(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 391 639**

(51) Int. CI.:
H04L 9/06 (2006.01)
G09C 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05781289 .3**
(96) Fecha de presentación: **30.08.2005**
(97) Número de publicación de la solicitud: **1788542**
(97) Fecha de publicación de la solicitud: **23.05.2007**

(54) Título: **Dispositivo de cifrado, método de cifrado, y programa de ordenador**

(30) Prioridad:
03.09.2004 JP 2004256465

(45) Fecha de publicación de la mención BOPI:
28.11.2012

(45) Fecha de la publicación del folleto de la patente:
28.11.2012

(73) Titular/es:
SONY CORPORATION (100.0%)
1-7-1, Konan Minato-ku
Tokyo, JP

(72) Inventor/es:
SHIRAI, TAIZO y
BART, PRENEEL

(74) Agente/Representante:
DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Dispositivo de cifrado, método de cifrado, y programa de ordenador.

Campo técnico

Este invento se refiere a un aparato de tratamiento criptográfico, A un método de tratamiento criptográfico, y a un programa de ordenador para llevarlo a cabo, y más específicamente a un aparato de tratamiento criptográfico con una resistencia mejorada al análisis lineal y al análisis diferencial conocido como tratamiento de análisis de descifrar y tratamiento de ataque de criptoanálisis, a un método de tratamiento criptográfico, y a un programa de ordenador para ello.

Técnica antecedente

Actualmente, con el desarrollo de las comunicaciones de red y el comercio electrónico, garantizar la seguridad en las comunicaciones resulta una cuestión vital. Un medio de garantizar la seguridad es una tecnología criptográfica o de cifrado o codificación, y actualmente están siendo ejecutadas comunicaciones que utilizan distintas técnicas criptográficas.

Por ejemplo, se ha puesto en uso de manera práctica un sistema en el que el módulo de tratamiento criptográfico está integrado en un pequeño dispositivo, tal como una tarjeta de IC, la transmisión y recepción de datos es realizada entre la tarjeta de IC y un lector/escritor que actúa como un dispositivo de lectura y escritura de datos, y el tratamiento de autenticación o cifrado/descifrado de enviar/recibir datos es realizado.

Hay distintos algoritmos en el tratamiento criptográfico, que están ampliamente divididos en un sistema criptográfico clave en el que una clave de cifrado y una clave de descifrado, por ejemplo, una clave pública y una clave secreta son establecidas, y el sistema criptográfico de clave común en el que una clave común es establecida o establecida como una clave de cifrado y una clave de descifrado.

Hay también distintos algoritmos en el sistema criptográfico de clave común. Uno de ellos es un sistema en el que se genera una pluralidad de claves utilizando una clave común cuando un tratamiento de conversión de base y de datos es realizado repetidamente para cada unidad de bloque (64 bits, 128 bits, etc.) utilizando la pluralidad de claves generadas. Un algoritmo típico que aplica tal método de generación de claves y el tratamiento de conversión de datos es un método criptográfico de bloque de clave común.

Como un algoritmo típico del tratamiento criptográfico de bloque de clave común, por ejemplo, hay un algoritmo DES (Norma de Cifrado de Datos) como un cifrado de norma federal de los Estados Unidos de Norteamérica, y es ampliamente utilizado en distintos campos.

Cualquier algoritmo del tratamiento criptográfico de bloque de clave común tipificado por el DES puede estar principalmente dividido en una sección de función de ronda para realizar la conversión de datos de entrada y una sección de programa de clave para generar una clave que ha de ser aplicada en cada ronda de una parte de la función de ronda (función F). Una clave de ronda (subclave) que ha de ser aplicada en cada ronda de la sección de función de ronda es generada en la sección de programa de clave a la que es introducida una clave maestra (clave principal), y es aplicada en cada parte de la función de ronda.

Sin embargo, en tal tratamiento criptográfico de clave común, la fuga o pérdida de la clave por criptoanálisis ha resultado un problema. Como una técnica típica de criptoanálisis o técnica de ataque, se conoce un análisis diferencial (también llamado método de criptoanálisis diferencial o ataque de criptoanálisis diferencial) en el que es analizada una clave de aplicación en cada función de ronda analizando muchos datos de entrada (texto sin codificar o sin formato) y sus datos de salida (texto cifrado), y un análisis lineal (también llamado método de criptoanálisis lineal o ataque de criptoanálisis lineal) que realiza un análisis basado en textos sin cifrar y textos cifrados correspondientes.

