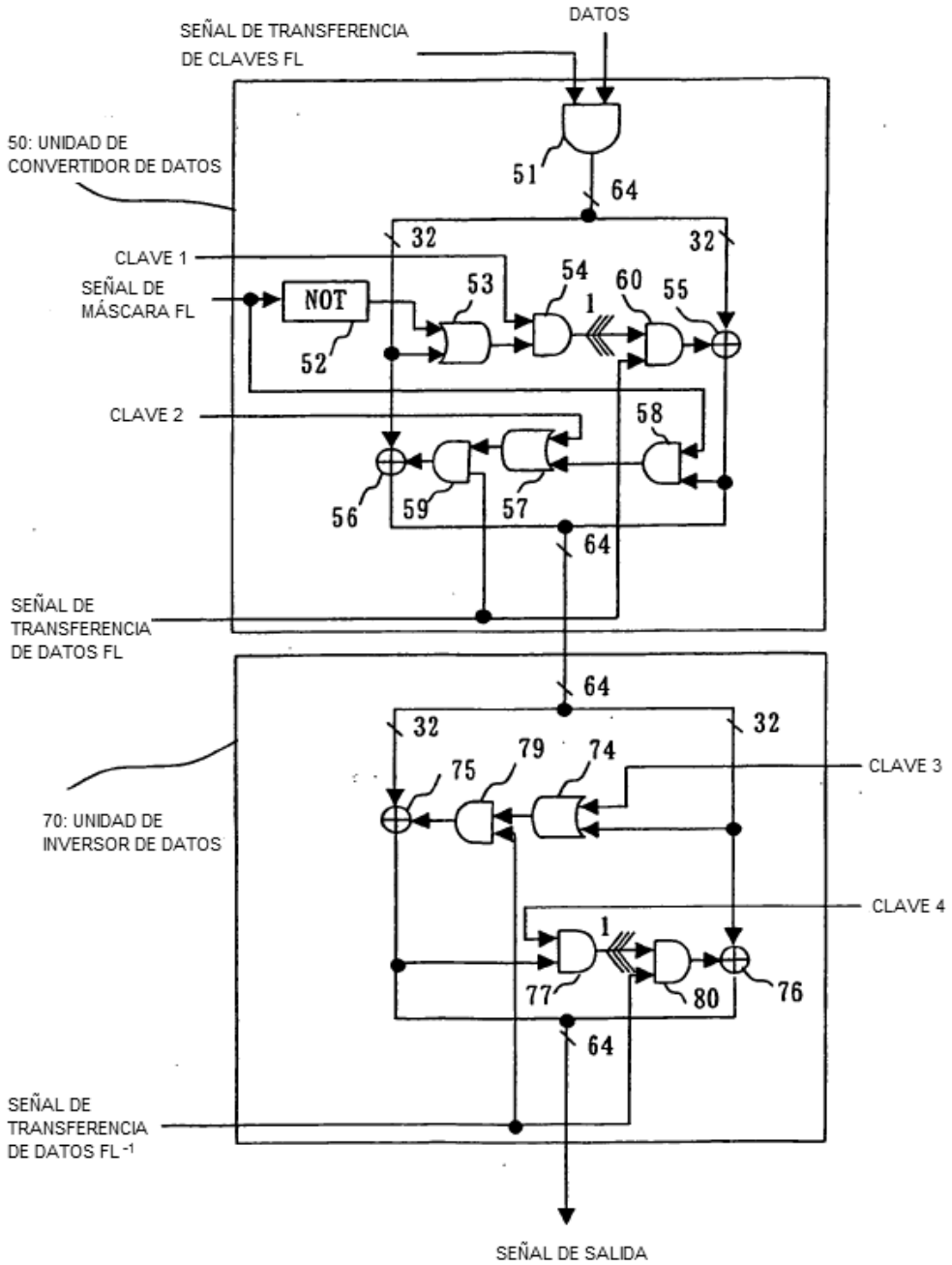

DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL
50: UNIDAD DE CONVERTIDOR DE DATOS
51
64
32
32
CLAVE 1
SEÑAL DE MÁSCARA FL
NOT
53
54
60
55
1
52
CLAVE 2
58
56
59
57
64
SEÑAL DE TRANSFERENCIA DE DATOS FL
64
32
32
79
74
75
CLAVE 3
70: UNIDAD DE INVERSOR DE DATOS
CLAVE 4
1
77
80
76
64
SEÑAL DE TRANSFERENCIA DE DATOS FL-1
SEÑAL DE SALIDA

Fig. 28

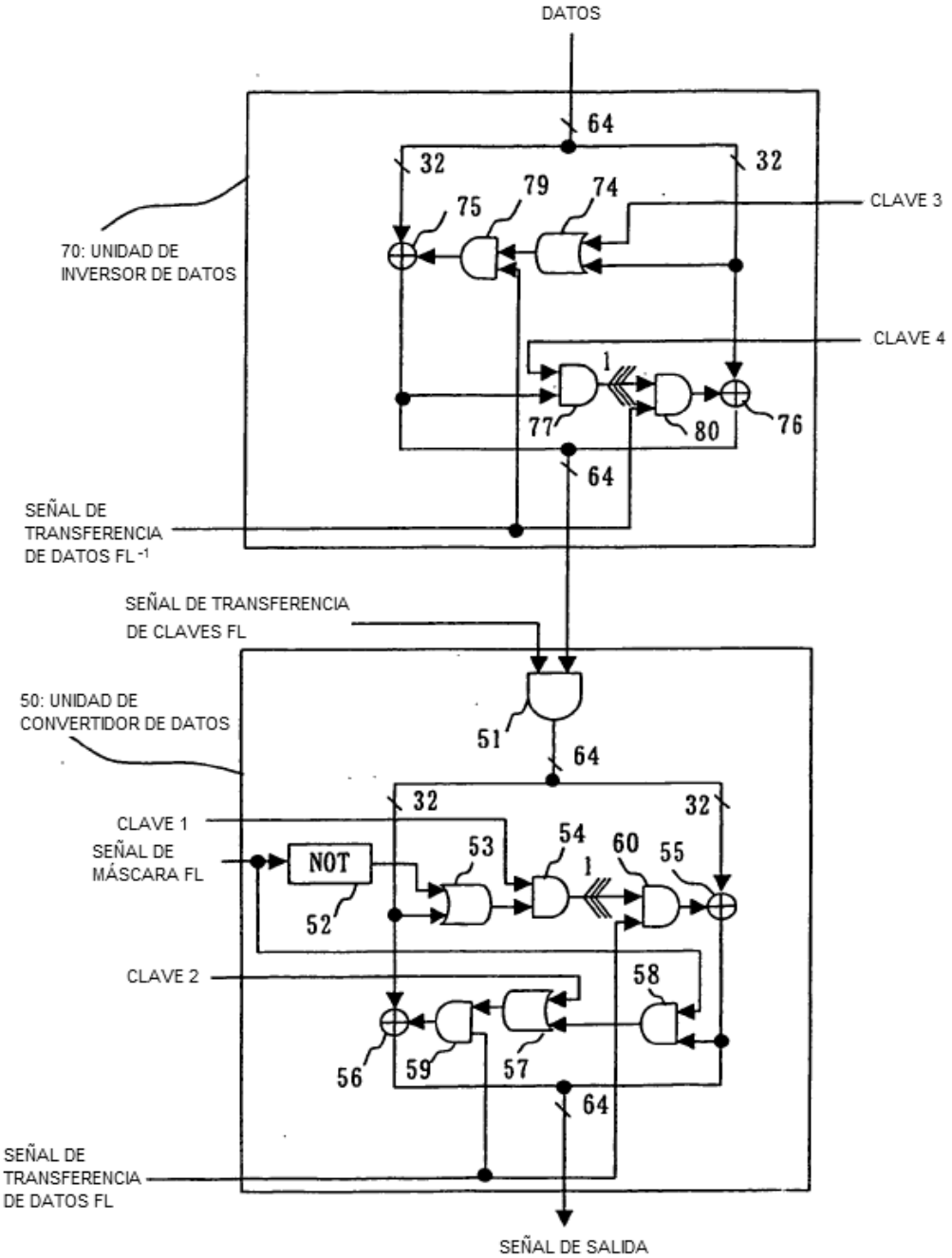

DATOS
64
32
32
75
79
74
CLAVE 3
70: UNIDAD DE
INVERSOR DE DATOS
CLAVE 4
1
77
80
76
64
SEÑAL DE
TRANSFERENCIA
DE DATOS FL -1
SEÑAL DE TRANSFERENCIA
DE CLAVES FL
50: UNIDAD DE
CONVERTIDOR DE DATOS
51
64
32
32
CLAVE 1
SEÑAL DE
MÁSCARA FL
NOT
53
54
1
60
55
52
CLAVE 2
58
56
59
57
64
SEÑAL DE
TRANSFERENCIA
DE DATOS FL
SEÑAL DE SALIDA

Fig. 29

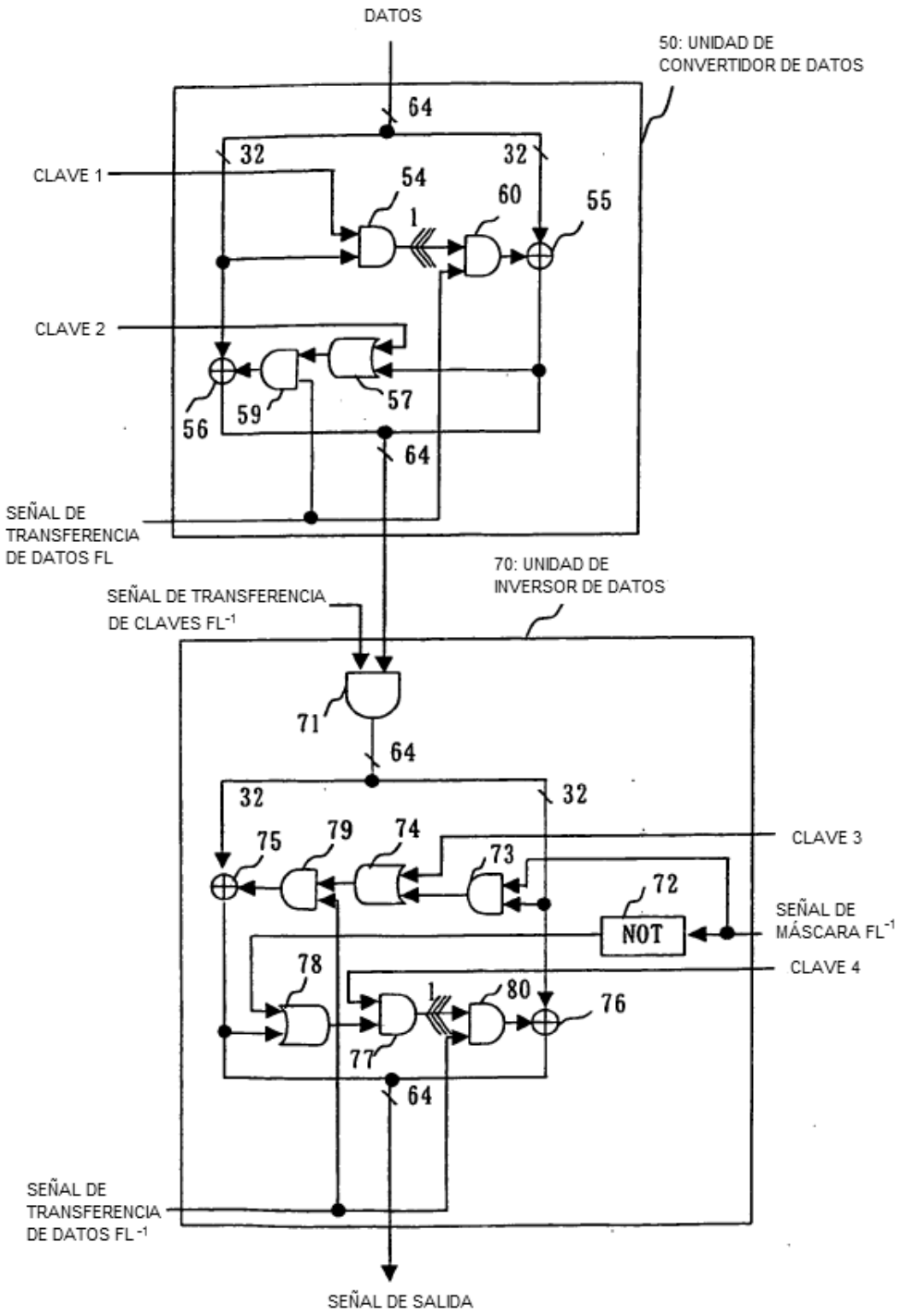

DATOS
50: UNIDAD DE CONVERTIDOR DE DATOS
64
32
32
CLAVE 1
54
60
55
1
CLAVE 2
57
56
59
64
SEÑAL DE TRANSFERENCIA DE DATOS FL
70: UNIDAD DE INVERSOR DE DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL-1
71
64
32
32
75
79
74
73
CLAVE 3
72
NOT
SEÑAL DE MÁSCARA FL-1
78
CLAVE 4
1
80
76
77
64
SEÑAL DE TRANSFERENCIA DE DATOS FL-1
SEÑAL DE SALIDA

Fig. 30

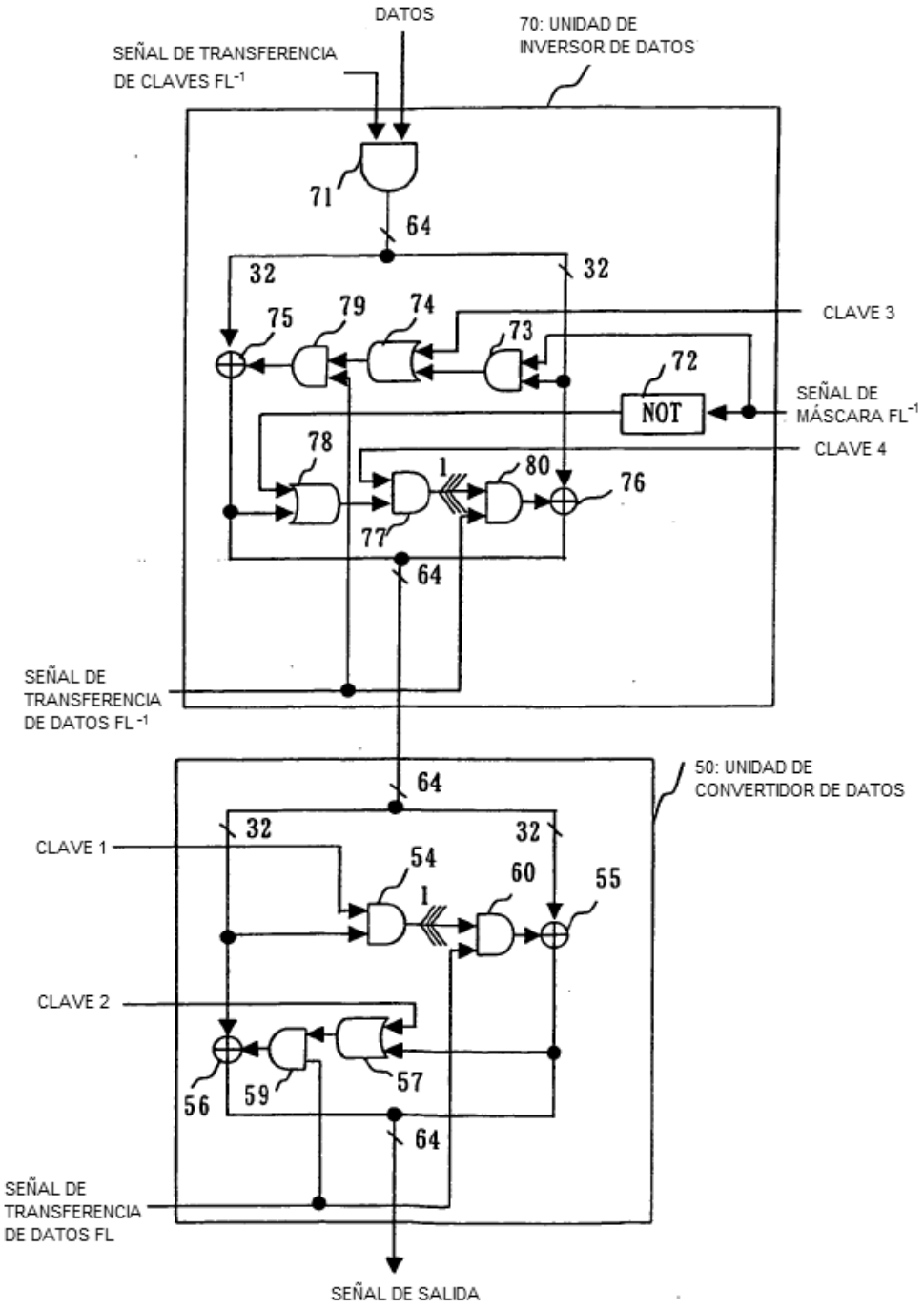

DATOS
70: UNIDAD DE INVERSOR DE DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL-1
71
64
32
32
75
79
74
73
CLAVE 3
72
NOT
SEÑAL DE MÁSCARA FL-1
78
1
80
76
CLAVE 4
77
64
SEÑAL DE TRANSFERENCIA DE DATOS FL-1
64
50: UNIDAD DE CONVERTIDOR DE DATOS
32
32
CLAVE 1
54
1
60
55
CLAVE 2
56
59
57
64
SEÑAL DE TRANSFERENCIA DE DATOS FL
SEÑAL DE SALIDA

Fig. 31

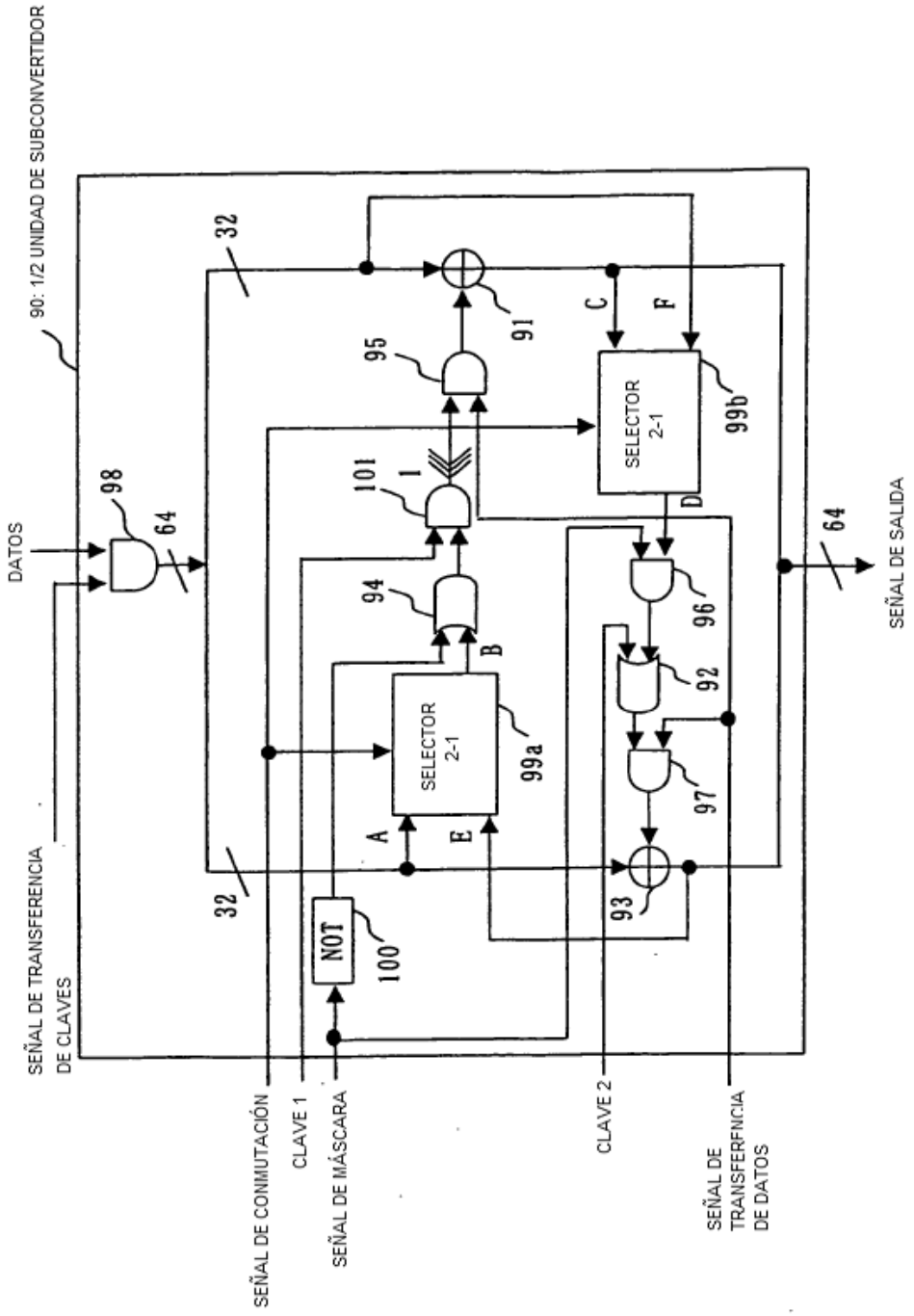

90: 1/2 UNIDAD DE SUBCONVERTIDOR
DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES
SEÑAL DE CONMUTACIÓN
CLAVE 1
SEÑAL DE MÁSCARA
CLAVE 2
SEÑAL DE TRANSFERNCIA DE DATOS
SEÑAL DE SALIDA
SELECTOR 2-1
SELECTOR 2-1
NOT
98
64
32
32
64
91
95
101
94
96
92
97
93
100
99a
99b
A
B
C
D
E
F
I