Que sea fácil de analizar una clave por criptoanálisis significa que hay una baja seguridad en el tratamiento criptográfico. En el algoritmo DES convencional, hay un problema de que, como el tratamiento (matriz de conversión) que ha de ser aplicado en una sección de conversión lineal en una sección de función de ronda (función F) es equivalente en una ronda de cada etapa, el criptoanálisis es fácil de hacer, y por consiguiente da como resultado un análisis fácil de la clave.

En “Perfeccionar la inmunidad de códigos o cifras Feistel contra el criptoanálisis diferencial utilizando múltiples matrices MDS”, Taizo Shirai y Kyoji Shibutami, Cifrado de Software Rápido 2004. Notas de lectura en Ciencia Informática, vol. 3017, páginas 260-278, Springer Verlag, Febrero de 2004, se ha descrito una estrategia de diseño para evitar una cancelación de diferencia empleando múltiples matrices basadas en MDS en una capa de difusión de una función F de un código de bloque. La efectividad del método propuesto es confirmada por un resultado experimental que muestra que el porcentaje de cajas S activas del código Feistel recientemente diseñado resulta el mismo que para AES.

En “Construcción de códigos MDS”, publicada en el Seminario de criptografía en el Departamento de Matemáticas aplicadas e Informática de Rennes por Jérôme Lacan, se ha descrito que las matrices de Reed-Solomon son reversibles, este documento describe la construcción de códigos MDS sistemáticos y su aplicación en criptografía.

Descripción del Invento

Problema que ha de ser resuelto por el Invento

Este invento se ha llevado a cabo en vista de los problemas antes mencionados, y tiene como objeto proporcionar un aparato de tratamiento criptográfico que realiza un algoritmo criptográfico de bloque de clave común muy resistente al análisis lineal y al análisis diferencial, un método de tratamiento criptográfico, y un programa de ordenador para llevarlo a cabo.

Medios para Resolver el Problema

El problema es resuelto por las características de las reivindicaciones independientes. Realizaciones adicionales son el objeto de las reivindicaciones dependientes.

Breve Descripción de los Dibujos

La figura 1 es un diagrama que muestra una configuración de un código de bloque de clave común típica que tiene una estructura Feistel.

Las figuras 2A y 2B son diagramas que explican una estructura de una función F que es establecida como una sección de función de ronda. La figura 2A es un diagrama que muestra una entrada y una salida de la función F 120 en una ronda. La figura 2B es un diagrama que muestra detalles de la estructura de la función F 120.

La figura 3 es un diagrama que muestra un ejemplo de una matriz cuadrada que ha de ser aplicada al tratamiento de conversión lineal.

La figura 4 es un diagrama que explica la cancelación de diferencia simultánea de tres etapas en un código de bloque de 128 bits de m = 8 y n = 8.

La figura 5 es un diagrama que explica un ejemplo concreto para generar una diferencia ΔY_i de salida de la función F realizando la conversión lineal con una matriz MDS cuadrada.

La figura 6 es un diagrama que explica la cancelación de la diferencia simultánea de cinco etapas en un código de bloque de 128 bits de m = 8 y n = 8.

La figura 7 es un diagrama que explica una definición de la cancelación de la diferencia simultánea de la etapa arbitraria en tratamiento criptográfico de bloque de clave común.

La figura 8 muestra un ejemplo de la matriz MDS cuadrada.

La figura 9 es un diagrama que explica un ejemplo de ajuste de matrices MDS cuadradas como matrices de conversión lineal de las funciones F de las rondas respectivas en un algoritmo criptográfico de bloque de clave común de acuerdo con este invento.

La figura 10 es un diagrama de flujo que explica una secuencia del tratamiento de configuración de matrices MDS cuadradas como las matrices de conversión lineal de las funciones F de rondas respectivas en el algoritmo criptográfico de bloque de clave común de acuerdo con el invento.

La figura 11 es un diagrama de flujo que explica un ejemplo a1 de tratamiento para generar matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis diferenciales como una técnica de generación de matrices MDS cuadradas que son las matrices de conversión lineal que han de ser establecidas en las funciones F de rondas respectivas.