Fig. 32

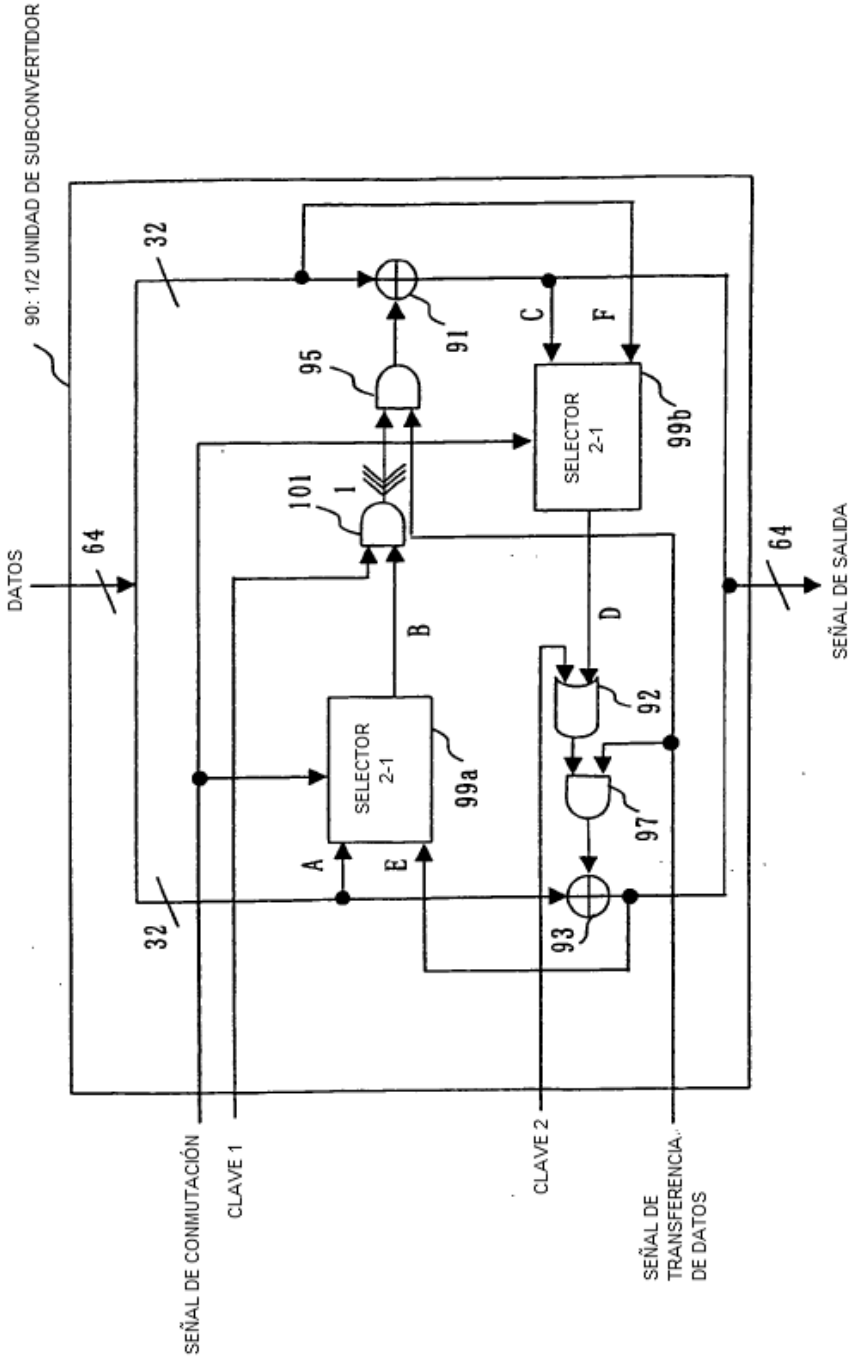

90: 1/2 UNIDAD DE SUBCONVERTIDOR
DATOS
64
32
32
64
SEÑAL DE SALIDA
91
95
101
SELECTOR 2-1
99b
SELECTOR 2-1
99a
92
97
93
A
B
C
D
E
F
SEÑAL DE CONMUTACIÓN
CLAVE 1
CLAVE 2
SEÑAL DE TRANSFERENCIA DE DATOS

Fig. 33

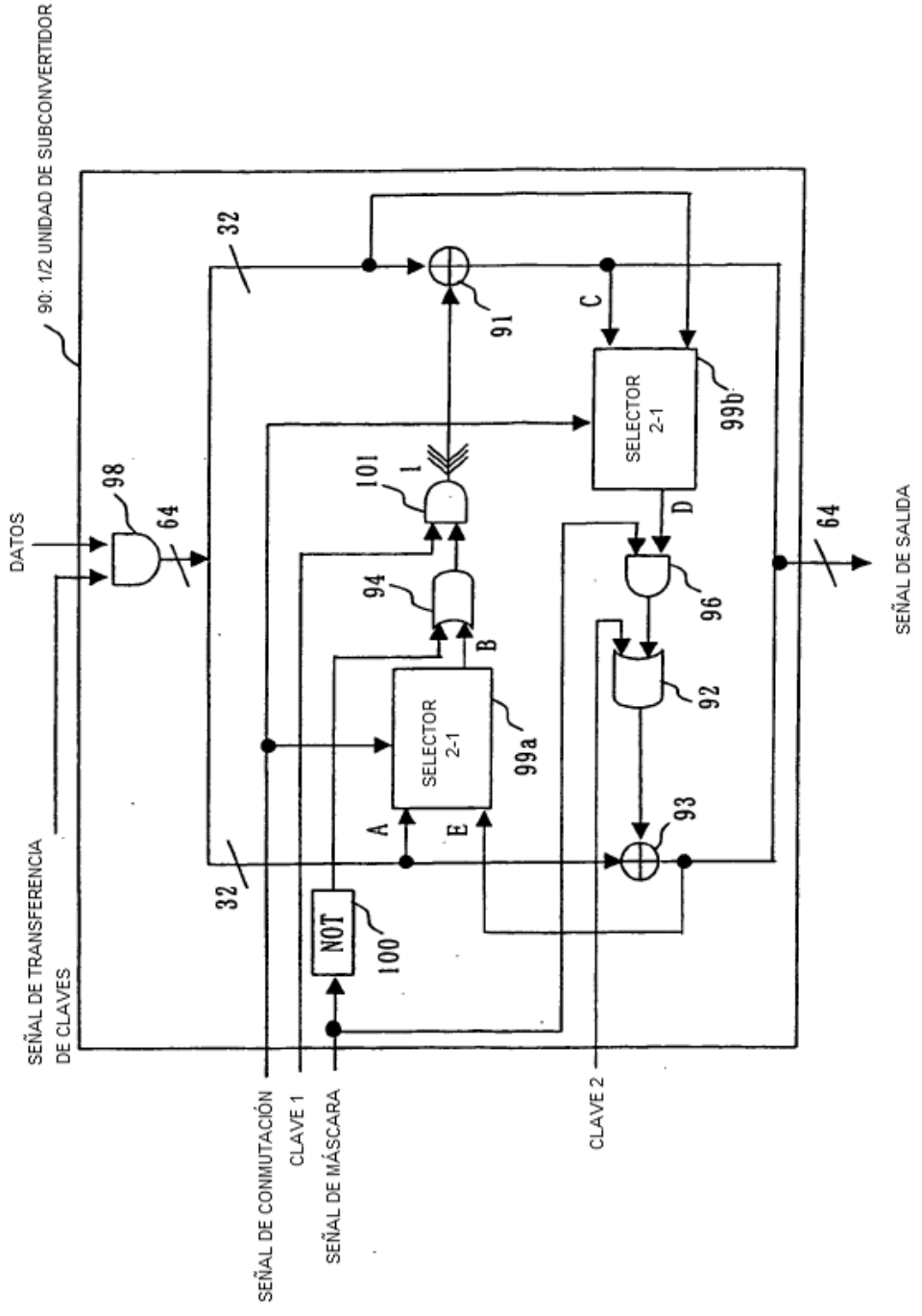

90: 1/2 UNIDAD DE SUBCONVERTIDOR
DATOS
98
64
32
91
C
SELECTOR 2-1
99b
101
1
94
B
SELECTOR 2-1
99a
A
E
96
92
93
64
SEÑAL DE SALIDA
D
32
NOT
100
SEÑAL DE TRANSFERENCIA DE CLAVES
SEÑAL DE CONMUTACIÓN
CLAVE 1
SEÑAL DE MÁSCARA
CLAVE 2

Fig. 34

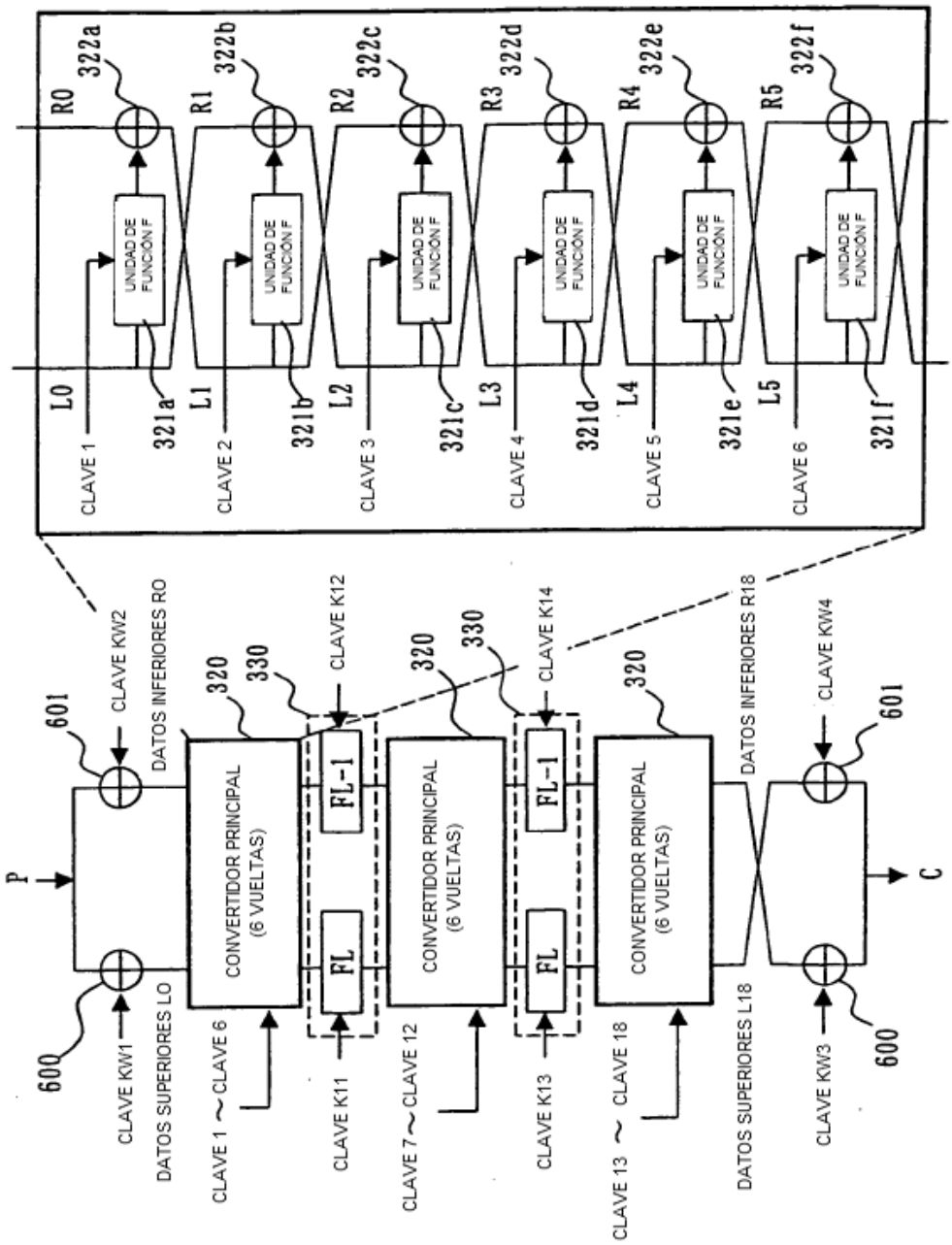

R0
322a
R1
322b
R2
322c
R3
322d
R4
322e
R5
322f
L0
L1
L2
L3
L4
L5
UNIDAD DE FUNCIÓN F
CLAVE 1
CLAVE 2
CLAVE 3
CLAVE 4
CLAVE 5
CLAVE 6
321a
321b
321c
321d
321e
321f
P
C
601
600
CLAVE KW2
CLAVE KW1
CLAVE KW4
CLAVE KW3
DATOS INFERIORES R0
DATOS SUPERIORES L0
DATOS INFERIORES R18
DATOS SUPERIORES L18
320
330
CONVERTIDOR PRINCIPAL (6 VUELTAS)
FL
FL-1
CLAVE K11
CLAVE K12
CLAVE K13
CLAVE K14
CLAVE 1 ~ CLAVE 6
CLAVE 7 ~ CLAVE 12
CLAVE 13 ~ CLAVE 18

Fig. 35

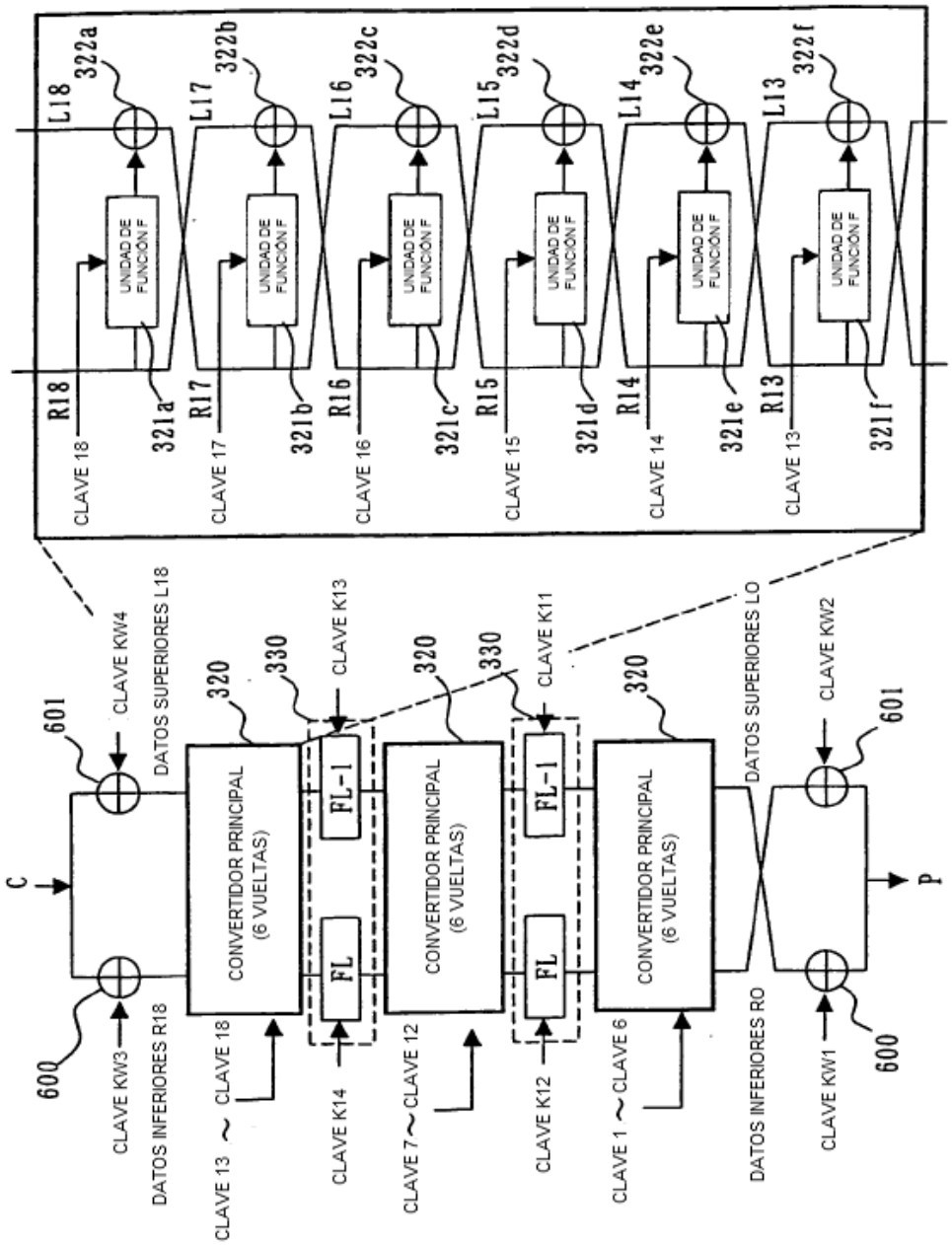

L18
322a
L17
322b
L16
322c
L15
322d
L14
322e
L13
322f
UNIDAD DE FUNCIÓN F
R18
R17
R16
R15
R14
R13
CLAVE 18
CLAVE 17
CLAVE 16
CLAVE 15
CLAVE 14
CLAVE 13
321a
321b
321c
321d
321e
321f
C
601
CLAVE KW4
DATOS SUPERIORES L18
320
330
CLAVE K13
CLAVE K11
CONVERTIDOR PRINCIPAL (6 VUELTAS)
FL-1
FL
DATOS SUPERIORES LO
CLAVE KW2
P
600
CLAVE KW3
DATOS INFERIORES R18
CLAVE 13 ~ CLAVE 18
CLAVE K14
CLAVE 7 ~ CLAVE 12
CLAVE K12
CLAVE 1 ~ CLAVE 6
DATOS INFERIORES RO
CLAVE KW1

Fig. 36

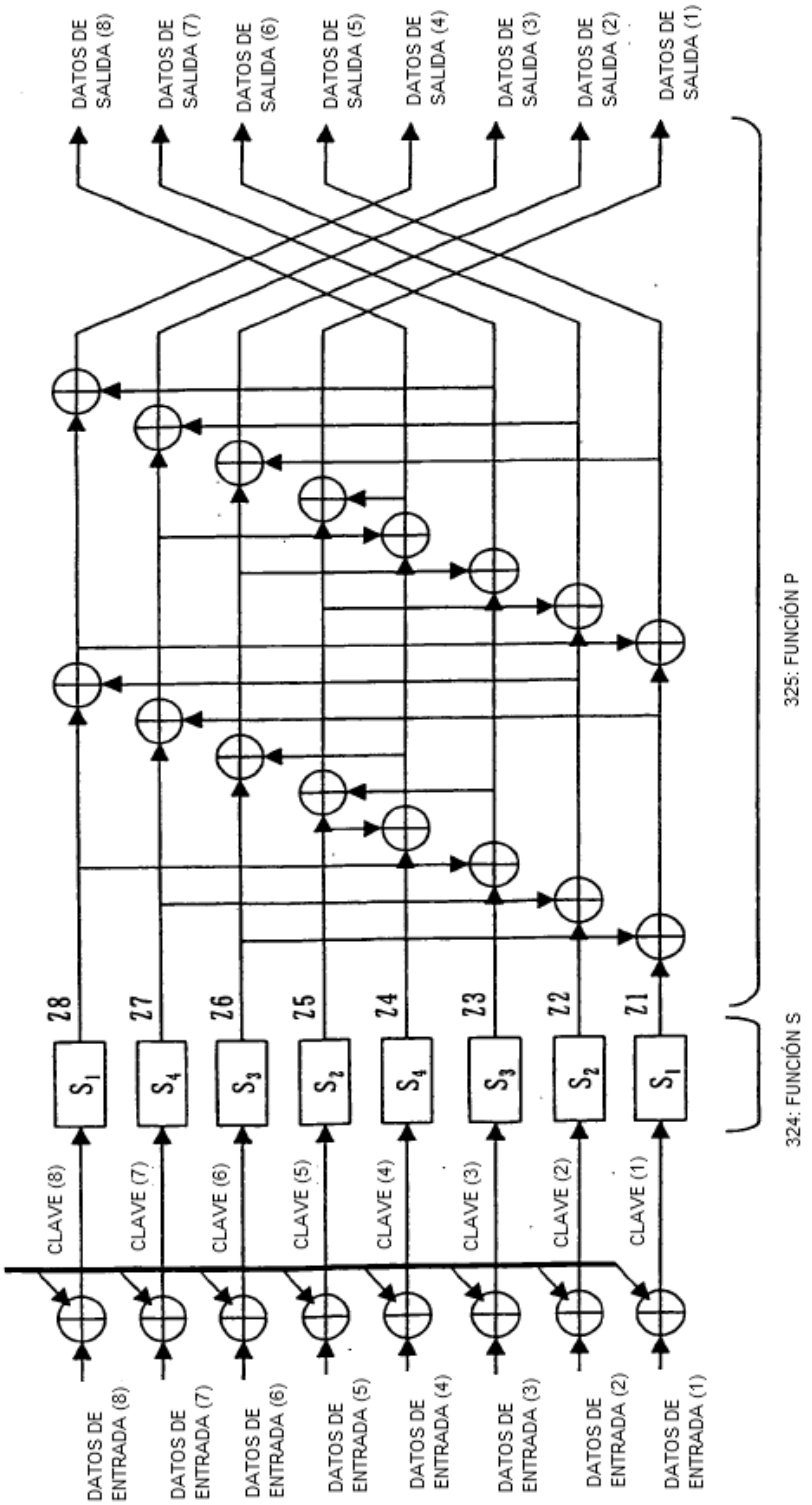

DATOS DE SALIDA (8)
DATOS DE SALIDA (7)
DATOS DE SALIDA (6)
DATOS DE SALIDA (5)
DATOS DE SALIDA (4)
DATOS DE SALIDA (3)
DATOS DE SALIDA (2)
DATOS DE SALIDA (1)
325: FUNCIÓN P
324: FUNCIÓN S
Z8
Z7
Z6
Z5
Z4
Z3
Z2
Z1
S1
S4
S3
S2
S4
S3
S2
S1
CLAVE (8)
CLAVE (7)
CLAVE (6)
CLAVE (5)
CLAVE (4)
CLAVE (3)
CLAVE (2)
CLAVE (1)
DATOS DE ENTRADA (8)
DATOS DE ENTRADA (7)
DATOS DE ENTRADA (6)
DATOS DE ENTRADA (5)
DATOS DE ENTRADA (4)
DATOS DE ENTRADA (3)
DATOS DE ENTRADA (2)
DATOS DE ENTRADA (1)