La figura 12 es un diagrama de flujo que explica una ejemplo a2 de tratamiento para generar matrices MDS cuadradas que producen una resistencia mejorada a los ataques de criptoanálisis diferenciales como una técnica de generación de matrices MDS cuadradas que son las matrices de conversión lineal que han de ser establecidas en las funciones F de rondas respectivas.

La figura 13 es un diagrama de flujo que explica un ejemplo a3 de tratamiento para generar matrices MDS cuadradas que producen una resistencia mejorada a los ataques de criptoanálisis diferencial como una técnica de generación de matrices MDS cuadradas que son matrices de conversión lineal que han de ser establecidas en las funciones F de rondas respectivas.

La figura 14 es un diagrama que explica una técnica concreta del ejemplo a3 de tratamiento para generar matrices MDS cuadradas que son las matrices de conversión lineal que han de ser establecidas en las funciones F de rondas respectivas.

La figura 15 es un diagrama de flujo que explica un ejemplo b1 de tratamiento para generar matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis lineal como una técnica de generación de matrices cuadradas MDS que son las matrices de conversión lineal que han de ser ajustadas en las funciones F de rondas respectivas.

La figura 16 es un diagrama de flujo que explica un ejemplo de tratamiento para generar matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis lineal como una técnica de generación de matrices MDS cuadradas que son las matrices de conversión lineal que han de ser ajustadas en las funciones F de rondas respectivas.

La figura 17 es un diagrama de flujo que explica un ejemplo de tratamiento para generar matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis diferencial y a ataques de criptoanálisis lineal como una técnica de generación de matrices MDS cuadradas que son las matrices de conversión lineal que han de ser ajustadas en las funciones F de rondas respectivas.

La figura 18 es un diagrama que muestra un ejemplo de una configuración de un módulo IC como un aparato de tratamiento criptográfico para realizar un tratamiento criptográfico de acuerdo con este invento.

Mejor Modo para Llevar a la Práctica el Invento

A continuación, se explicarán detalles de un aparato de tratamiento criptográfico de este invento, un método de tratamiento criptográfico, y un programa de ordenador para ello. La explicación será dada en el siguiente orden de artículos.

1. Tratamiento de análisis diferencial en un algoritmo criptográfico de bloque de clave común
2. Tratamiento de análisis lineal en el algoritmo criptográfico de bloque de clave común
3. Algoritmo criptográfico basado en este invento

(3-a) Ejemplo de generación de matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis diferencial y ajustarlas a las funciones F

(3-b) Ejemplo de generación de matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis lineal y ajustarlas a las funciones F

(3-c) Ejemplo de generación de matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis diferencial y ataques de criptoanálisis lineal y ajustarlas a las funciones F.

[1. Tratamiento de análisis diferencial en algoritmo criptográfico de bloque de clave común]

En primer lugar, se explicará un esbozo o perfil del tratamiento de análisis diferencial en el algoritmo criptográfico de bloque de clave común tipificado por el tratamiento criptográfico DES (Norma de Cifrado de Datos) que utiliza un modelo generalizado de tratamiento criptográfico de bloque de clave común.

El algoritmo del tratamiento criptográfico de bloque de clave común puede estar dividido principalmente en una sección de la función de ronda para realizar la conversión de datos de entrada y una sección de programa de claves para generar una clave que ha de ser aplicada en cada ronda de la parte de la función de ronda. Una clave (subclave) aplicada en cada ronda de la función de ronda es generada por la sección de programa de clave en la que es introducida una clave maestra (clave principal), basada en ella, y es aplicada en cada ronda. Entre los sistema típicos de este sistema criptográfico de clave común, hay un DES (Norma de Cifrado de Datos) como un sistema de normas Federales de los Estados Unidos de Norteamérica.

Una estructura del tratamiento criptográfico de bloque de clave común típico denominada estructura Feistel será explicada con referencia a la figura 1.

La estructura Feistel tiene una configuración de convertir un texto sin codificar en un texto cifrado mediante la simple repetición de una función de conversión. La longitud de un texto sin codificar es ajustada a 2mn (2xmxn) bit. Aquí, m y n son ambos números enteros. En primer lugar, un texto sin codificar de 2mn bit está dividido en dos datos de entrada, un P_L (Perfil-Izquierdo) 101 de mn bit y un P_R (Perfil-Derecho) 102 de mn bit, y son utilizados como valores de entrada.

La estructura Feistel es expresada por repetición de una estructura básica denominada función de ronda, y una función de conversión de datos que está incluida en cada ronda es denominada una función F 120. La figura 1 muestra una configuración ejemplar compuesta de las funciones F (funciones de ronda) 120 repetidas para las etapas-r.

Por ejemplo, en la primera ronda, los datos de entrada X de mn bit y una clave de ronda $K_1$103 de mn bit introducida desde una unidad de generación de claves (no mostrada en la figura) son introducidos en la función F 120, que emite datos Y de mn bit después del tratamiento de conversión de datos en él. Una sección 104 OR-exclusiva ejecuta una operación OR-exclusiva en la salida y las otras piezas de datos de entrada procedentes de la etapa anterior, y emite un resultado de la operación de mn bit para la siguiente función de ronda. El tratamiento criptográfico se completa aplicando este tratamiento, es decir, la función F repetidamente para un número de ronda predeterminado (r), y emite datos divididos CL (Cifrado-Izquierdo) y datos CR (Cifrado-Derecho) de un texto cifrado. La configuración anterior conduce al hecho de que con el fin de realizar el descifrado con la estructura Feistel, solo es necesario invertir una secuencia de inserción de claves de ronda, no necesarias para configurar una función inversa.

La estructura de la función F 120 que es establecida como una función de cada ronda será explicada con referencia a la figura 2. La figura 2A es un diagrama que muestra una entrada y una salida de la función F 120 en una ronda. La figura 2B es un diagrama que muestra detalles de la estructura de la función F 120. La función F 120 tiene la denominada estructura tipo SPN que consiste de una capa de conversión no lineal y una capa de conversión lineal conectadas juntas, como se ha mostrado en la figura 2B.

La función F tipo SPN 120 tiene una pluralidad de cajas S 121 para realizar el tratamiento de conversión no lineal, como se ha mostrado en la figura 2B. La operación O-exclusiva es ejecutada sobre un valor de entrada X de mn bit procedente de una etapa anterior de la sección de la función de ronda junto con una clave de ronda K_i introducida desde la sección de programa de clave, y su emisión es introducida a una pluralidad (m) de cajas S cada una de las cuales ejecuta un tratamiento de conversión no lineal por n bit. Cada una de las cajas S realiza el tratamiento de conversión no lineal que aplica, por ejemplo, una tabla de conversión.

Un valor de salida Z de mn bit que son datos de salida desde la caja S 121 es introducido en una sección de conversión lineal 122 para realizar el tratamiento de conversión lineal, que ejecuta el tratamiento de conversión lineal, por ejemplo, tratamiento de intercambio de posiciones de bit etc., y emite un valor de salida Y de mn bit. El valor de salida Y junto con los datos de entrada procedentes de la etapa precedente es sometido a la operación O-exclusiva, y su resultado es asignado a un valor de entrada de la función F de la siguiente ronda.

En la función F 120 mostrada en la figura 2, la longitud de bit de una entrada/salida es mxn (m, n: números enteros), la capa de conversión no lineal tiene una configuración en la que m cajas S 121 cada una de las cuales sirve como la capa de conversión no lineal cuya entrada y salida son n bit están dispuestas en paralelo, y la sección 122 de conversión lineal cuando la capa de conversión lineal ejecuta el tratamiento de conversión lineal basándose en una matriz cuadrada emésima que tiene elementos en un campo de extensión $GF(2^n)$ definido por un polinomio irreducible enésimo como sus elementos.

La figura 3 muestra un ejemplo de una matriz cuadrada que ha de ser aplicada al tratamiento de conversión lineal en la sección de conversión lineal 122. Una matriz cuadrada 125 mostrada en la figura 3 es un ejemplo de n = 8 y m = 8. La conversión lineal es ejecutada sobre datos de m n bits, Z [1], Z [2], ..., Z[m] emitidos desde la sección de conversión no lineal (caja S 121) que aplica la matriz cuadrada predeterminada 125, e Y[1], Y[2], ..., Y[m] cuando salidas de la función F (función de ronda) emitida son determinadas. Nótese que la operación lineal de elementos de una matriz de cada dato es ejecutada sobre el campo de extensión predeterminado $GF(2^n)$ de 2.