Fig. 37

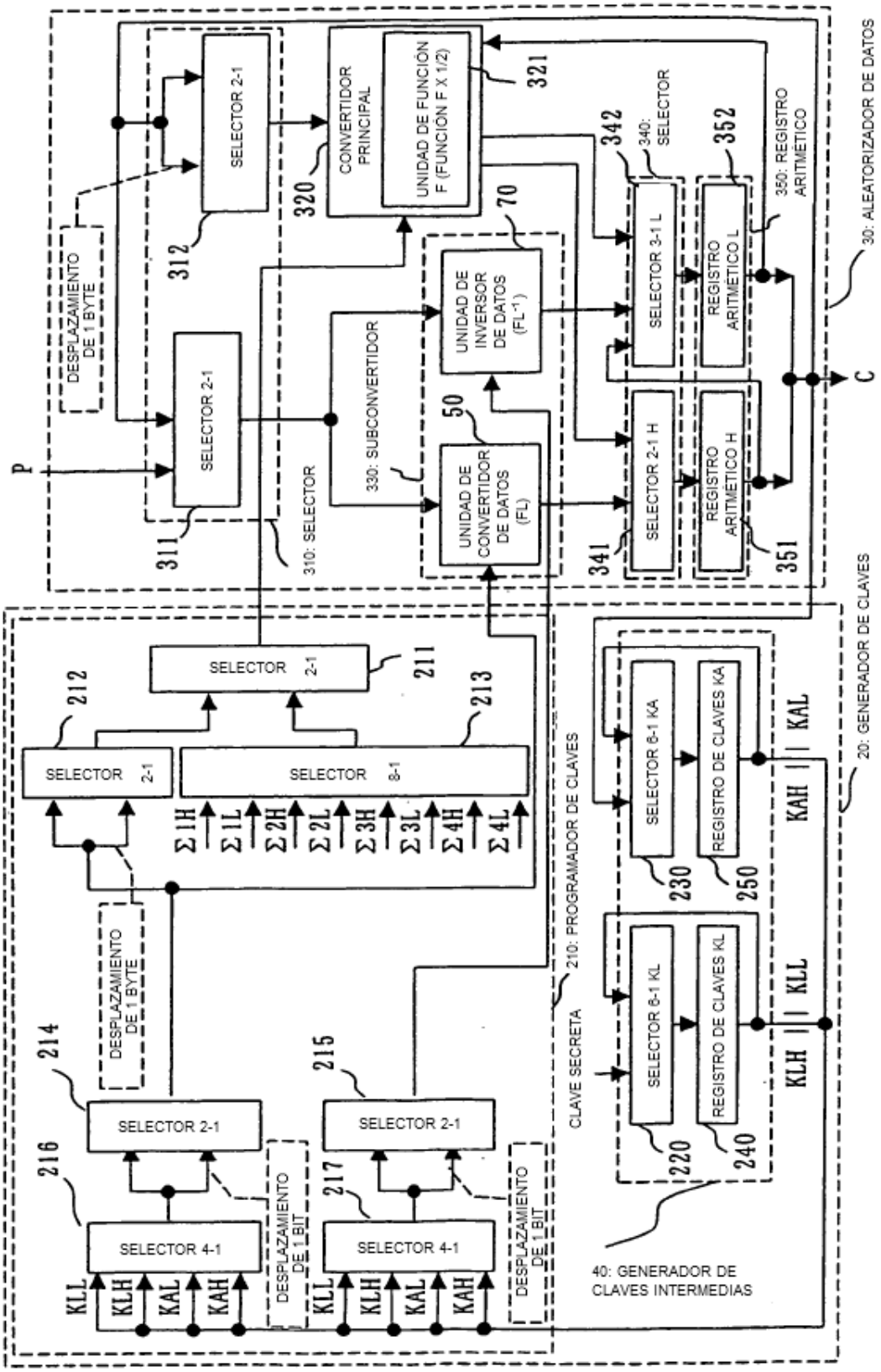

P
C
DESPLAZAMIENTO DE 1 BYTE
SELECTOR 2-1
312
320
CONVERTIDOR PRINCIPAL
UNIDAD DE FUNCIÓN F (FUNCIÓN F X 1/2)
321
342
340: SELECTOR
352
350: REGISTRO ARITMÉTICO
30: ALEATORIZADOR DE DATOS
70
UNIDAD DE INVERSOR DE DATOS (FL-1)
SELECTOR 3-1 L
REGISTRO ARITMÉTICO L
311
310: SELECTOR
330: SUBCONVERTIDOR
50
UNIDAD DE CONVERTIDOR DE DATOS (FL)
SELECTOR 2-1 H
REGISTRO ARITMÉTICO H
341
351
SELECTOR 2-1
211
212
213
SELECTOR 8-1
Σ1H Σ1L Σ2H Σ2L Σ3H Σ3L Σ4H Σ4L
DESPLAZAMIENTO DE 1 BYTE
214
215
SELECTOR 2-1
SELECTOR 2-1
216
217
SELECTOR 4-1
SELECTOR 4-1
DESPLAZAMIENTO DE 1 BIT
DESPLAZAMIENTO DE 1 BIT
KLL KLH KAL KAH
KLL KLH KAL KAH
CLAVE SECRETA
210: PROGRAMADOR DE CLAVES
SELECTOR 8-1 KA
REGISTRO DE CLAVES KA
230
250
SELECTOR 6-1 KL
REGISTRO DE CLAVES KL
220
240
KAL
KAH
KLL
KLH
20: GENERADOR DE CLAVES
40: GENERADOR DE CLAVES INTERMEDIAS

Fig. 38

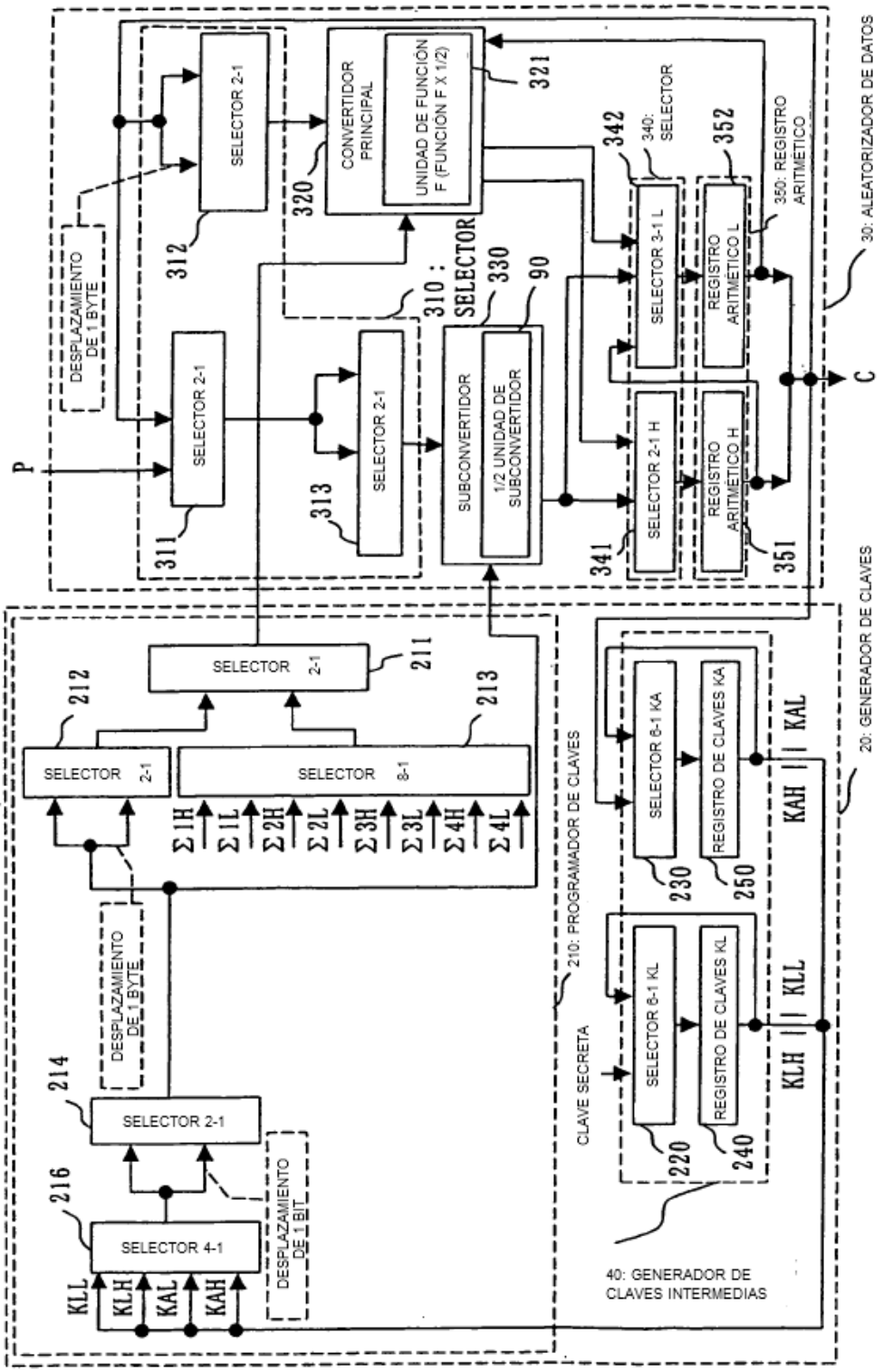

P
C
DESPLAZAMIENTO DE 1 BYTE
SELECTOR 2-1
CONVERTIDOR PRINCIPAL
UNIDAD DE FUNCIÓN F (FUNCIÓN F X 1/2)
310 : SELECTOR
SUBCONVERTIDOR
1/2 UNIDAD DE SUBCONVERTIDOR
SELECTOR 3-1 L
SELECTOR 2-1 H
REGISTRO ARITMÉTICO L
REGISTRO ARITMÉTICO H
340: SELECTOR
350: REGISTRO ARITMÉTICO
30: ALEATORIZADOR DE DATOS
20: GENERADOR DE CLAVES
210: PROGRAMADOR DE CLAVES
CLAVE SECRETA
SELECTOR 8-1
SELECTOR 4-1
DESPLAZAMIENTO DE 1 BIT
SELECTOR 6-1 KA
SELECTOR 6-1 KL
REGISTRO DE CLAVES KA
REGISTRO DE CLAVES KL
40: GENERADOR DE CLAVES INTERMEDIAS
KLL
KLH
KAL
KAH
Σ1H
Σ1L
Σ2H
Σ2L
Σ3H
Σ3L
Σ4H
Σ4L

Fig. 39

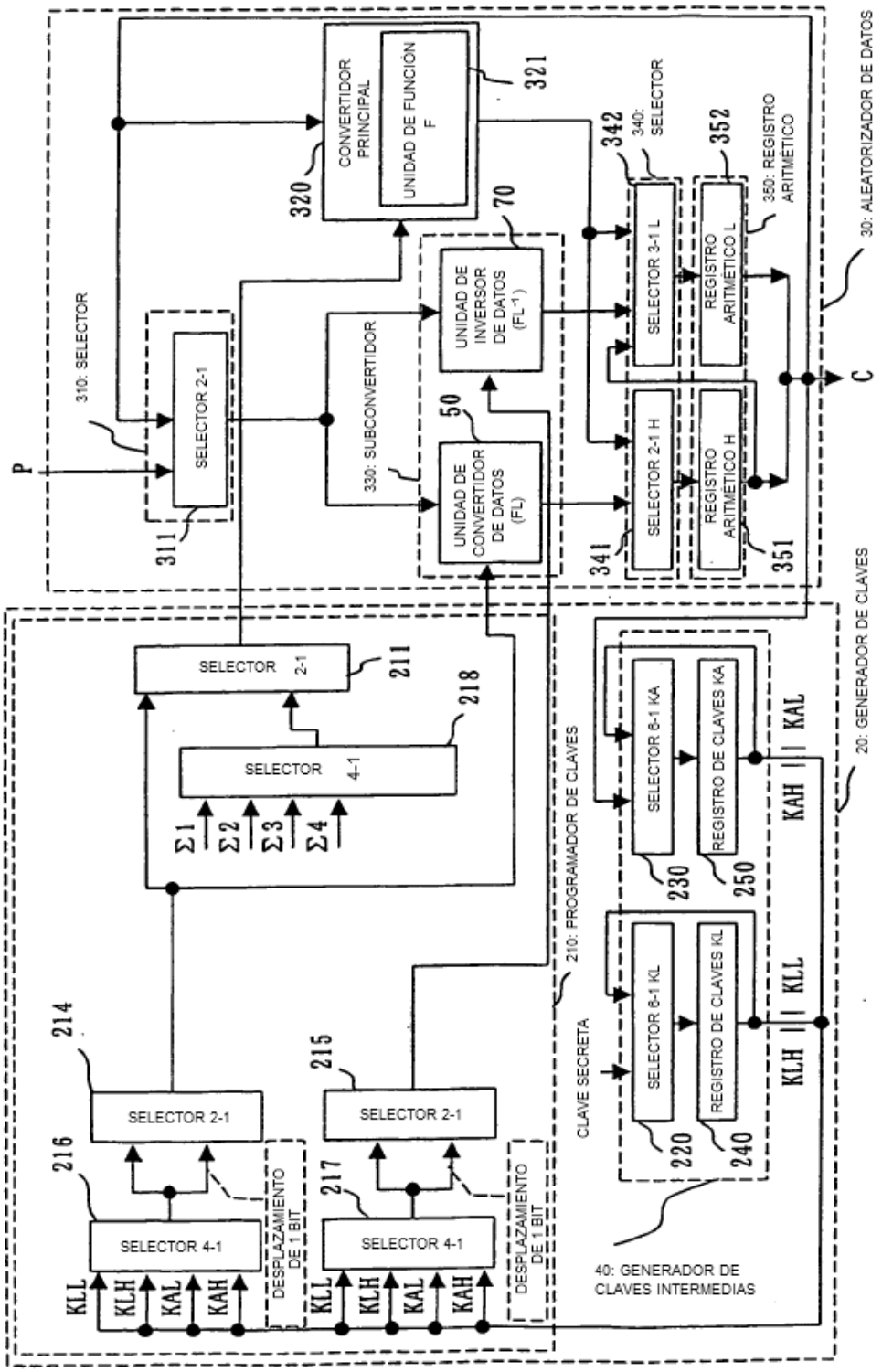

P
310: SELECTOR
SELECTOR 2-1
311
330: SUBCONVERTIDOR
320
CONVERTIDOR PRINCIPAL
UNIDAD DE FUNCION F
321
UNIDAD DE CONVERTIDOR DE DATOS (FL)
50
UNIDAD DE INVERSOR DE DATOS (FL-1)
70
340: SELECTOR
341
342
SELECTOR 2-1 H
SELECTOR 3-1 L
REGISTRO ARITMÉTICO H
REGISTRO ARITMÉTICO L
351
352
350: REGISTRO ARITMÉTICO
C
30: ALEATORIZADOR DE DATOS
20: GENERADOR DE CLAVES
210: PROGRAMADOR DE CLAVES
CLAVE SECRETA
SELECTOR 2-1
211
SELECTOR 4-1
218
Σ1
Σ2
Σ3
Σ4
214
215
SELECTOR 2-1
SELECTOR 2-1
216
217
SELECTOR 4-1
SELECTOR 4-1
DESPLAZAMIENTO DE 1 BIT
DESPLAZAMIENTO DE 1 BIT
KLL
KLH
KAL
KAH
SELECTOR 8-1 KA
SELECTOR 8-1 KL
REGISTRO DE CLAVES KA
REGISTRO DE CLAVES KL
230
220
250
240
KAL
KAH
KLL
KLH
40: GENERADOR DE CLAVES INTERMEDIAS

Fig. 40

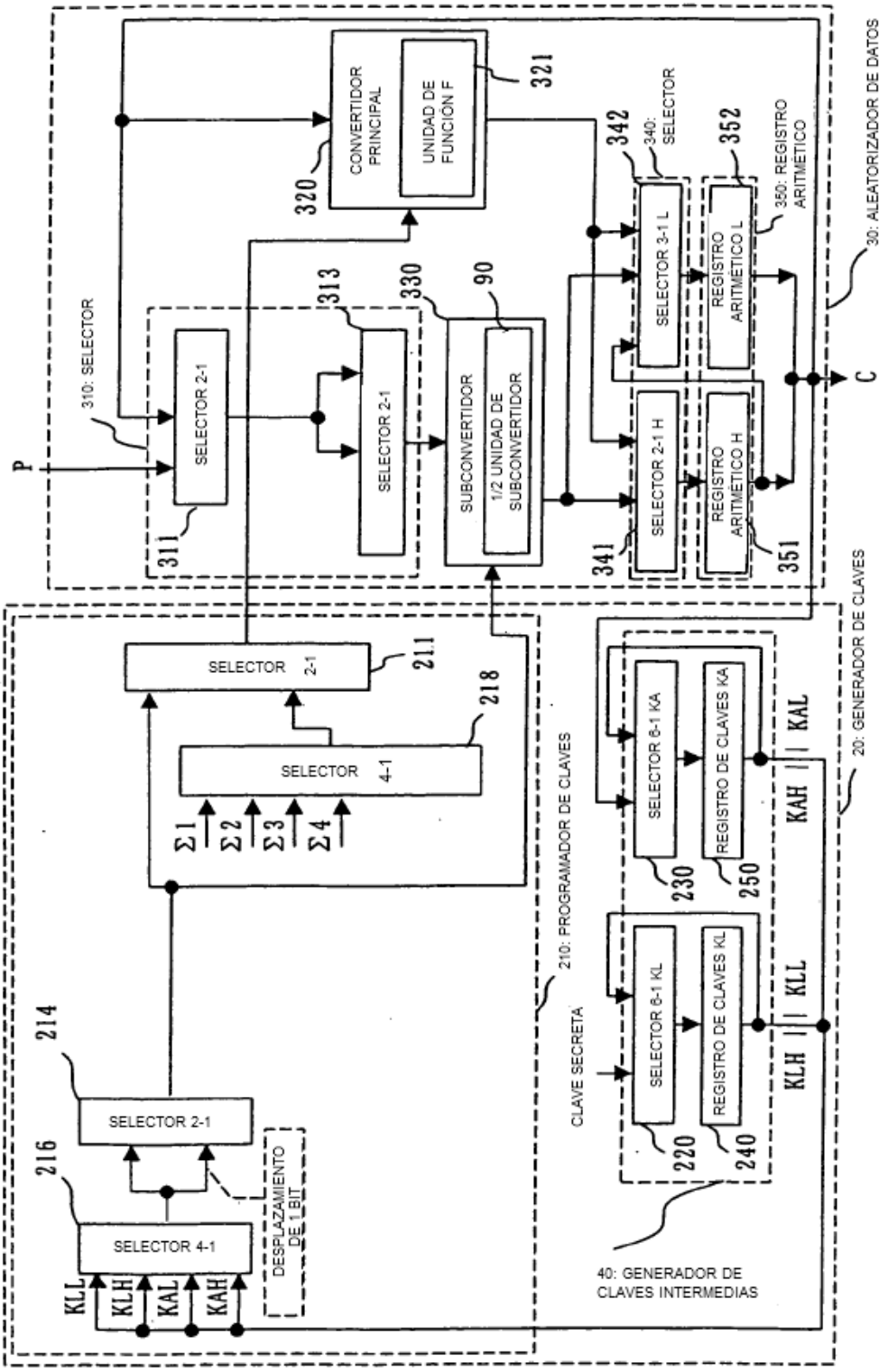

P
C
310: SELECTOR
SELECTOR 2-1
311
313
SELECTOR 2-1
330
90
SUBCONVERTIDOR
1/2 UNIDAD DE SUBCONVERTIDOR
320
CONVERTIDOR PRINCIPAL
UNIDAD DE FUNCION F
321
342
340: SELECTOR
SELECTOR 3-1 L
352
350: REGISTRO ARITMÉTICO
REGISTRO ARITMÉTICO L
30: ALEATORIZADOR DE DATOS
341
SELECTOR 2-1 H
REGISTRO ARITMÉTICO H
351
SELECTOR 2-1
211
SELECTOR 4-1
218
Σ1
Σ2
Σ3
Σ4
214
SELECTOR 2-1
216
SELECTOR 4-1
DESPLAZAMIENTO DE 1 BIT
KLL
KLH
KAL
KAH
210: PROGRAMADOR DE CLAVES
CLAVE SECRETA
SELECTOR 6-1 KA
REGISTRO DE CLAVES KA
230
250
KAH || KAL
SELECTOR 6-1 KL
REGISTRO DE CLAVES KL
220
240
KLH || KLL
20: GENERADOR DE CLAVES
40: GENERADOR DE CLAVES INTERMEDIAS

Fig. 41

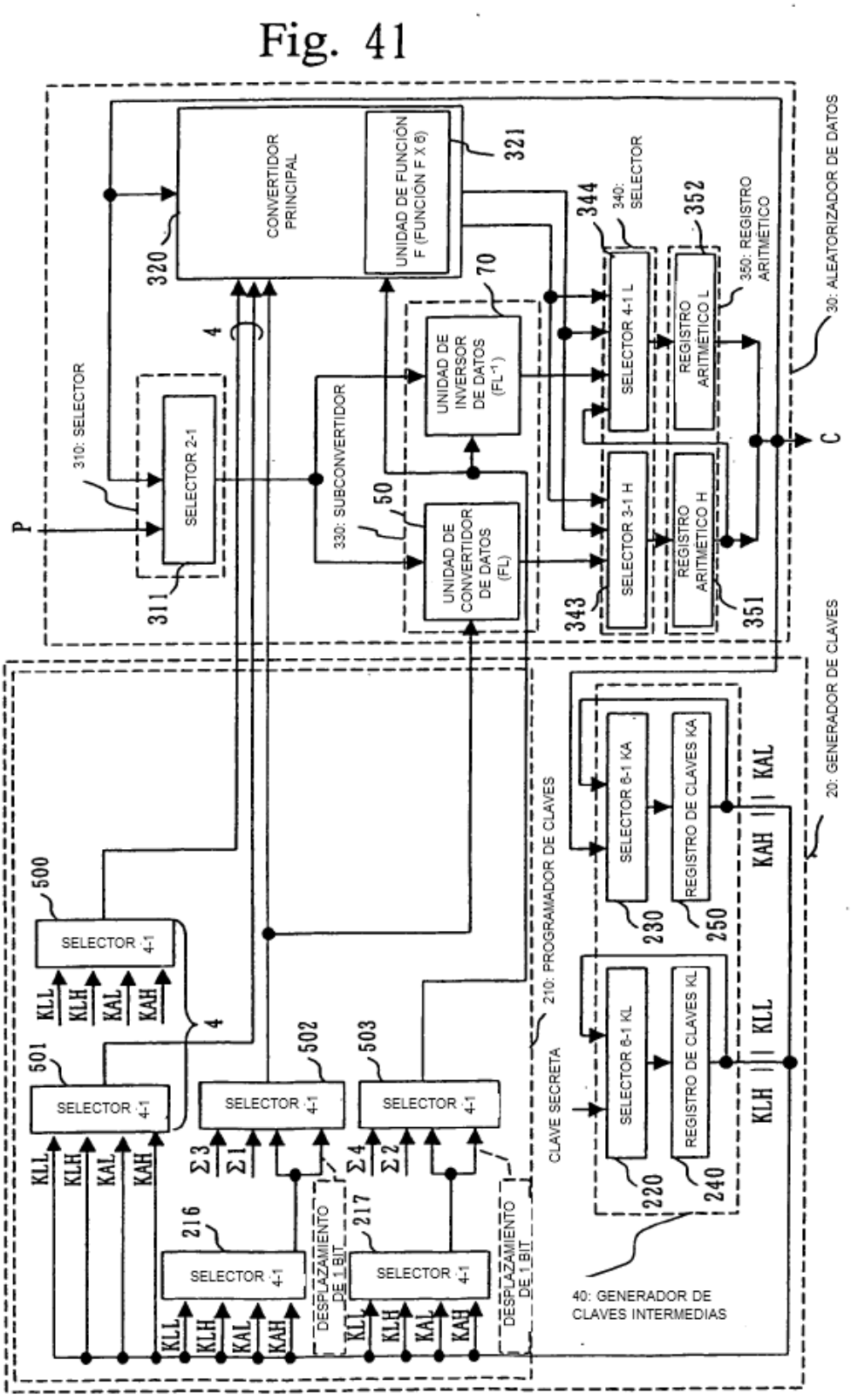

30: ALEATORIZADOR DE DATOS
20: GENERADOR DE CLAVES
310: SELECTOR
SELECTOR 2-1
311
320
CONVERTIDOR PRINCIPAL
UNIDAD DE FUNCION F (FUNCION F X 6)
321
330: SUBCONVERTIDOR
50
UNIDAD DE CONVERTIDOR DE DATOS (FL)
70
UNIDAD DE INVERSOR DE DATOS (FL-1)
340: SELECTOR
344
SELECTOR 4-1 L
SELECTOR 3-1 H
343
350: REGISTRO ARITMETICO
352
REGISTRO ARITMETICO L
REGISTRO ARITMETICO H
351
P
C
4
210: PROGRAMADOR DE CLAVES
CLAVE SECRETA
SELECTOR 4-1
500
501
502
503
KLL
KLH
KAL
KAH
Σ3
Σ1
Σ4
Σ2
216
217
DESPLAZAMIENTO DE 1 BIT
SELECTOR 6-1 KA
REGISTRO DE CLAVES KA
230
250
SELECTOR 6-1 KL
REGISTRO DE CLAVES KL
220
240
40: GENERADOR DE CLAVES INTERMEDIAS

Fig. 42

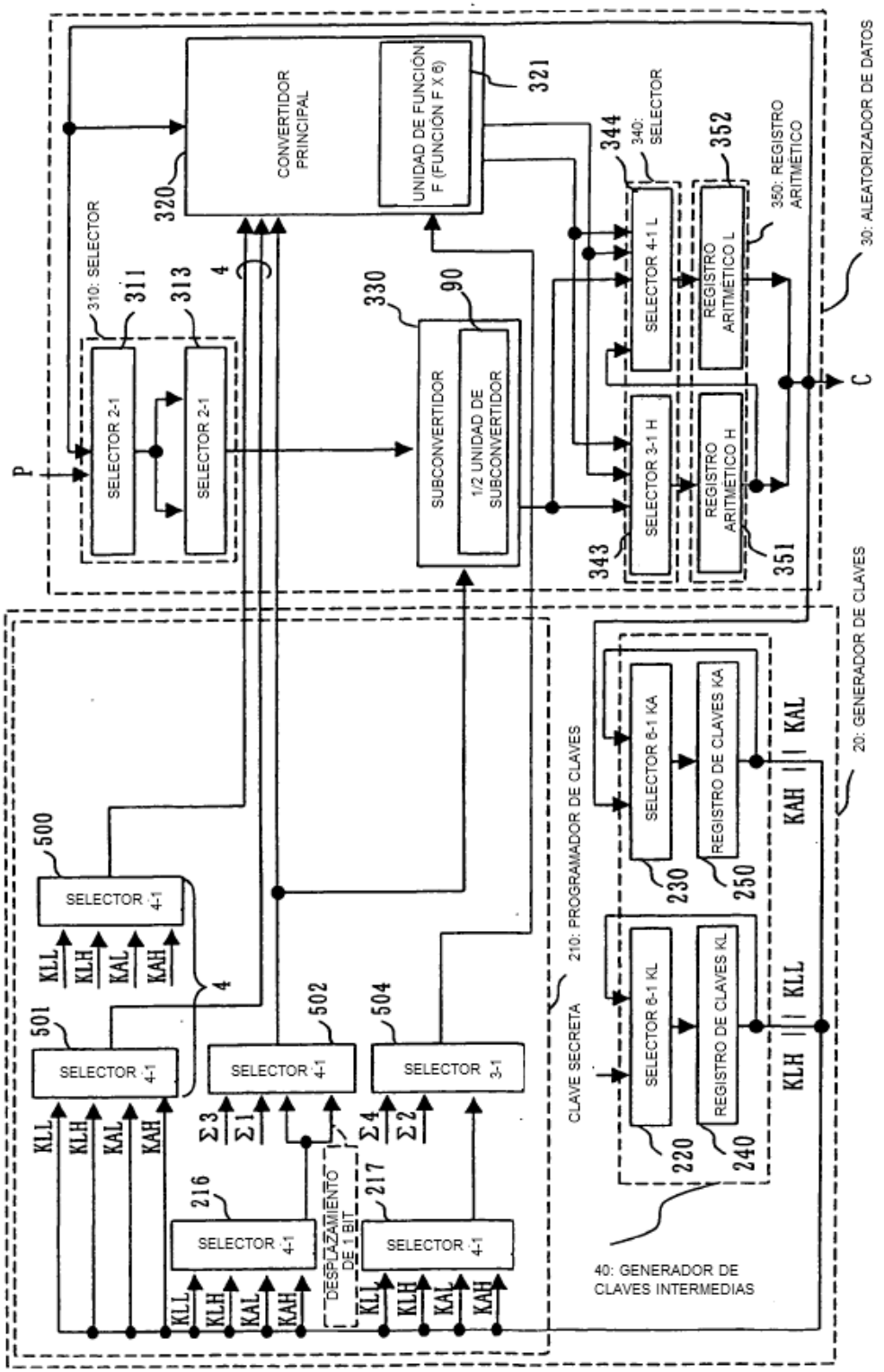

P
C
CONVERTIDOR PRINCIPAL
320
UNIDAD DE FUNCIÓN F (FUNCIÓN F X 6)
321
SUBCONVERTIDOR
330
1/2 UNIDAD DE SUBCONVERTIDOR
90
310: SELECTOR
311
313
4
SELECTOR 2-1
SELECTOR 2-1
340: SELECTOR
344
SELECTOR 4-1 L
SELECTOR 3-1 H
343
350: REGISTRO ARITMÉTICO
352
REGISTRO ARITMÉTICO L
REGISTRO ARITMÉTICO H
351
30: ALEATORIZADOR DE DATOS
20: GENERADOR DE CLAVES
210: PROGRAMADOR DE CLAVES
CLAVE SECRETA
SELECTOR 6-1 KA
REGISTRO DE CLAVES KA
230
250
KAH
KAL
SELECTOR 6-1 KL
REGISTRO DE CLAVES KL
220
240
KLH
KLL
40: GENERADOR DE CLAVES INTERMEDIAS
500
SELECTOR 4-1
KLL
KLH
KAL
KAH
501
SELECTOR 4-1
502
SELECTOR 4-1
504
SELECTOR 3-1
Σ3
Σ1
Σ4
Σ2
DESPLAZAMIENTO DE 1 BIT
216
217
SELECTOR 4-1
SELECTOR 4-1

Fig. 43

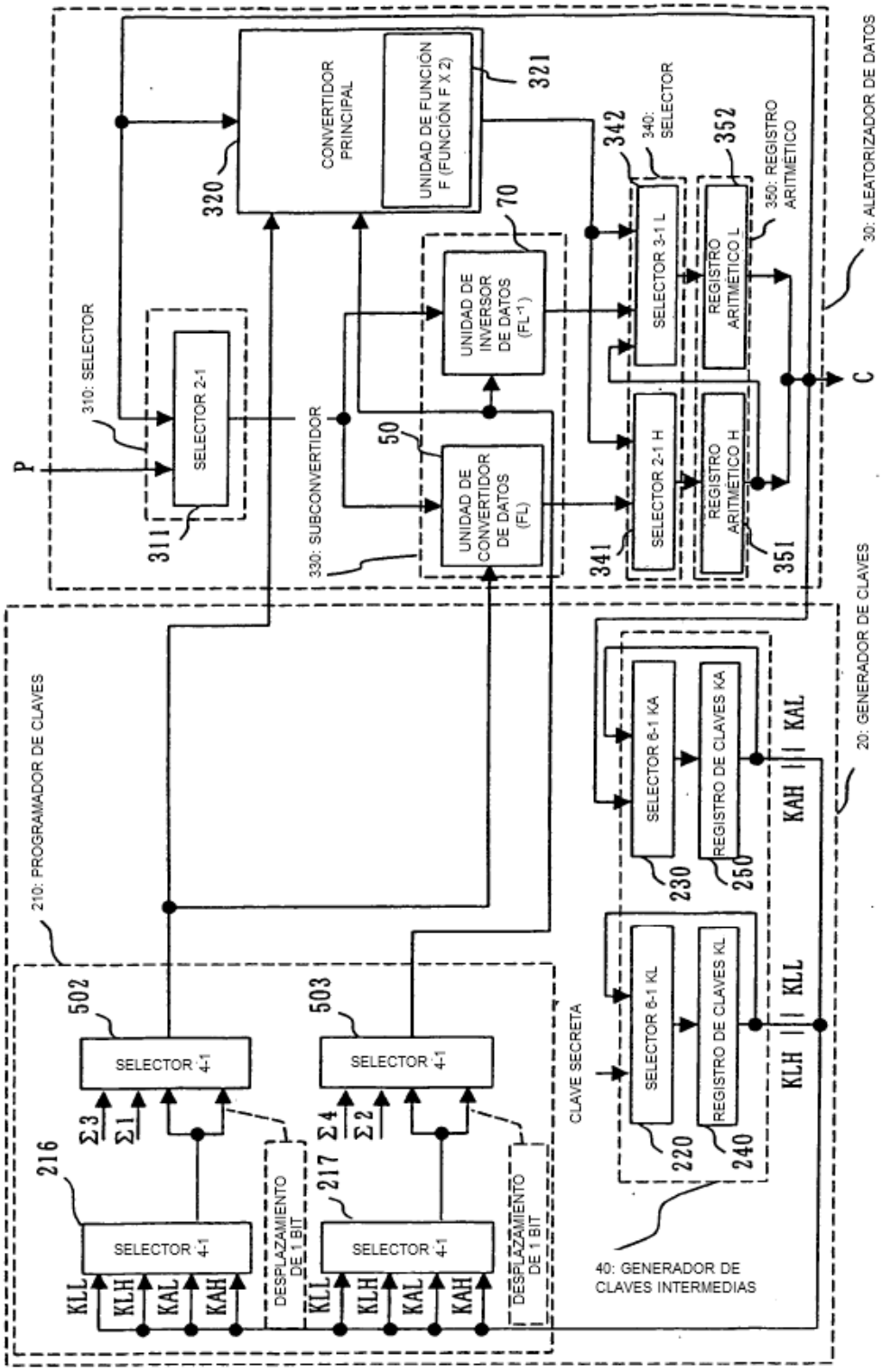

P
C
310: SELECTOR
SELECTOR 2-1
311
330: SUBCONVERTIDOR
50
CONVERTIDOR PRINCIPAL
320
UNIDAD DE FUNCIÓN F (FUNCIÓN F X 2)
321
UNIDAD DE INVERSOR DE DATOS (FL-1)
70
UNIDAD DE CONVERTIDOR DE DATOS (FL)
340: SELECTOR
342
SELECTOR 3-1 L
SELECTOR 2-1 H
341
350: REGISTRO ARITMÉTICO
352
REGISTRO ARITMÉTICO L
REGISTRO ARITMÉTICO H
351
30: ALEATORIZADOR DE DATOS
20: GENERADOR DE CLAVES
210: PROGRAMADOR DE CLAVES
502
503
SELECTOR 4-1
Σ3
Σ1
Σ4
Σ2
216
217
DESPLAZAMIENTO DE 1 BIT
KLL
KLH
KAL
KAH
CLAVE SECRETA
SELECTOR 8-1 KA
REGISTRO DE CLAVES KA
230
250
SELECTOR 8-1 KL
REGISTRO DE CLAVES KL
220
240
40: GENERADOR DE CLAVES INTERMEDIAS

Fig. 44

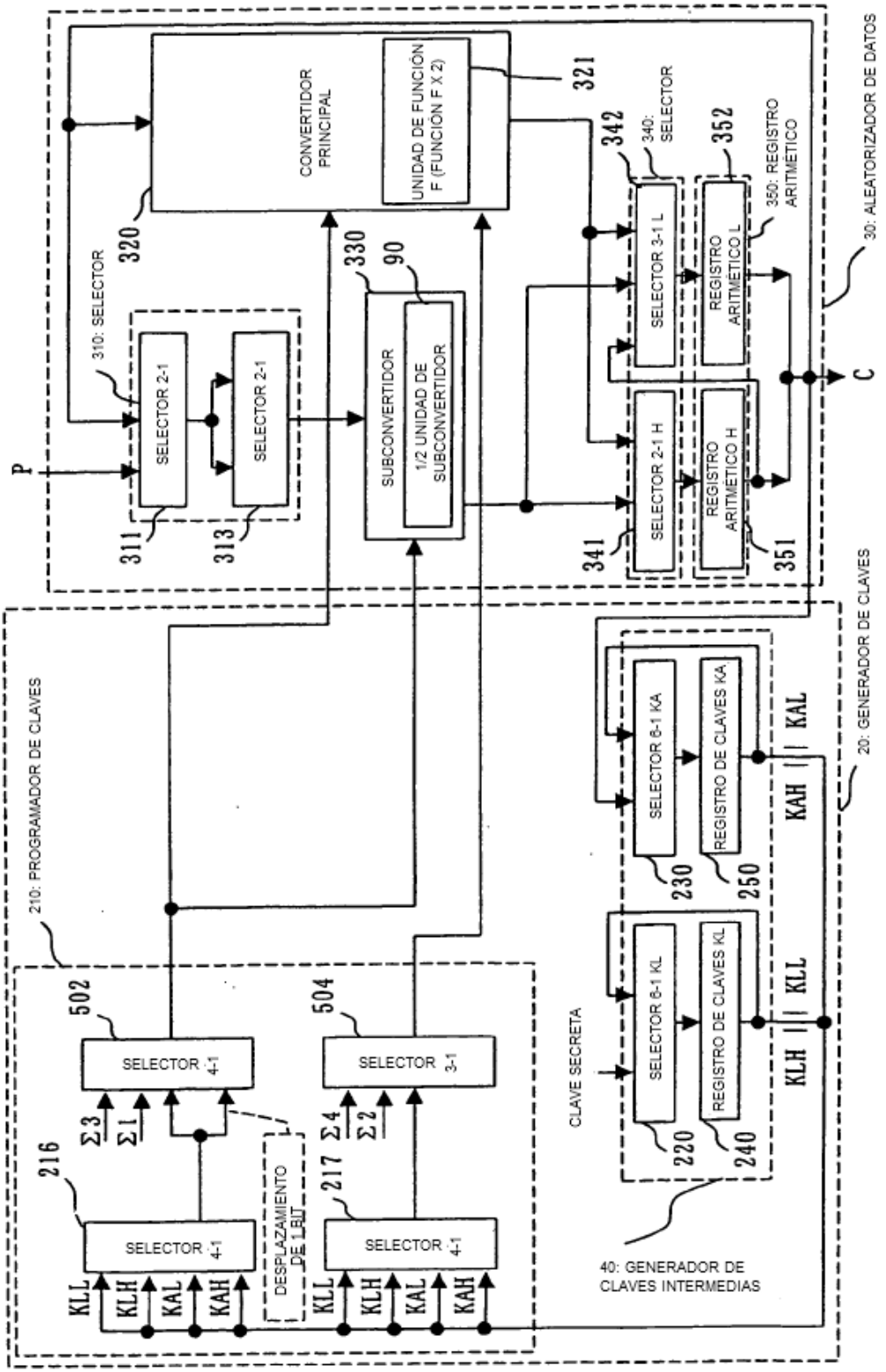

P
C
310: SELECTOR
SELECTOR 2-1
SELECTOR 2-1
311
313
320
CONVERTIDOR PRINCIPAL
UNIDAD DE FUNCIÓN F (FUNCIÓN F X 2)
321
330
90
SUBCONVERTIDOR
1/2 UNIDAD DE SUBCONVERTIDOR
340: SELECTOR
342
SELECTOR 3-1 L
SELECTOR 2-1 H
341
350: REGISTRO ARITMÉTICO
352
REGISTRO ARITMÉTICO L
REGISTRO ARITMÉTICO H
351
30: ALEATORIZADOR DE DATOS
20: GENERADOR DE CLAVES
210: PROGRAMADOR DE CLAVES
502
SELECTOR 4-1
Σ3
Σ1
216
SELECTOR 4-1
DESPLAZAMIENTO DE 1 BIT
504
SELECTOR 3-1
217
Σ4
Σ2
SELECTOR 4-1
KLL
KLH
KAL
KAH
CLAVE SECRETA
SELECTOR 6-1 KA
REGISTRO DE CLAVES KA
230
250
SELECTOR 6-1 KL
REGISTRO DE CLAVES KL
220
240
KAL
KAH
KLL
KLH
40: GENERADOR DE CLAVES INTERMEDIAS

Fig. 45

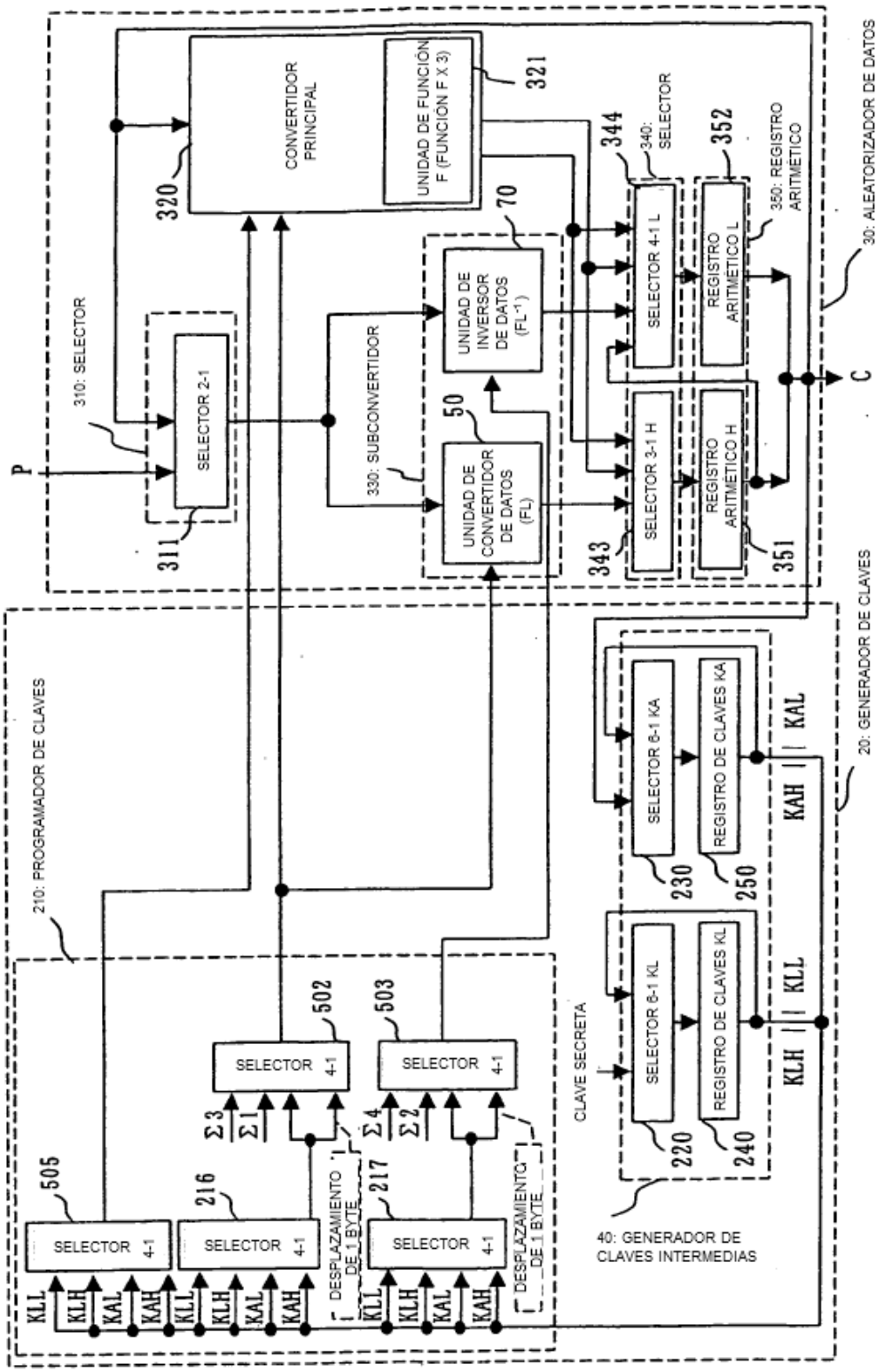

P
310: SELECTOR
SELECTOR 2-1
311
320
CONVERTIDOR PRINCIPAL
UNIDAD DE FUNCIÓN F (FUNCIÓN F X 3)
321
330: SUBCONVERTIDOR
50
UNIDAD DE CONVERTIDOR DE DATOS (FL)
70
UNIDAD DE INVERSOR DE DATOS (FL-1)
343
SELECTOR 3-1 H
344
340: SELECTOR
SELECTOR 4-1 L
REGISTRO ARITMÉTICO H
351
REGISTRO ARITMÉTICO L
352
350: REGISTRO ARITMÉTICO
30: ALEATORIZADOR DE DATOS
C
20: GENERADOR DE CLAVES
210: PROGRAMADOR DE CLAVES
SELECTOR 4-1
505
216
217
502
503
Σ3
Σ1
Σ4
Σ2
DESPLAZAMIENTO DE 1 BYTE
KLL
KLH
KAL
KAH
CLAVE SECRETA
SELECTOR 8-1 KA
REGISTRO DE CLAVES KA
230
250
SELECTOR 8-1 KL
REGISTRO DE CLAVES KL
220
240
40: GENERADOR DE CLAVES INTERMEDIAS