Como el código de tipo Feistel utilizado aquí usa la misma capa de conversión lineal para las funciones F de todas las etapas, hay una propiedad de que una pluralidad de diferencias se cancelan simultáneamente cuando las diferencias se propagan. Como se ha explicado en el párrafo de la técnica anterior, como una técnica de criptoanálisis típica, se conoce un análisis diferencial (o técnica de descifrado de diferencia) en la que una clave de aplicación para cada función de ronda es analizada analizando muchos datos de entrada (texto sin codificar) y sus datos de salida (texto cifrado). En el tratamiento criptográfico de bloque de clave común convencional tal como el algoritmo criptográfico DES, como el tratamiento (matriz de conversión) que ha de ser aplicado en la sección de conversión lineal 122 de las funciones F 120 es ajustado para que sea equivalente en una ronda de cada etapa, es fácil realizar un análisis diferencial y como resultado proporciona una análisis fácil de una clave.

Un ejemplo en el que una pluralidad de diferencias se cancelan simultáneamente en el instante de propagación de las diferencias será explicado con referencia a la figura 4. En esta descripción, cuando se expresa una diferencia, la diferencia es indicada añadiendo un símbolo Δ (delta).

La figura 4 es un diagrama que explica la cancelación de diferencia simultánea de tres etapas en una cifra de bloque de 128 bits de m = 8 y n = 8. Nótese que en la figura, los datos de 64 bits estarán divididos por byte, cada uno será expresado como un vector, y cada elemento estará representado en sistema hexadecimal.

La cancelación de la diferencia simultánea en la función F que tiene una estructura de tres etapas, ocurre, por ejemplo, basada en un mecanismo de ajuste de los estados de datos siguientes 1-4. Los estados de datos generados por un mecanismo que será explicado más adelante son estados de datos que pueden ser generados ajustando muchos datos de entrada diferentes, es decir, esto puede ser generado analizando una clave (clave de ronda) en el denominado análisis diferencial.

(Estado 1)
Supóngase que la mitad izquierda de la diferencia de entrada a ronda i consiste de diferencias de entrada todas ceros (ΔX_{i-1} = (00, 00, 00, 00, 00, 00, 00, 00) y la mitad derecha de la misma consiste de diferencias de entrada de todas ceros excepto para una entrada solo a una caja S (ΔX_{i-1} = (34, 00, 00, 00, 00, 00, 00, 00)). Este estado de datos indica que estableciendo muchos datos de entrada diferentes, tal estado de datos puede ser obtenido en la ronda i.

Los ocho elementos en ΔX_i = (34, 00, 00, 00, 00, 00, 00, 00) corresponden a diferencias de entrada correspondientes a las m cajas S respectivas (m = 8) estructuradas en la función F. Una diferencia (34) es introducida en la primera caja S ((S1) en la figura 4), y las (00) son diferencias de entrada a las cajas segunda a octava.

Aquí, una diferencia de salida de una caja S que tiene una diferencia de entrada de cero (00) es cero (00). En tanto en cuanto estén afectados los datos de diferencia, la caja S que tiene una diferencia de entrada de cero (00) no provoca ningún efecto, siendo denominada por consiguiente una caja S que no es activa, es decir, una caja S inactiva. Por otro lado, una caja S que tiene una diferencia de entrada distinta de cero (en el ejemplo de la figura 4, diferencia = 34) genera un resultado de conversión no lineal correspondiente a la diferencia de entrada distinta de cero, siendo denominada por consiguiente una caja S activa.

En el ejemplo de la figura 4, se ha generado la diferencia de salida (b7) de una caja S activa (S1) a la que es introducida la diferencia de entrada (34) distinta de cero. Las otras cajas S inactivas S2-S8 generan diferencia de salida (00) basadas en las diferencias de entrada (00) de ceros, respectivamente, y las proporciona como entradas de diferencia de la sección de conversión lineal.