Fig. 46

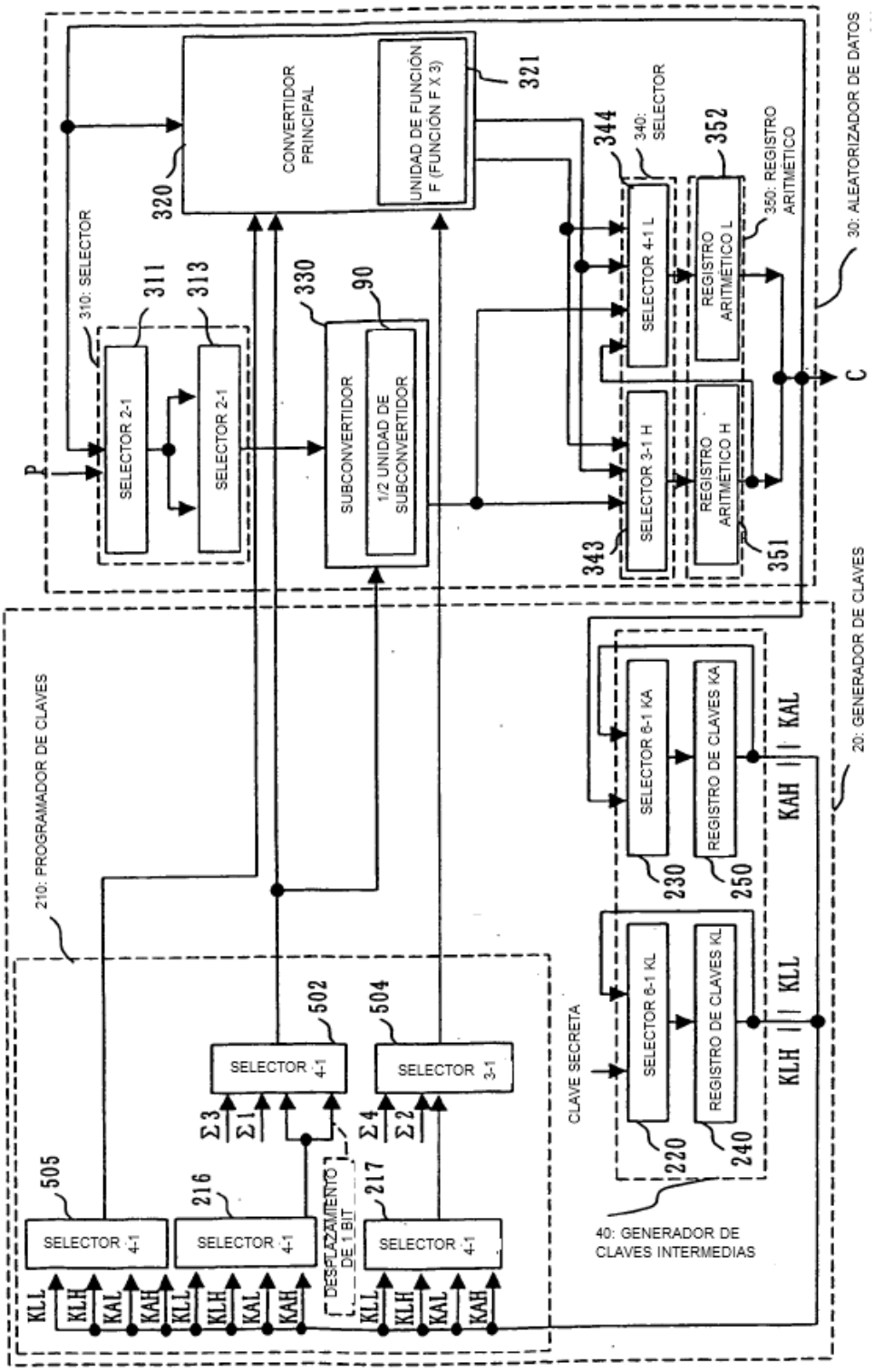

30: ALEATORIZADOR DE DATOS
20: GENERADOR DE CLAVES
310: SELECTOR
311
313
SELECTOR 2-1
SELECTOR 2-1
320
CONVERTIDOR PRINCIPAL
321
UNIDAD DE FUNCIÓN F (FUNCIÓN F X 3)
330
90
SUBCONVERTIDOR
1/2 UNIDAD DE SUBCONVERTIDOR
340: SELECTOR
344
SELECTOR 4-1 L
SELECTOR 3-1 H
343
350: REGISTRO ARITMÉTICO
352
REGISTRO ARITMÉTICO L
REGISTRO ARITMÉTICO H
351
P
C
210: PROGRAMADOR DE CLAVES
CLAVE SECRETA
SELECTOR 8-1 KA
SELECTOR 8-1 KL
230
220
REGISTRO DE CLAVES KA
REGISTRO DE CLAVES KL
250
240
KAH
KAL
KLH
KLL
40: GENERADOR DE CLAVES INTERMEDIAS
SELECTOR 4-1
SELECTOR 3-1
502
504
Σ3
Σ1
Σ4
Σ2
505
216
217
DESPLAZAMIENTO DE 1 BIT
KLL
KLH
KAL
KAH

Fig. 47

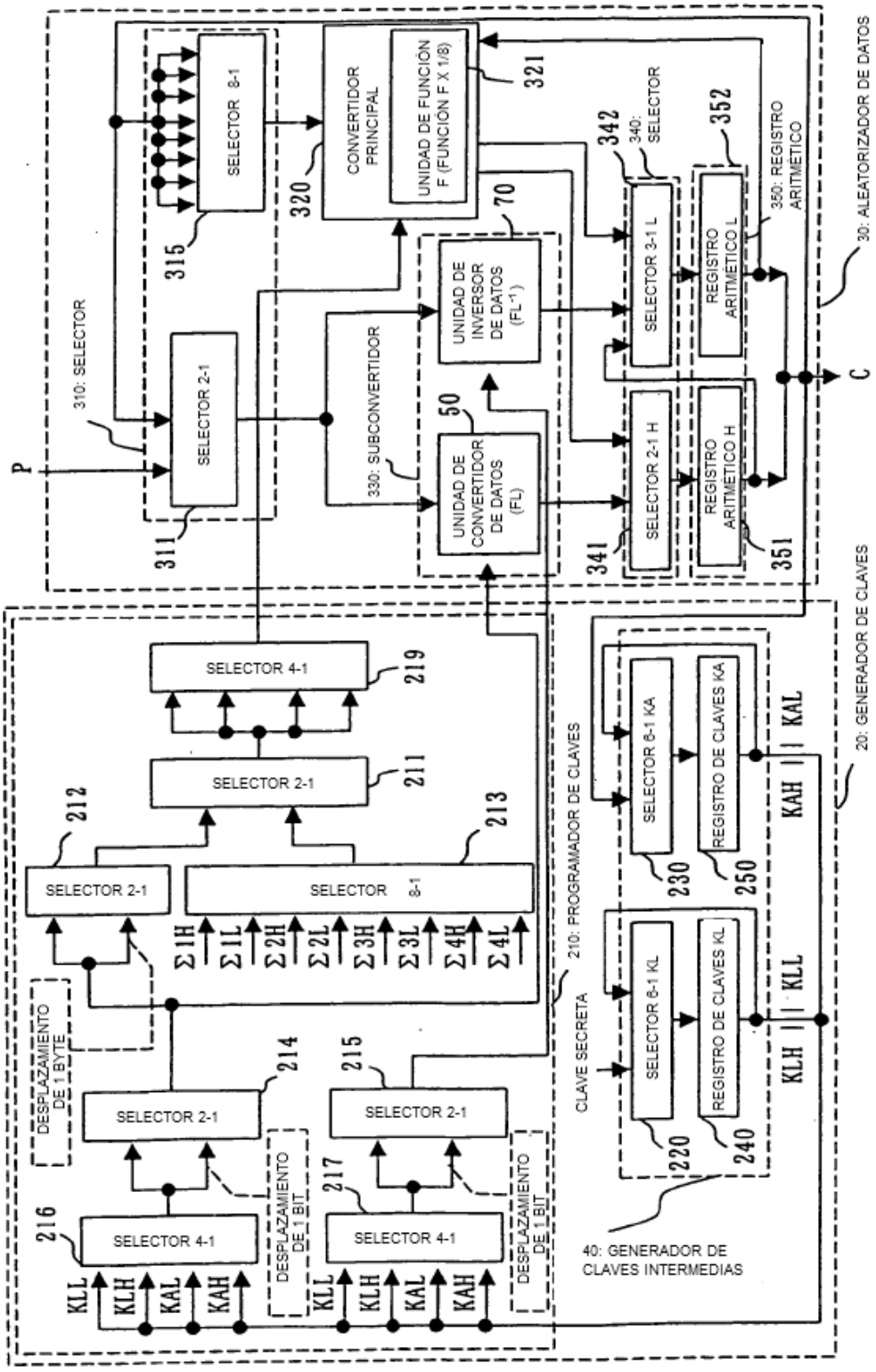

P
310: SELECTOR
SELECTOR 2-1
311
315
SELECTOR 8-1
320
CONVERTIDOR PRINCIPAL
321
UNIDAD DE FUNCIÓN F (FUNCIÓN F X 1/8)
330: SUBCONVERTIDOR
50
UNIDAD DE CONVERTIDOR DE DATOS (FL)
70
UNIDAD DE INVERSOR DE DATOS (FL-1)
340: SELECTOR
341
SELECTOR 2-1 H
342
SELECTOR 3-1 L
350: REGISTRO ARITMÉTICO
351
REGISTRO ARITMÉTICO H
352
REGISTRO ARITMÉTICO L
30: ALEATORIZADOR DE DATOS
C
20: GENERADOR DE CLAVES
210: PROGRAMADOR DE CLAVES
SELECTOR 4-1
219
SELECTOR 2-1
211
212
213
SELECTOR 2-1
SELECTOR 8-1
Σ1H
Σ1L
Σ2H
Σ2L
Σ3H
Σ3L
Σ4H
Σ4L
DESPLAZAMIENTO DE 1 BYTE
214
215
SELECTOR 2-1
SELECTOR 2-1
DESPLAZAMIENTO DE 1 BIT
DESPLAZAMIENTO DE 1 BIT
216
217
SELECTOR 4-1
SELECTOR 4-1
KLL
KLH
KAL
KAH
KLL
KLH
KAL
KAH
CLAVE SECRETA
SELECTOR 8-1 KA
230
REGISTRO DE CLAVES KA
250
KAH
KAL
SELECTOR 8-1 KL
220
REGISTRO DE CLAVES KL
240
KLH
KLL
40: GENERADOR DE CLAVES INTERMEDIAS

Fig. 48

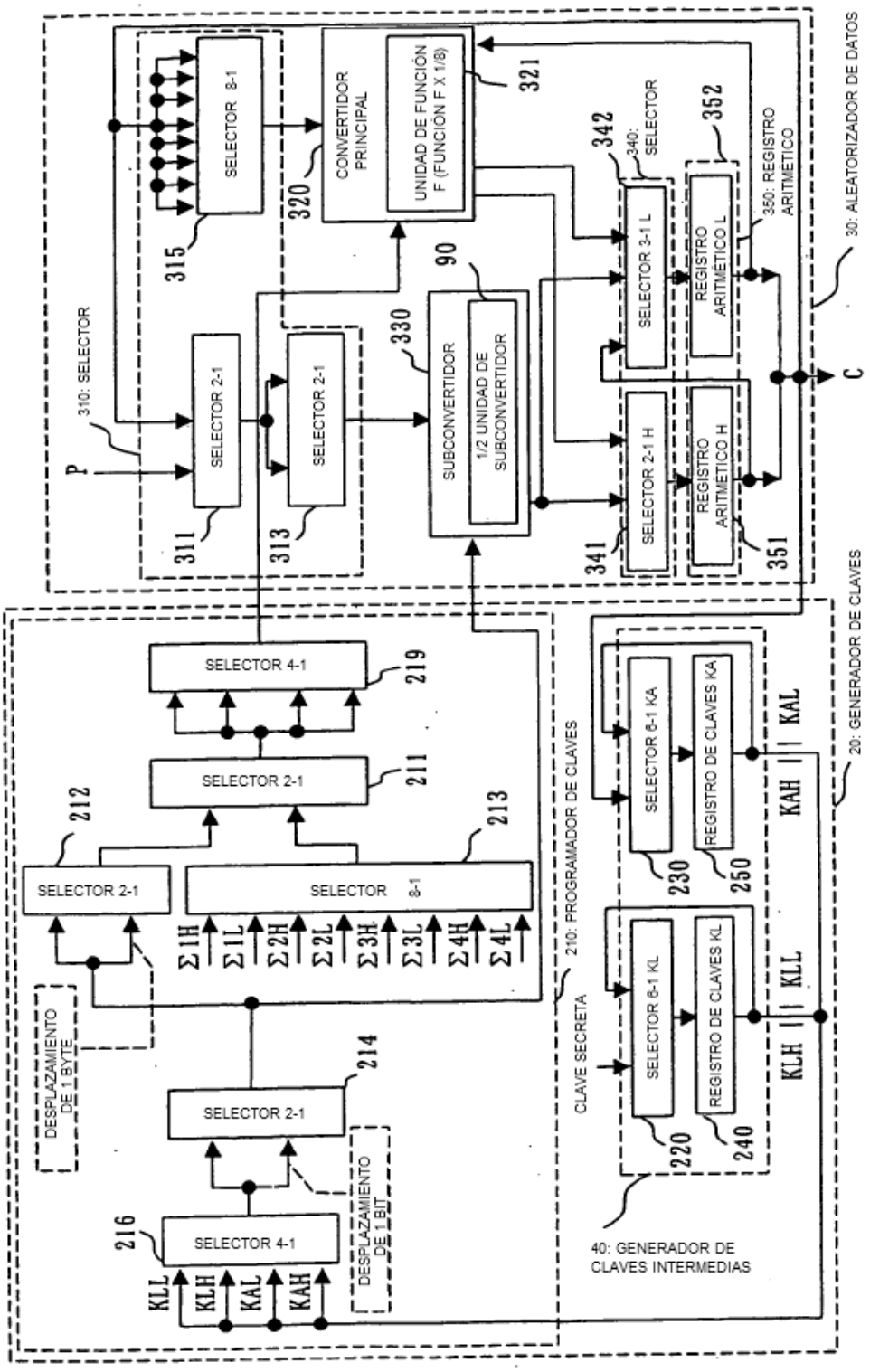

30: ALEATORIZADOR DE DATOS
20: GENERADOR DE CLAVES
210: PROGRAMADOR DE CLAVES
CLAVE SECRETA
40: GENERADOR DE CLAVES INTERMEDIAS
310: SELECTOR
SELECTOR 8-1
CONVERTIDOR PRINCIPAL
UNIDAD DE FUNCIÓN F (FUNCIÓN F X 1/8)
SELECTOR 2-1
SUBCONVERTIDOR
1/2 UNIDAD DE SUBCONVERTIDOR
SELECTOR 3-1 L
SELECTOR 2-1 H
REGISTRO ARITMÉTICO L
REGISTRO ARITMÉTICO H
350: REGISTRO ARITMÉTICO
SELECTOR 4-1
SELECTOR 6-1 KA
SELECTOR 6-1 KL
REGISTRO DE CLAVES KA
REGISTRO DE CLAVES KL
DESPLAZAMIENTO DE 1 BYTE
DESPLAZAMIENTO DE 1 BIT
Σ1H
Σ1L
Σ2H
Σ2L
Σ3H
Σ3L
Σ4H
Σ4L
KLL
KLH
KAL
KAH

Fig. 49

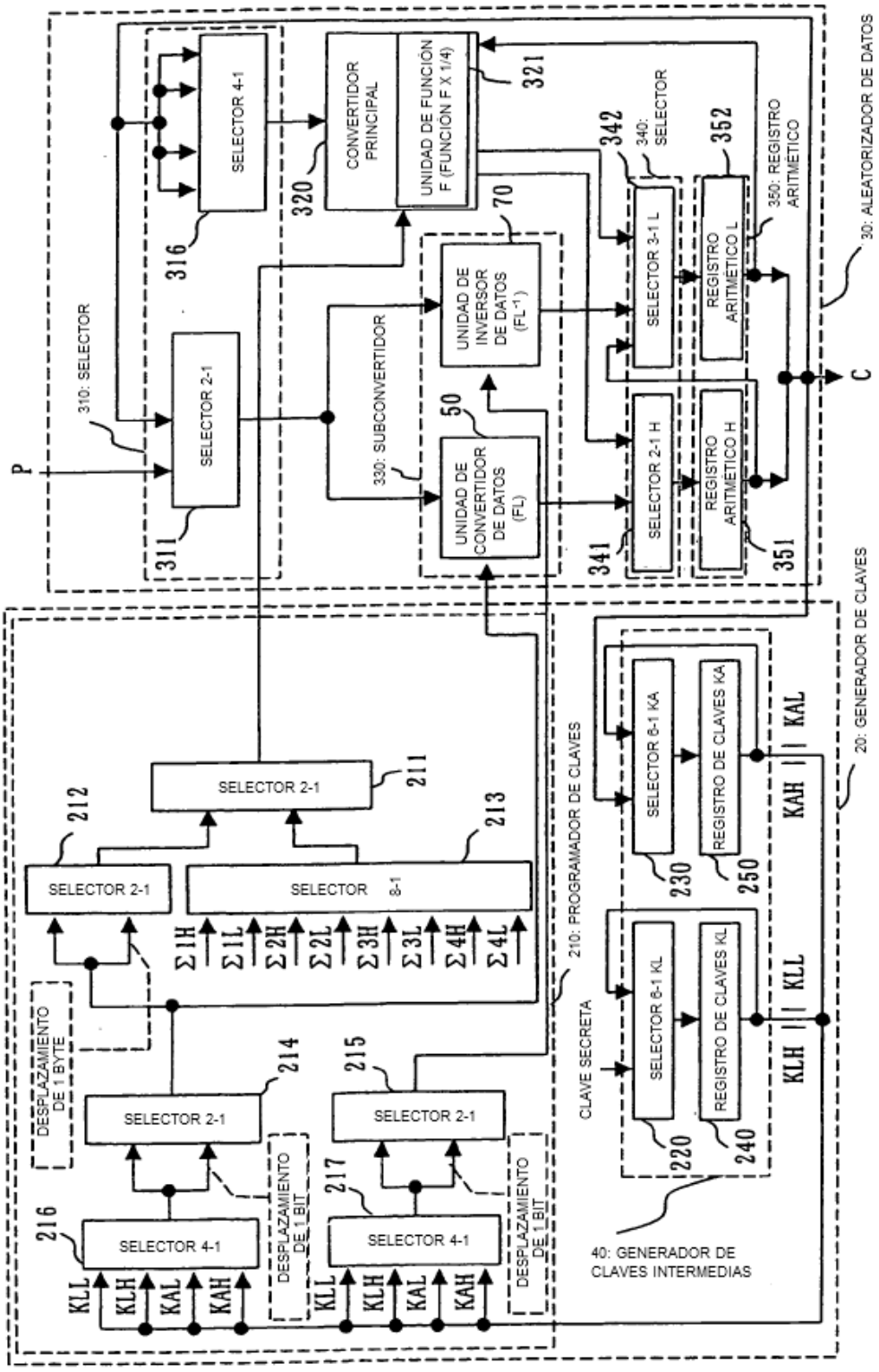

P
C
310: SELECTOR
SELECTOR 4-1
SELECTOR 2-1
316
311
320
CONVERTIDOR PRINCIPAL
UNIDAD DE FUNCIÓN F (FUNCIÓN F X 1/4)
321
330: SUBCONVERTIDOR
UNIDAD DE INVERSOR DE DATOS (FL-1)
70
UNIDAD DE CONVERTIDOR DE DATOS (FL)
50
340: SELECTOR
342
SELECTOR 3-1 L
SELECTOR 2-1 H
341
REGISTRO ARITMÉTICO L
REGISTRO ARITMÉTICO H
350: REGISTRO ARITMÉTICO
352
351
30: ALEATORIZADOR DE DATOS
20: GENERADOR DE CLAVES
210: PROGRAMADOR DE CLAVES
CLAVE SECRETA
SELECTOR 2-1
211
212
213
SELECTOR 8-1
Σ1H
Σ1L
Σ2H
Σ2L
Σ3H
Σ3L
Σ4H
Σ4L
DESPLAZAMIENTO DE 1 BYTE
214
215
DESPLAZAMIENTO DE 1 BIT
217
216
KLL
KLH
KAL
KAH
SELECTOR 6-1 KA
REGISTRO DE CLAVES KA
230
250
SELECTOR 6-1 KL
REGISTRO DE CLAVES KL
220
240
40: GENERADOR DE CLAVES INTERMEDIAS

Fig. 50

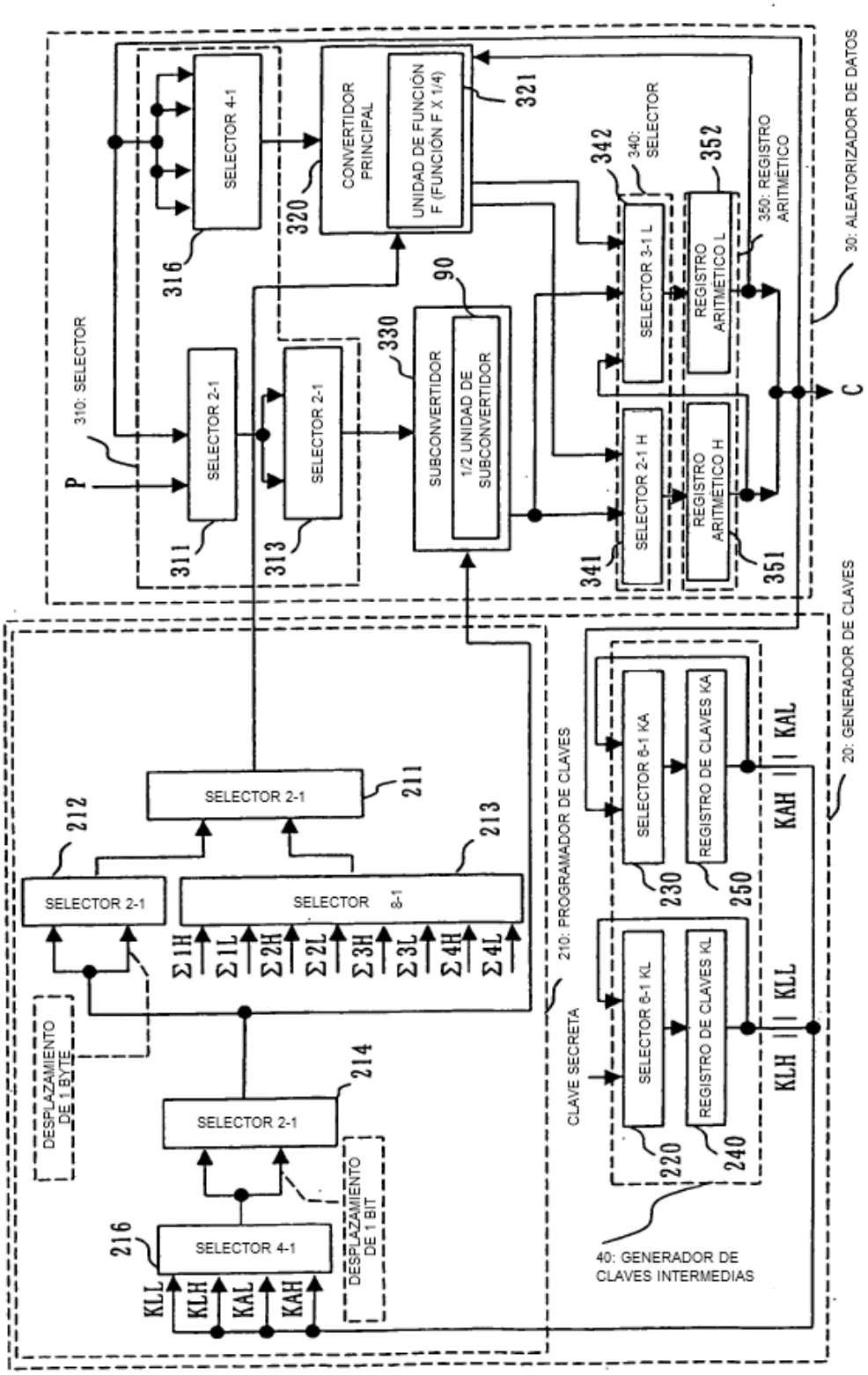

P
310: SELECTOR
SELECTOR 4-1
316
CONVERTIDOR PRINCIPAL
UNIDAD DE FUNCION F (FUNCION F X 1/4)
320
321
342
340: SELECTOR
352
350: REGISTRO ARITMETICO
SELECTOR 3-1 L
REGISTRO ARITMETICO L
30: ALEATORIZADOR DE DATOS
C
SELECTOR 2-1
311
SELECTOR 2-1
313
330
SUBCONVERTIDOR
1/2 UNIDAD DE SUBCONVERTIDOR
90
SELECTOR 2-1 H
REGISTRO ARITMETICO H
341
351
SELECTOR 2-1
211
212
213
SELECTOR 2-1
SELECTOR 8-1
Σ1H
Σ1L
Σ2H
Σ2L
Σ3H
Σ3L
Σ4H
Σ4L
DESPLAZAMIENTO DE 1 BYTE
214
SELECTOR 2-1
DESPLAZAMIENTO DE 1 BIT
216
SELECTOR 4-1
KLL
KLH
KAL
KAH
210: PROGRAMADOR DE CLAVES
CLAVE SECRETA
SELECTOR 8-1 KA
REGISTRO DE CLAVES KA
230
250
SELECTOR 8-1 KL
REGISTRO DE CLAVES KL
220
240
KAH || KAL
KLH || KLL
20: GENERADOR DE CLAVES
40: GENERADOR DE CLAVES INTERMEDIAS

Fig. 51

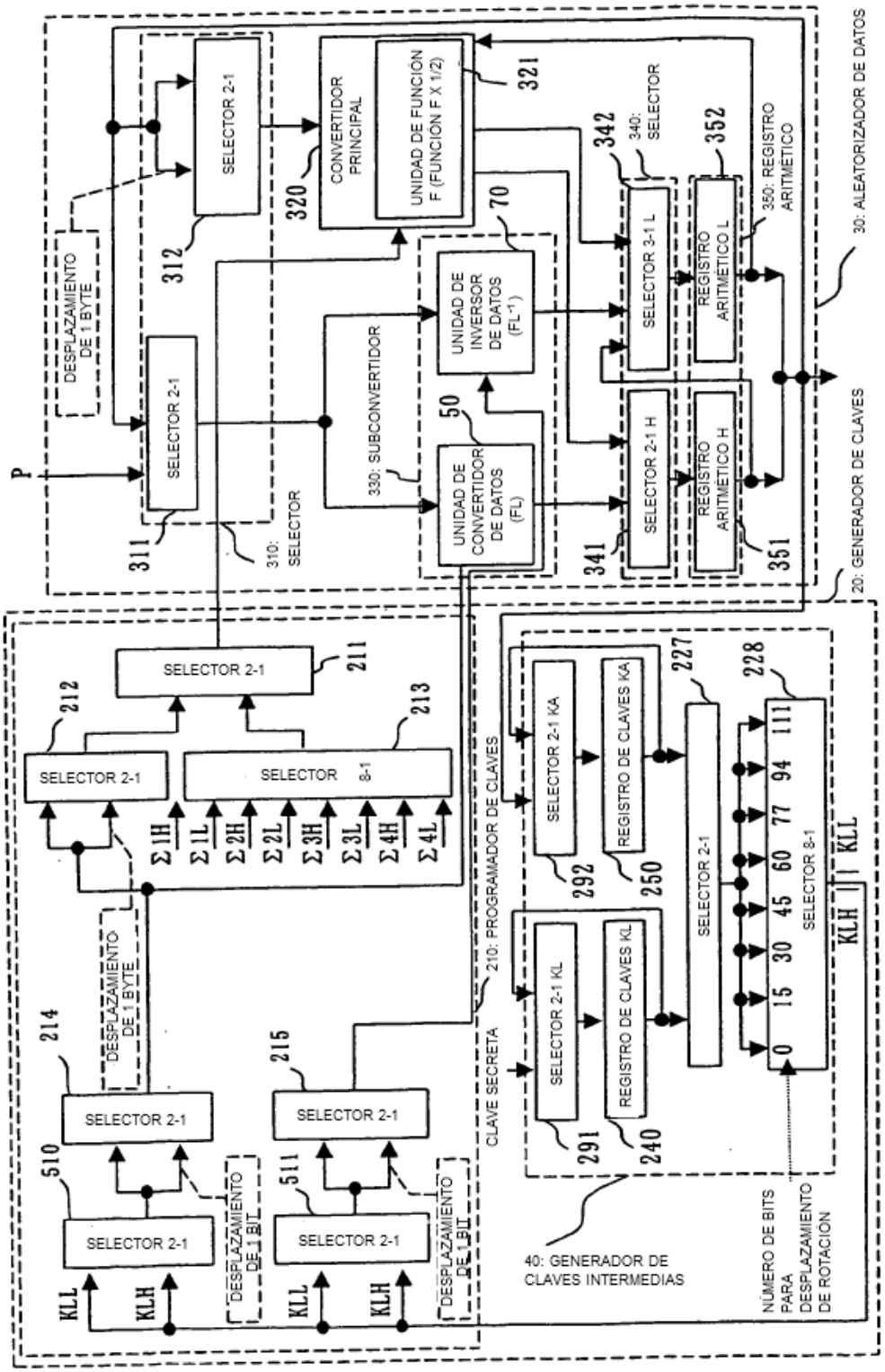

P
DESPLAZAMIENTO DE 1 BYTE
SELECTOR 2-1
SELECTOR 2-1
311
310: SELECTOR
312
330: SUBCONVERTIDOR
CONVERTIDOR PRINCIPAL
320
UNIDAD DE FUNCIÓN F (FUNCIÓN F X 1/2)
321
UNIDAD DE CONVERTIDOR DE DATOS (FL)
50
UNIDAD DE INVERSOR DE DATOS (FL-1)
70
341
SELECTOR 2-1 H
342
340: SELECTOR
SELECTOR 3-1 L
REGISTRO ARITMETICO H
351
REGISTRO ARITMETICO L
352
350: REGISTRO ARITMÉTICO
30: ALEATORIZADOR DE DATOS
20: GENERADOR DE CLAVES
SELECTOR 2-1
211
212
213
SELECTOR 2-1
SELECTOR 8-1
Σ 1H
Σ 1L
Σ 2H
Σ 2L
Σ 3H
Σ 3L
Σ 4H
Σ 4L
DESPLAZAMIENTO DE 1 BYTE
214
215
SELECTOR 2-1
SELECTOR 2-1
510
511
SELECTOR 2-1
SELECTOR 2-1
DESPLAZAMIENTO DE 1 BIT
DESPLAZAMIENTO DE 1 BIT
KLL
KLH
KLL
KLH
210: PROGRAMADOR DE CLAVES
CLAVE SECRETA
SELECTOR 2-1 KA
SELECTOR 2-1 KL
292
291
REGISTRO DE CLAVES KA
REGISTRO DE CLAVES KL
250
240
227
SELECTOR 2-1
228
111
SELECTOR 8-1
0 15 30 45 60 77 94
KLH
KLL
40: GENERADOR DE CLAVES INTERMEDIAS
NÚMERO DE BITS PARA DESPLAZAMIENTO DE ROTACIÓN

Fig. 52

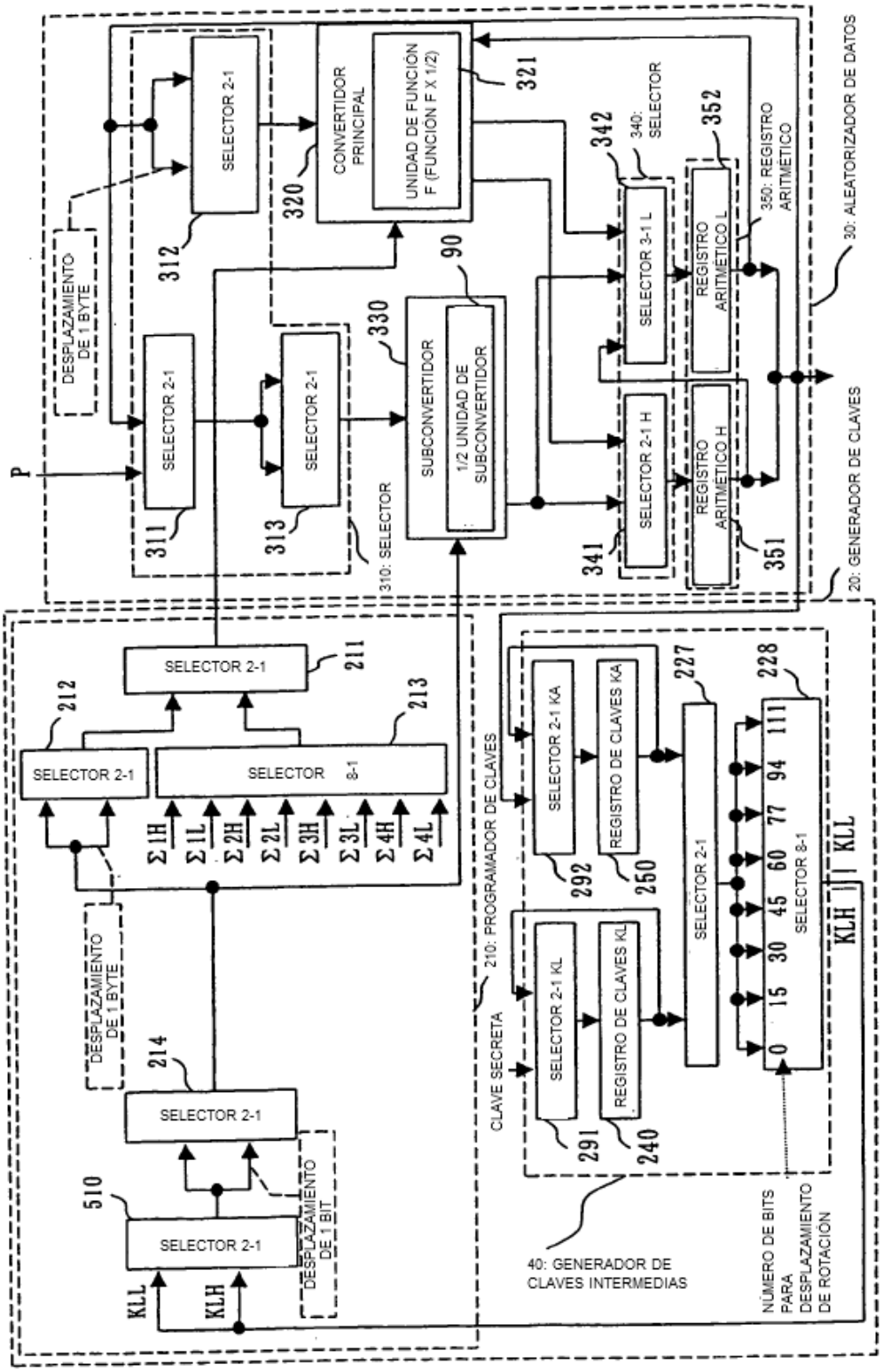

P
DESPLAZAMIENTO DE 1 BYTE
SELECTOR 2-1
SELECTOR 2-1
SELECTOR 2-1
311
312
313
310: SELECTOR
CONVERTIDOR PRINCIPAL
UNIDAD DE FUNCION F (FUNCION F X 1/2)
320
321
SUBCONVERTIDOR
1/2 UNIDAD DE SUBCONVERTIDOR
330
90
SELECTOR 3-1 L
SELECTOR 2-1 H
341
342
340: SELECTOR
REGISTRO ARITMETICO L
REGISTRO ARITMETICO H
351
352
350: REGISTRO ARITMETICO
30: ALEATORIZADOR DE DATOS
20: GENERADOR DE CLAVES
SELECTOR 2-1
SELECTOR 2-1
SELECTOR 8-1
211
212
213
Σ 1H
Σ 1L
Σ 2H
Σ 2L
Σ 3H
Σ 3L
Σ 4H
Σ 4L
DESPLAZAMIENTO DE 1 BYTE
SELECTOR 2-1
214
DESPLAZAMIENTO DE 1 BIT
SELECTOR 2-1
510
KLL
KLH
210: PROGRAMADOR DE CLAVES
CLAVE SECRETA
SELECTOR 2-1 KA
SELECTOR 2-1 KL
REGISTRO DE CLAVES KA
REGISTRO DE CLAVES KL
292
291
250
240
227
SELECTOR 2-1
228
SELECTOR 8-1
0 15 30 45 60 77 94 111
KLH KLL
40: GENERADOR DE CLAVES INTERMEDIAS
NÚMERO DE BITS PARA DESPLAZAMIENTO DE ROTACIÓN

Fig. 53

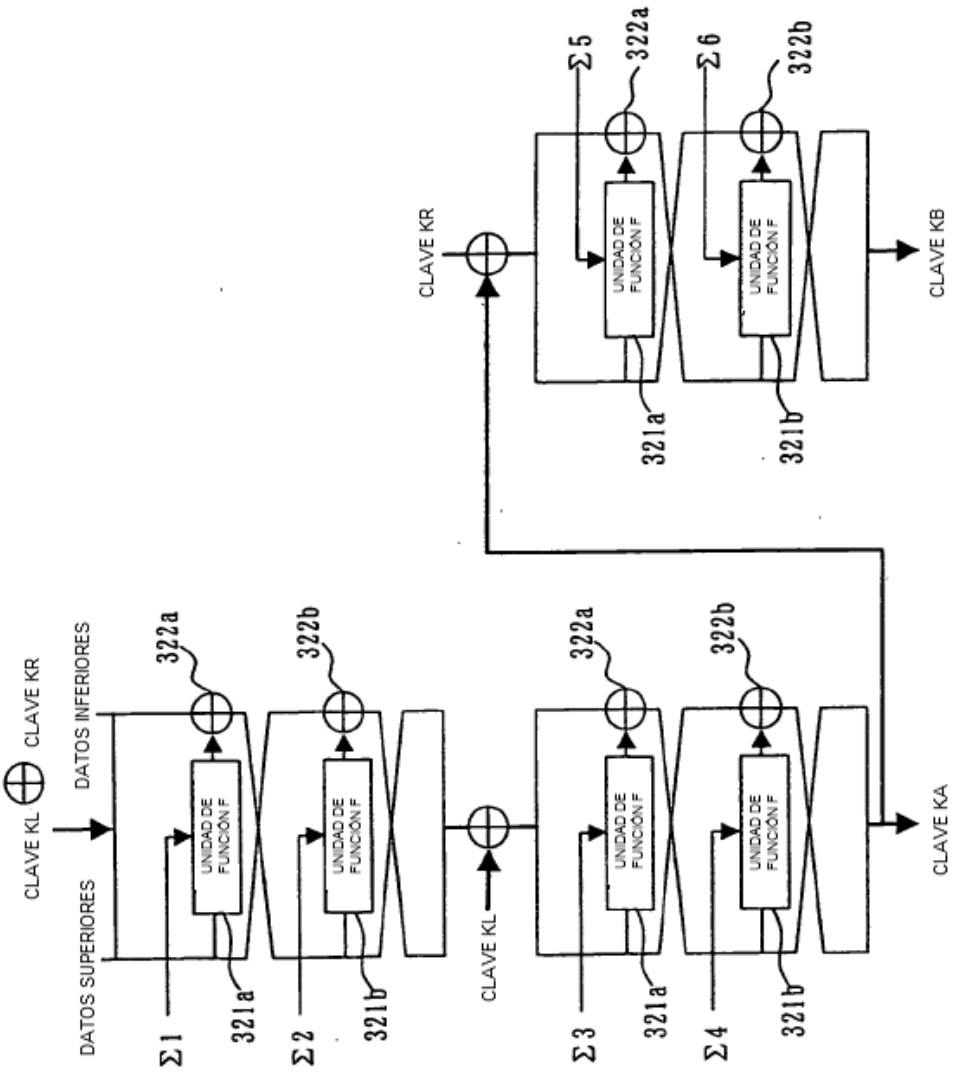

CLAVE KL
CLAVE KR
DATOS INFERIORES
DATOS SUPERIORES
322a
322b
UNIDAD DE FUNCIÓN F
321a
321b
Σ1
Σ2
Σ3
Σ4
Σ5
Σ6
CLAVE KL
CLAVE KR
CLAVE KB
CLAVE KA