(Estado 2)
Una diferencia de salida procedente de una caja S que tiene una diferencia de entrada distinta de cero a la ronda i (en lo sucesivo denominada caja S activa) es difundida en la capa de conversión lineal, y es emitida desde la función F (valor de salida= ΔY_i), resultando una diferencia de entrada ΔX_{i+1} para la siguiente ronda, cuando lo hay.

La conversión lineal en el ejemplo de la figura 4 es tal que la conversión lineal con cierta matriz cuadrada específica 125, por ejemplo, como se ha mostrado en la figura 5, común en las funciones F de las rondas respectivas es ejecutada para emitir una diferencia ΔY_i = (98, c4, b4, d3, ac, 72, 0f, 32) como una diferencia de salida de una función F de ronda i. Como puede comprenderse a partir de la estructura de conversión lineal mostrada en la figura 5, la diferencia de salida ΔY_i = (98, c4, b4, d3, ac, 72, 0f, 32) se ha determinado como un valor que sólo depende de un elemento de salida Z [1] = b7 desde una caja S activa (S1).

Este ΔY_i = (98, c4, b4, d3, ac, 72, 0f, 32) como diferencias de salida de la función F de esta ronda i junto con las diferencias de entrada de todo ceros (ΔX_{i-1} = (00, 00, 00, 00, 00, 00, 00, 00)) son sometidas a la operación O-exclusiva (XOR) en una sección O-exclusiva 131 mostrada en la figura 4, y un resultado de la operación es proporcionado como ΔX_{i+1} a la siguiente ronda i+1.

Como los resultados de las operaciones O-exclusivas (XOR) en ΔY_i = (98, c4, b4, d3, ac, 72, 0f, 32), como diferencias de salida de la función F de ronda i, y diferencias de entrada todas ceros ΔX_{i+1} = (00, 00, 00, 00, 00, 00, 00, 00) son ΔY_i, las diferencias de entrada ΔX_{i+1} para la siguiente ronda i+1 resulta igual a ΔY_i = (98, c4, b4, d3, ac, 72, 0f, 32).

(Estado 3)
Una diferencia de salida ΔY_{i+1} de una función F de ronda i+1 tiene un valor distinto de cero sólo en una posición de la caja S activa en la ronda i. Este estado de datos indica que estableciendo muchos datos de entrada de diferencia, tal estado de datos puede ser obtenido.

Es decir, ΔX_{i+1} = (ad, 00, 00, 00, 00, 00, 00, 00), y la diferencia de salida ΔY_{i+1} tiene un valor distinto de cero en una posición de la caja S (primera caja S (S1)) que tiene un valor de diferencia distinto de cero, de modo similar con la ronda i. Casualmente, está claro que ad $\neq$ 00.

(Estado 4)
En el caso en el que una diferencia de salida de una caja S activa (S1) en la ronda i+2 concuerda con una diferencia de salida de una caja S activa (S1) en la ronda i, como se ha mostrado en la figura 4, una diferencia de salida de la caja S activa (S1) en la ronda i+2 resulta b7 y concuerda con la diferencia de salida (b7) de la caja S activa (S1). Este estado de datos indica que estableciendo muchos datos de entradas de diferencia, tal estado de datos puede ser obtenido.

Cuando este estado de datos ocurre, la diferencia de salida ΔY_{i+2} = (98, c4, b4, d3, ac, 72, 0f, 32) de una función F de ronda i+2 estará de acuerdo con la diferencia de salida ΔY_i = (98, c4, b4, d3, ac, 72, 0f, 32) de la función F de ronda i que es una ronda anterior pero una ronda.

Como resultado, una sección O-exclusiva 133 ejecutará la operación O-exclusiva en ΔX_{i+1} = ΔY_i = (98, c4, b4, d3, ac, 72, 0f, 32) y ΔY_{i+2} = (98, c4, b4, d3, ac, 72, 0f, 32), que son ambas el mismo valor, y emitirá valores de todo ceros como un resultado de la operación O-exclusiva.

Como resultado, la diferencia de entrada izquierda ΔX_{i+3} de la etapa anterior (ronda i+2) que produce la diferencia de salida a la siguiente etapa (ronda i+3) resulta ΔX_{i+3} = (00, 00, 00, 00, 00, 00, 00, 00).