Fig. 54

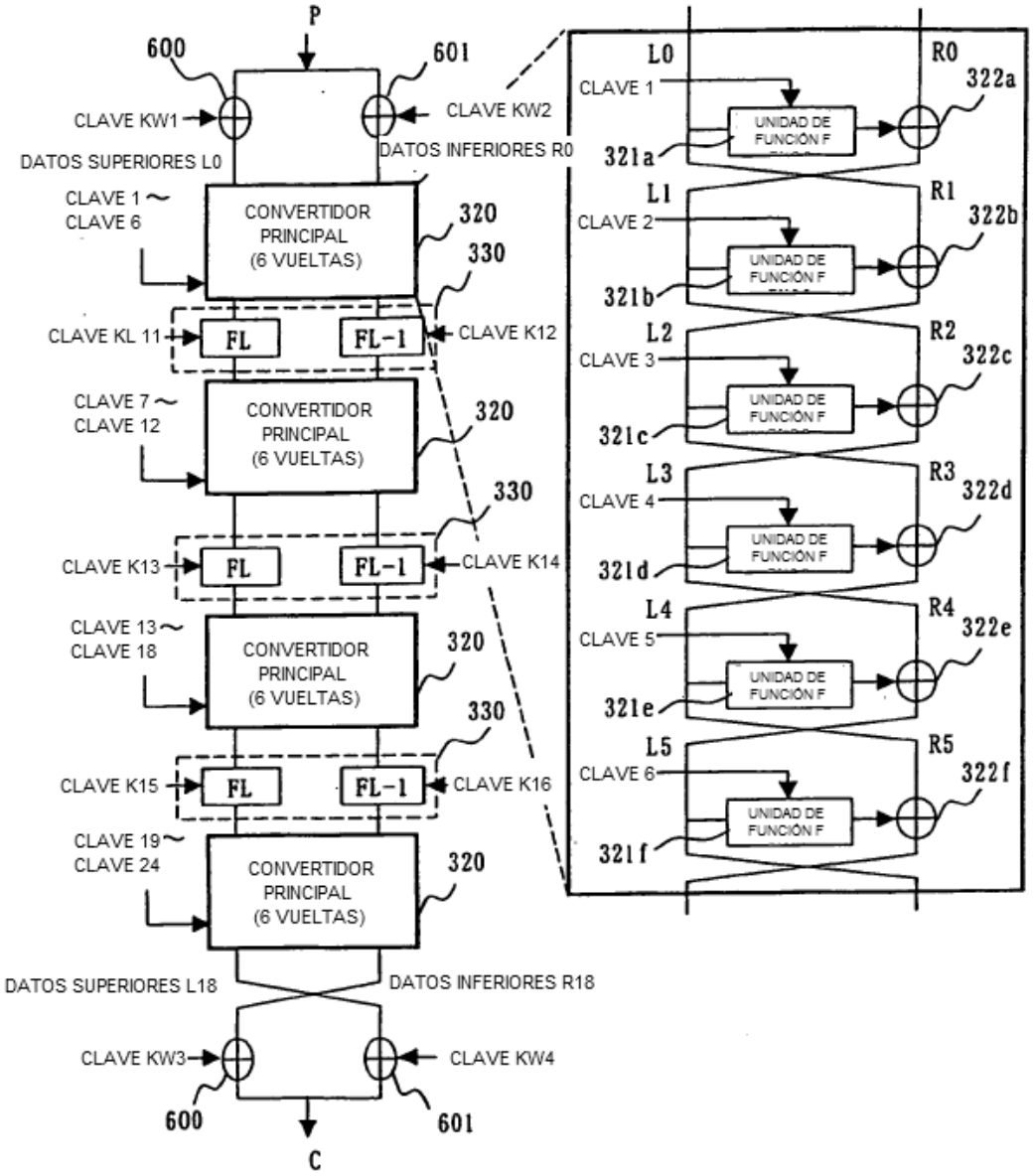

P
600
601
CLAVE KW1
CLAVE KW2
DATOS SUPERIORES L0
DATOS INFERIORES R0
CLAVE 1 ~ CLAVE 6
CONVERTIDOR PRINCIPAL (6 VUELTAS)
320
330
CLAVE KL 11
FL
FL-1
CLAVE K12
CLAVE 7 ~ CLAVE 12
CLAVE K13
CLAVE K14
CLAVE 13 ~ CLAVE 18
CLAVE K15
CLAVE K16
CLAVE 19 ~ CLAVE 24
DATOS SUPERIORES L18
DATOS INFERIORES R18
CLAVE KW3
CLAVE KW4
C
L0
R0
CLAVE 1
322a
UNIDAD DE FUNCIÓN F
321a
L1
R1
CLAVE 2
322b
321b
L2
R2
CLAVE 3
322c
321c
L3
R3
CLAVE 4
322d
321d
L4
R4
CLAVE 5
322e
321e
L5
R5
CLAVE 6
322f
321f

Fig. 55

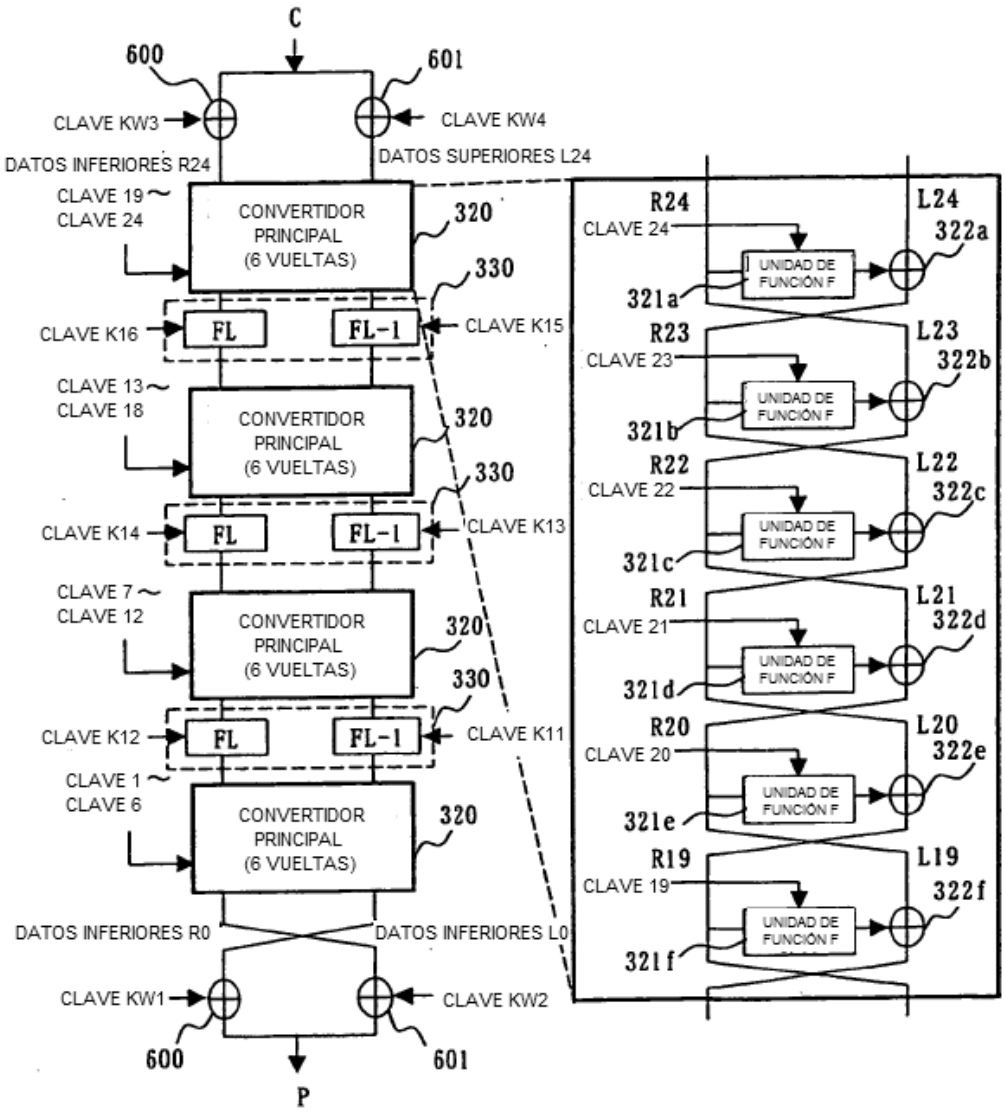

C
600
601
CLAVE KW3
CLAVE KW4
DATOS INFERIORES R24
DATOS SUPERIORES L24
CLAVE 19
CLAVE 24
CONVERTIDOR PRINCIPAL (6 VUELTAS)
320
330
CLAVE K16
FL
FL-1
CLAVE K15
CLAVE 13
CLAVE 18
CLAVE K14
CLAVE K13
CLAVE 7
CLAVE 12
CLAVE K12
CLAVE K11
CLAVE 1
CLAVE 6
DATOS INFERIORES R0
DATOS INFERIORES L0
CLAVE KW1
CLAVE KW2
P
R24
L24
322a
321a
R23
L23
322b
321b
R22
L22
322c
321c
R21
L21
322d
321d
R20
L20
322e
321e
R19
L19
322f
321f
UNIDAD DE FUNCIÓN F

Fig. 56

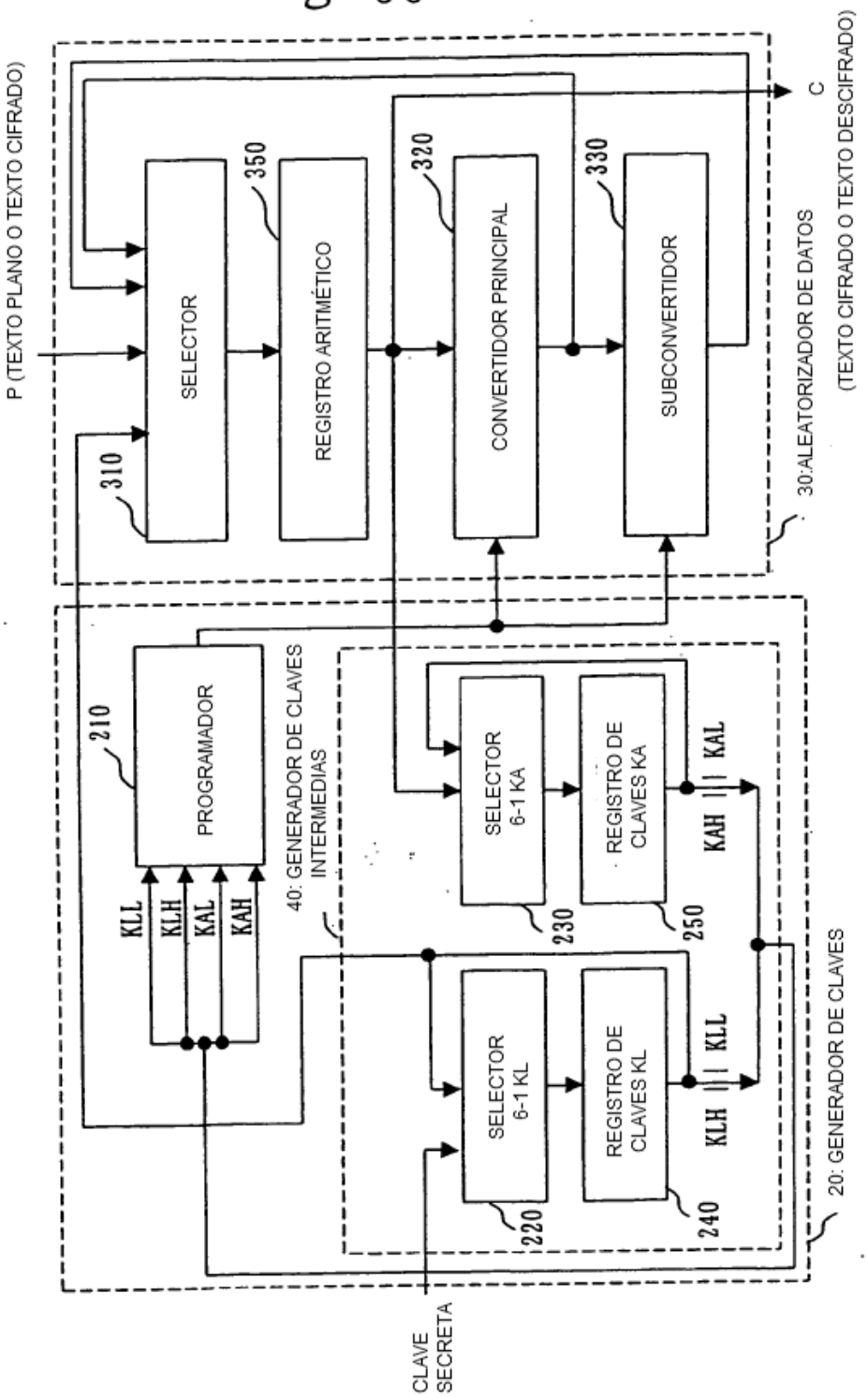

P (TEXTO PLANO O TEXTO CIFRADO)
C
(TEXTO CIFRADO O TEXTO DESCIFRADO)
30:ALEATORIZADOR DE DATOS
SELECTOR
REGISTRO ARITMÉTICO
CONVERTIDOR PRINCIPAL
SUBCONVERTIDOR
310
350
320
330
20: GENERADOR DE CLAVES
40: GENERADOR DE CLAVES INTERMEDIAS
PROGRAMADOR
210
KLL
KLH
KAL
KAH
SELECTOR 6-1 KA
REGISTRO DE CLAVES KA
SELECTOR 6-1 KL
REGISTRO DE CLAVES KL
230
250
220
240
CLAVE SECRETA

Fig. 57

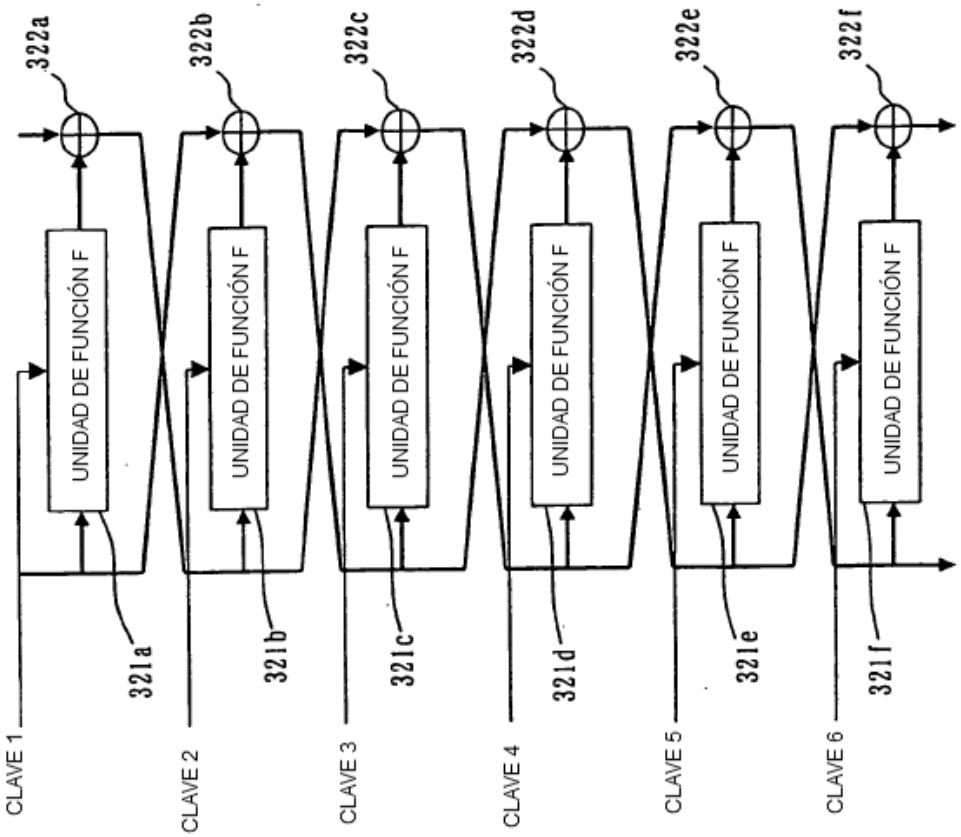

322a
322b
322c
322d
322e
322f
UNIDAD DE FUNCIÓN F
UNIDAD DE FUNCIÓN F
UNIDAD DE FUNCIÓN F
UNIDAD DE FUNCIÓN F
UNIDAD DE FUNCIÓN F
UNIDAD DE FUNCIÓN F
321a
321b
321c
321d
321e
321f
CLAVE 1
CLAVE 2
CLAVE 3
CLAVE 4
CLAVE 5
CLAVE 6

Fig. 58

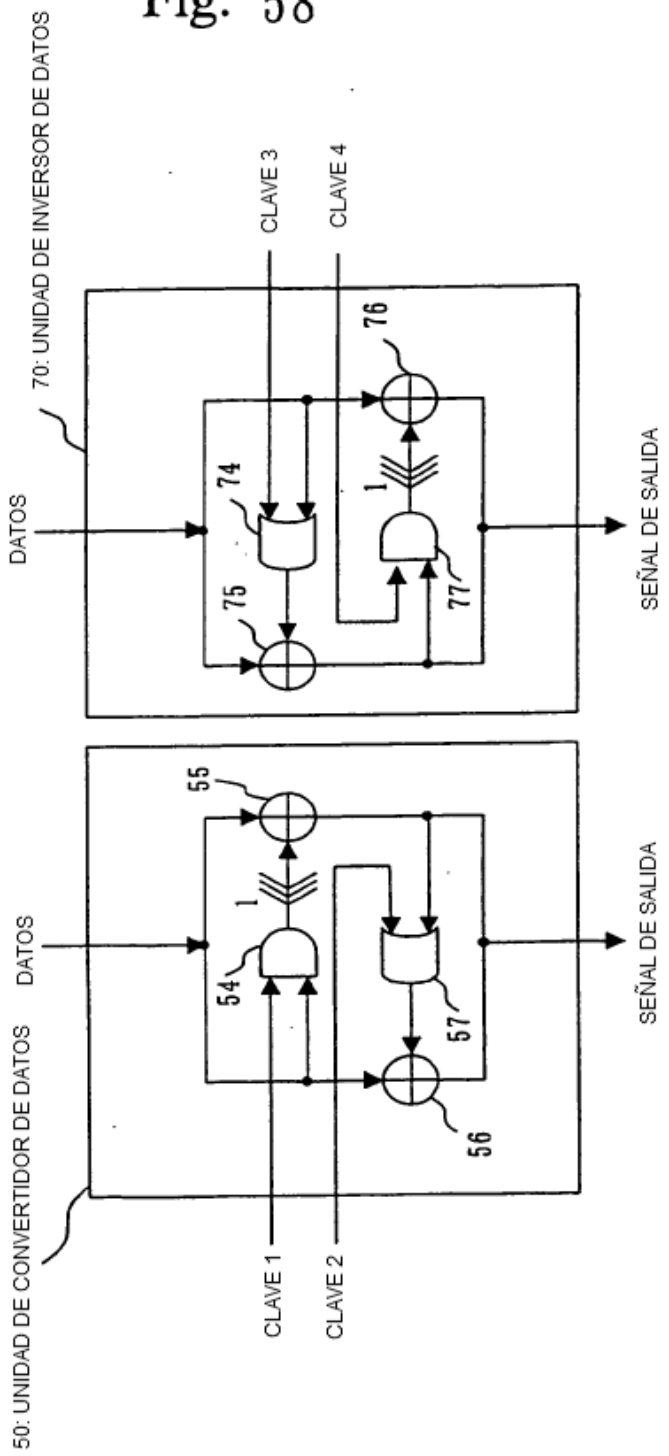

70: UNIDAD DE INVERSOR DE DATOS
CLAVE 3
CLAVE 4
DATOS
74
75
76
77
1
SEÑAL DE SALIDA
50: UNIDAD DE CONVERTIDOR DE DATOS
DATOS
55
54
56
57
1
SEÑAL DE SALIDA
CLAVE 1
CLAVE 2

Fig. 59

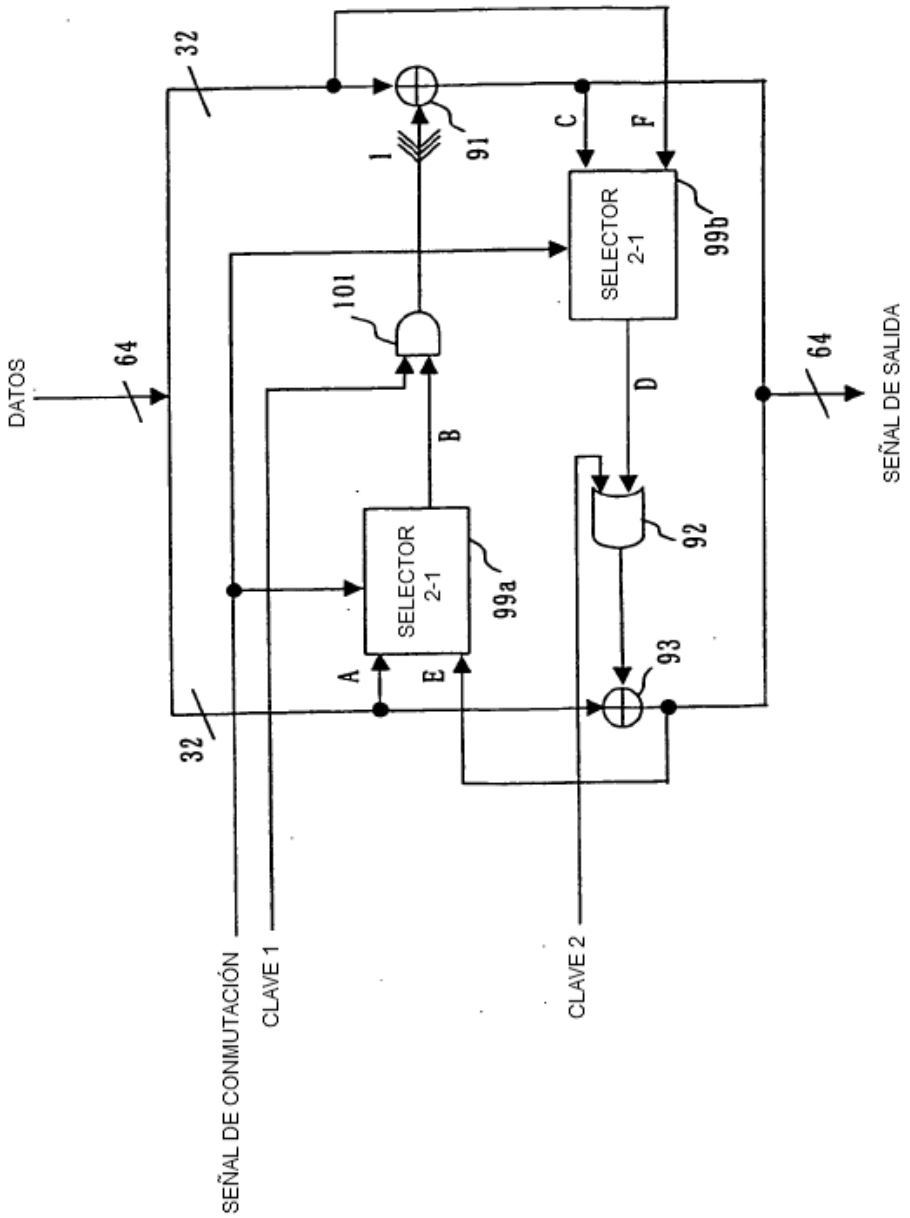

DATOS
64
32
32
64
SEÑAL DE SALIDA
SEÑAL DE CONMUTACIÓN
CLAVE 1
CLAVE 2
SELECTOR 2-1
99a
SELECTOR 2-1
99b
91
92
93
101
A
B
C
D
E
F
1

Fig. 60

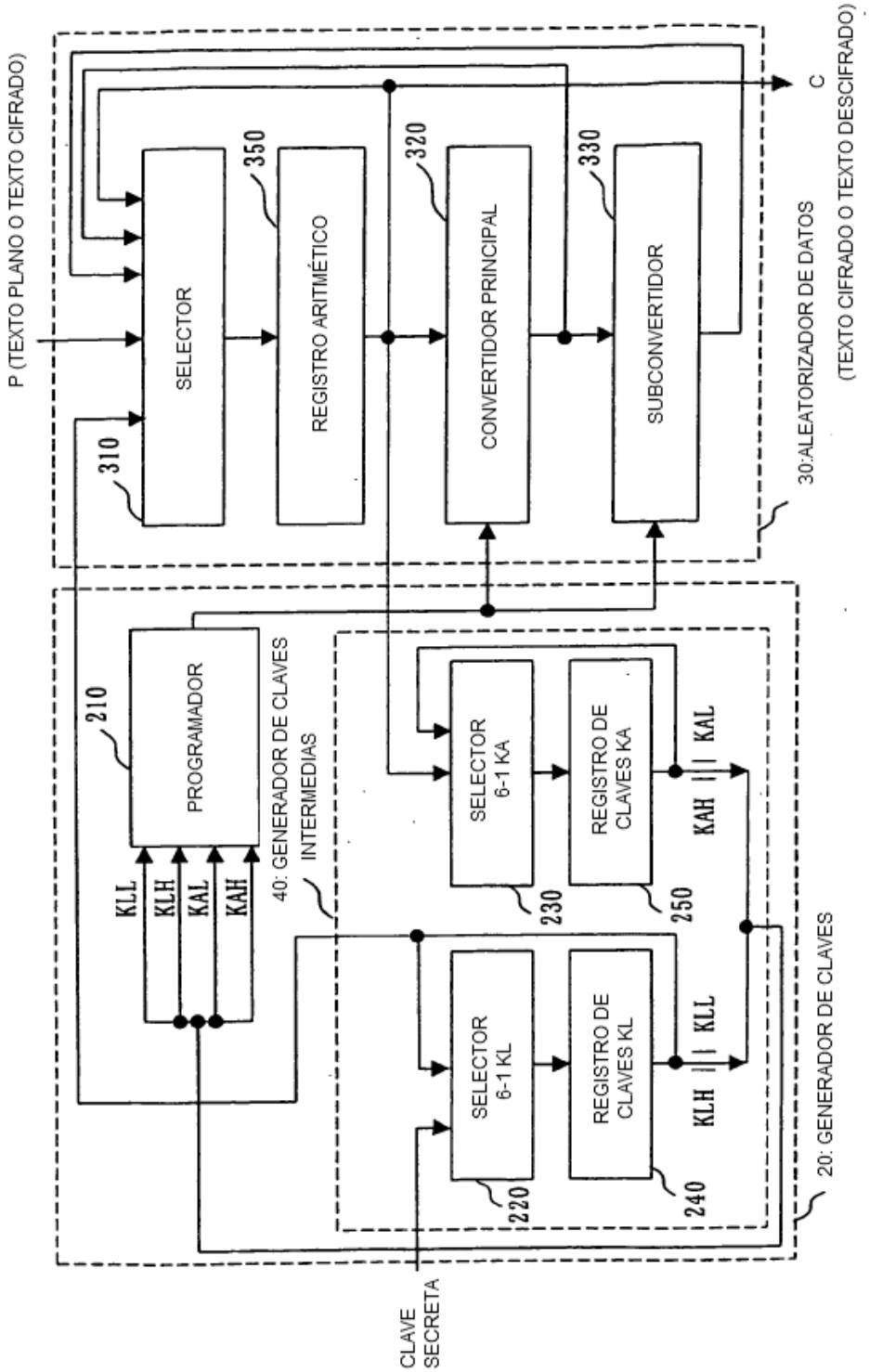

P (TEXTO PLANO O TEXTO CIFRADO)
C
(TEXTO CIFRADO O TEXTO DESCIFRADO)
30:ALEATORIZADOR DE DATOS
SELECTOR
REGISTRO ARITMÉTICO
CONVERTIDOR PRINCIPAL
SUBCONVERTIDOR
310
350
320
330
20: GENERADOR DE CLAVES
40: GENERADOR DE CLAVES INTERMEDIAS
PROGRAMADOR
210
KLL
KLH
KAL
KAH
SELECTOR 6-1 KA
REGISTRO DE CLAVES KA
SELECTOR 6-1 KL
REGISTRO DE CLAVES KL
230
250
220
240
CLAVE SECRETA

Fig. 61

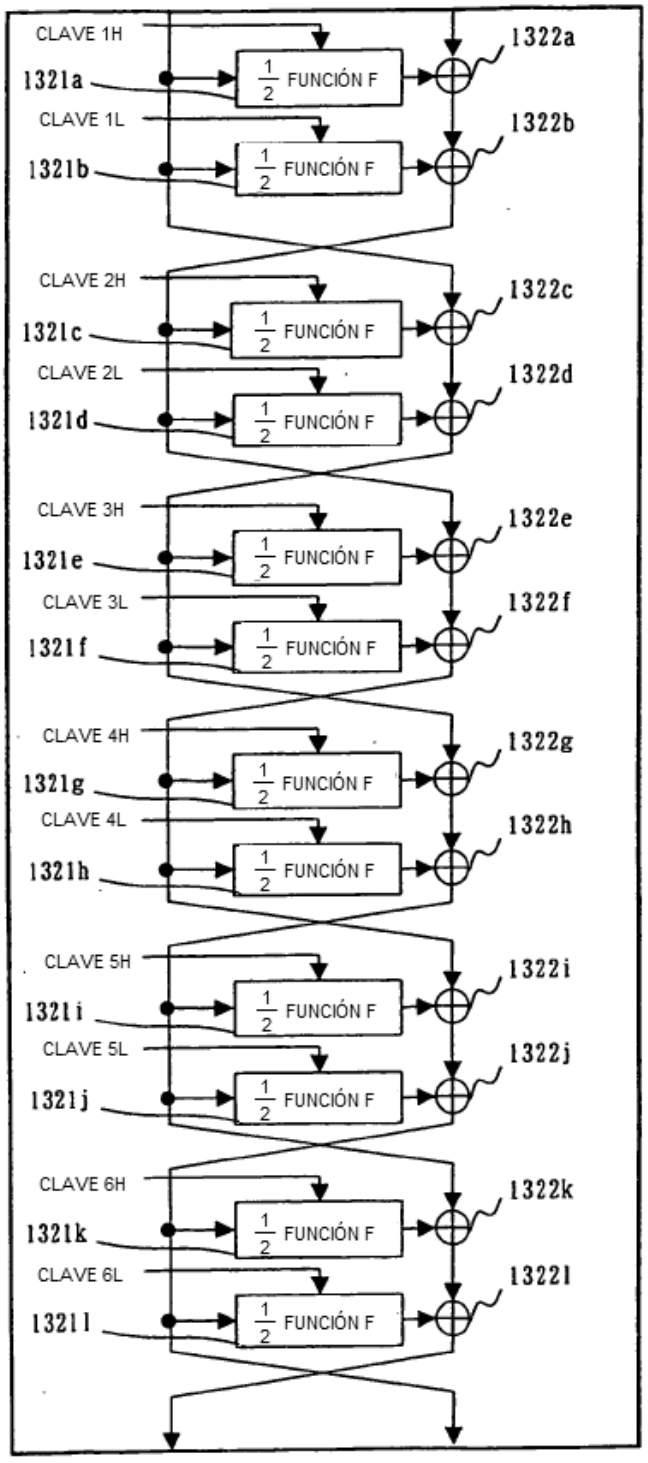

CLAVE 1H
1321a
CLAVE 1L
1321b
1/2 FUNCIÓN F
1322a
1322b
CLAVE 2H
1321c
CLAVE 2L
1321d
1322c
1322d
CLAVE 3H
1321e
CLAVE 3L
1321f
1322e
1322f
CLAVE 4H
1321g
CLAVE 4L
1321h
1322g
1322h
CLAVE 5H
1321i
CLAVE 5L
1321j
1322i
1322j
CLAVE 6H
1321k
CLAVE 6L
1321l
1322k
1322l

Fig. 62

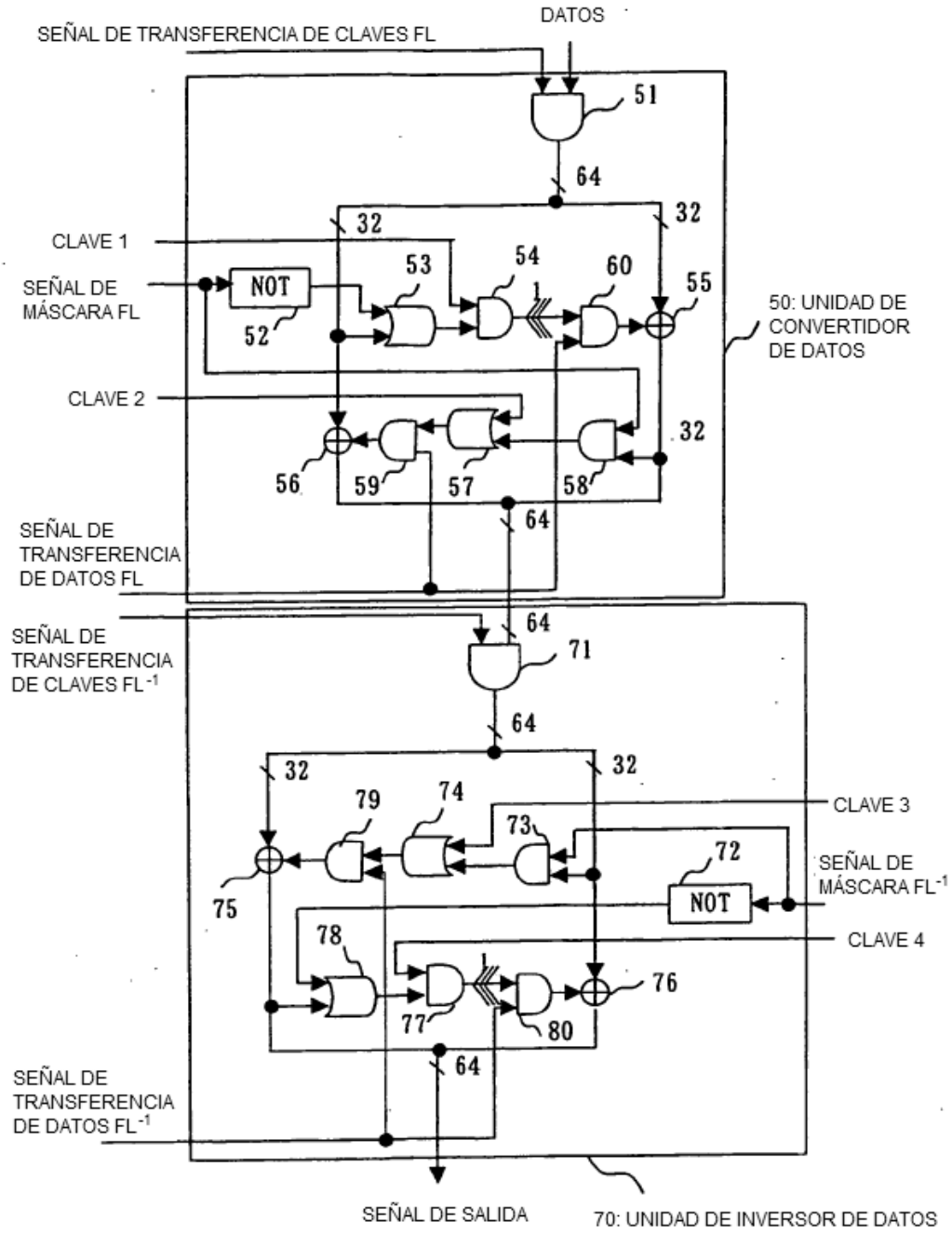

DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL
51
64
32
32
CLAVE 1
SEÑAL DE MÁSCARA FL
NOT
52
53
54
60
55
50: UNIDAD DE CONVERTIDOR DE DATOS
CLAVE 2
56
59
57
58
32
64
SEÑAL DE TRANSFERENCIA DE DATOS FL
SEÑAL DE TRANSFERENCIA DE CLAVES FL-1
64
71
64
32
32
CLAVE 3
79
74
73
72
SEÑAL DE MÁSCARA FL-1
75
NOT
78
CLAVE 4
76
77
80
64
SEÑAL DE TRANSFERENCIA DE DATOS FL-1
SEÑAL DE SALIDA
70: UNIDAD DE INVERSOR DE DATOS

Fig. 63

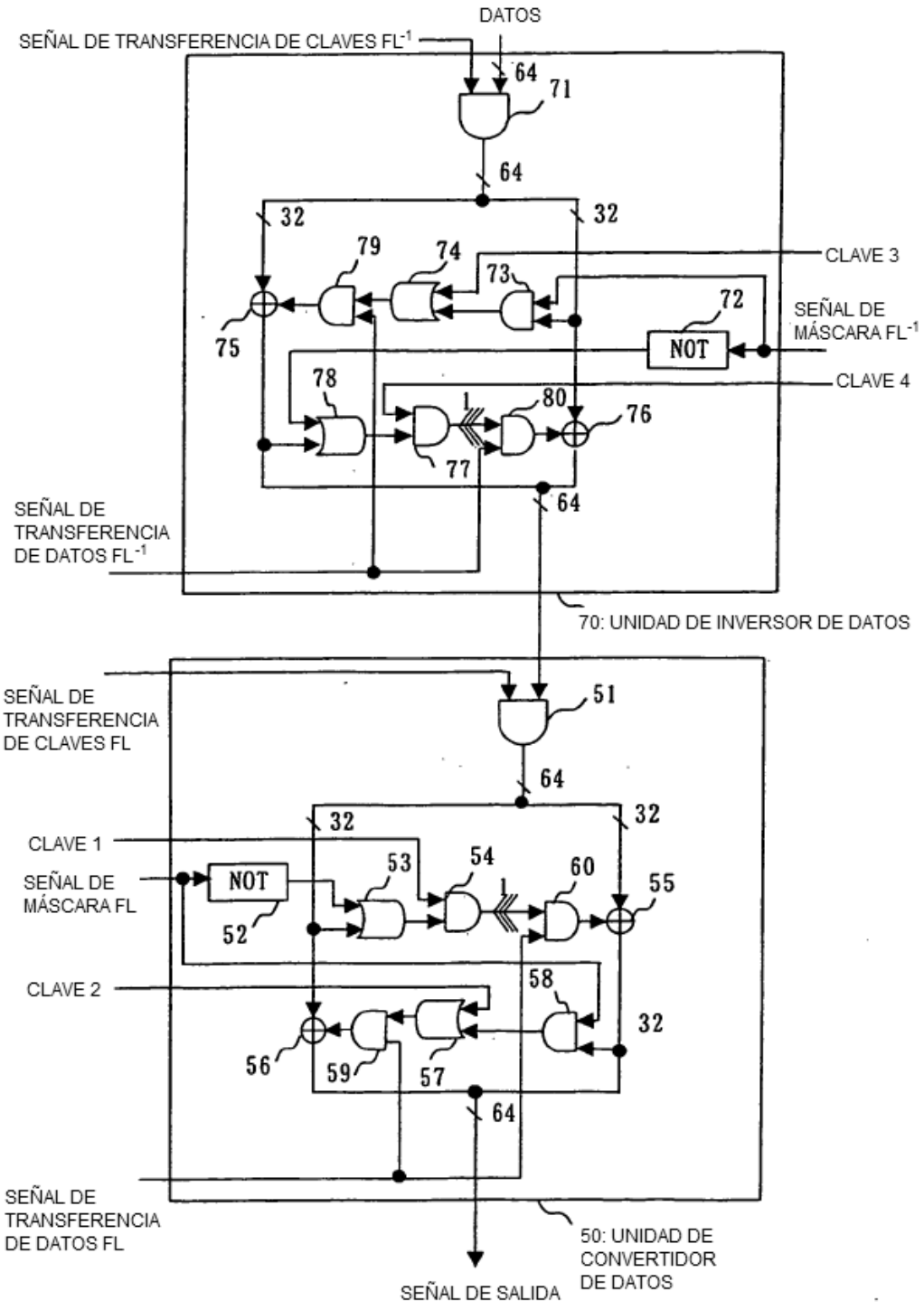
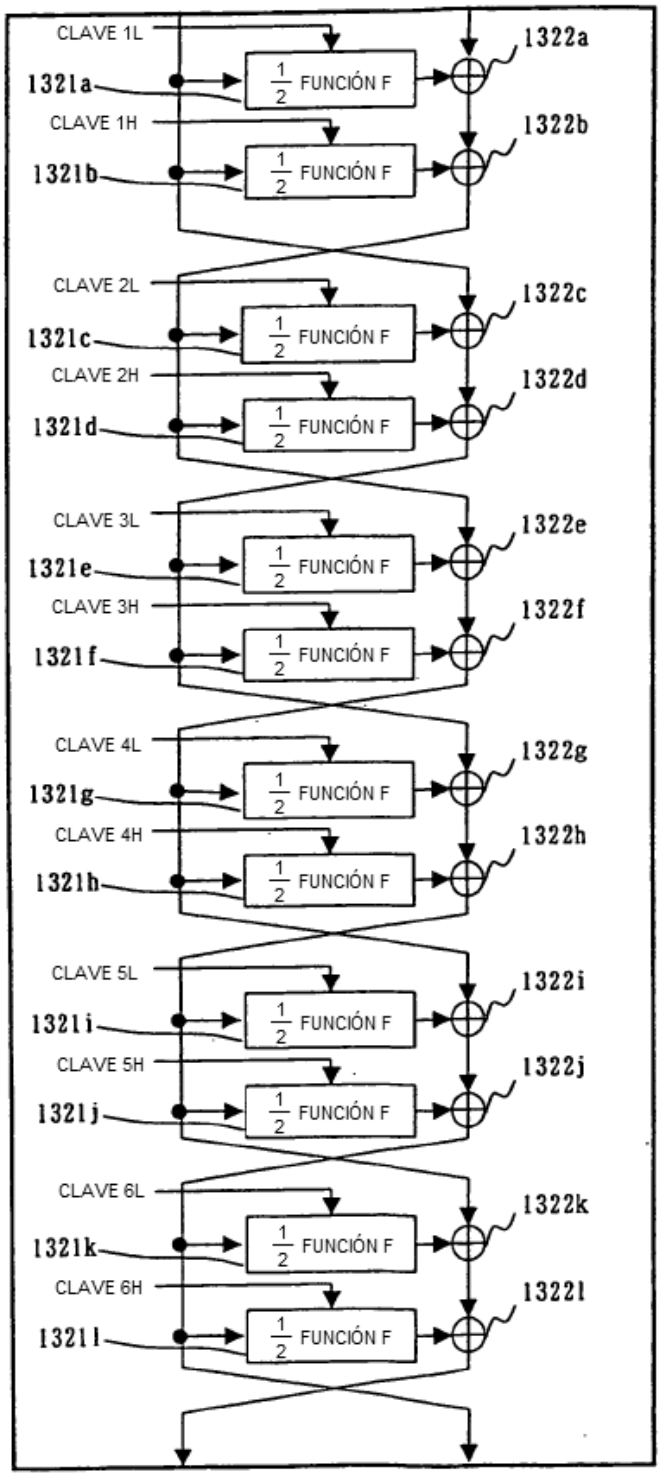

DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL-1
64
71
64
32
32
79
74
73
CLAVE 3
72
SEÑAL DE MÁSCARA FL-1
75
NOT
78
CLAVE 4
80
76
77
64
SEÑAL DE TRANSFERENCIA DE DATOS FL-1
70: UNIDAD DE INVERSOR DE DATOS
SEÑAL DE TRANSFERENCIA DE CLAVES FL
51
64
32
32
CLAVE 1
SEÑAL DE MÁSCARA FL
NOT
53
54
60
55
52
CLAVE 2
58
32
56
59
57
64
SEÑAL DE TRANSFERENCIA DE DATOS FL
50: UNIDAD DE CONVERTIDOR DE DATOS
SEÑAL DE SALIDA

Fig. 64


CLAVE 1L
1321a
CLAVE 1H
1321b
1/2 FUNCIÓN F
1322a
1322b
CLAVE 2L
1321c
CLAVE 2H
1321d
1322c
1322d
CLAVE 3L
1321e
CLAVE 3H
1321f
1322e
1322f
CLAVE 4L
1321g
CLAVE 4H
1321h
1322g
1322h
CLAVE 5L
1321i
CLAVE 5H
1321j
1322i
1322j
CLAVE 6L
1321k
CLAVE 6H
1321l
1322k
1322l