La entrada izquierda ΔX_{i+3} = (00, 00, 00, 00, 00, 00, 00, 00) a esta ronda i+3 consiste de todo ceros como con la diferencia de entrada izquierda ΔX_{i-1} = (00, 00, 00, 00, 00, 00, 00, 00) a la ronda i, y existe la posibilidad de que el mismo tratamiento

que el de las rondas i a i+2 se repita también en la ronda i+3 y rondas posteriores.

Como consecuencia, se ha planteado un problema que el número de cajas S activas no aumentará en comparación con un aumento del número de ronda, y la robustez a los ataques de criptoanálisis diferencial no resultará tan mejorada.

En el código de bloque de clave común, un número mínimo de cajas S activas en la totalidad de la función criptográfica es conocido como uno de los índices de robustez al ataque de criptoanálisis diferencial. Cuanto mayor es el número mínimo de cajas S activas, mayor se ha determinado que es la resistencia a los ataques de criptoanálisis diferencial.

Como se ha descrito antes, el análisis diferencial (ataque de criptoanálisis diferencial) es una técnica para analizar una clave de aplicación en cada función de ronda estableciendo muchos datos de entradas (textos sin código) con una cierta diferencia y sus datos de salida (textos cifrados) y analizar esta correspondencia. Si el número de cajas S activas puede ser reducido en este análisis diferencial, el análisis resultará fácil y el número de procesos de análisis podrá ser reducido.

Aunque el ejemplo que se refiere a la figura 4 antes mencionada, un estado de ocurrencia de un diseño en el que sólo una primera caja S (S1) es una caja S activa, para otras cajas S (S2-S8), un ajuste en el que cada caja S es establecida para ser una caja activa es posible estableciendo datos de entrada del análisis diferencial. Por ello, realizando un proceso de análisis diferencial como este, resulta posible analizar el tratamiento de conversión no lineal de cada caja S, y además analizar una clave de ronda introducida para la función F.

Con el fin de aumentar la resistencia a análisis diferenciales como éste, es necesario mantener un estado en el que el número de cajas S activas es siempre grande, es decir, que el número mínimo de cajas S activas es grande.

En el ejemplo explicado con referencia a la figura 4, en el caso de la función F para la que se ha proporcionado una entrada en una dirección de derecha a izquierda, es decir, cuando se considera sólo la ronda i y la ronda i+2 como rondas objeto de tratamiento de cálculo de caja S activa, el número de cajas S activas es sólo dos, en las funciones F a las que las entradas son proporcionadas en una dirección de izquierda a derecha, el número de cajas S activas en la ronda i+1 es ocho, pero el número de cajas S activas resulta cero por la cancelación de diferencia simultánea, y por consiguiente el tratamiento de análisis de tratamiento de conversión no lineal de cada caja S por el análisis diferencial resulta fácil.

El algoritmo criptográfico de bloque de clave común mostrado en la figura 4 es que las matrices de conversión lineal aplicadas en las secciones de conversión lineal en rondas respectivas son iguales, y esta configuración particular conduce a la posibilidad de que la cancelación de diferencia simultánea es provocada solo por dos cajas S activas, especialmente en las funciones F a las que se ha proporcionado una entrada en una dirección de derecha a izquierda. Por tanto, hay un problema de que el número mínimo de cajas S activas no aumenta totalmente en comparación con el crecimiento del número de ronda, y la robustez a los ataques de criptoanálisis diferencial no aumenta tanto.

A continuación, de manera similar, en la configuración en la que la misma matriz de conversión lineal es utilizada para las funciones F de todas las etapas (rondas), un mecanismo de ocurrencia de la cancelación de diferencia simultánea sobre cinco rondas será explicado con referencia a la figura 6.

La figura 6 es un diagrama que explica la cancelación de diferencia simultánea de cinco etapas en un código de bloque de 128 bits de m = 8 y n = 8. Nótese que, en la figura, los datos de 64 bits serán representados como vectores dividiéndolos por un byte y cada elemento será representado en hexadecimal.

La cancelación de diferencia simultánea en la función F tiene lugar con una configuración de cinco etapas, por ejemplo, basada en el mecanismo de ajuste siguiente de los estados de datos 1-7. El estado de datos generado por un mecanismo explicado más adelante es un estado de datos que puede ser generado estableciendo muchos datos de entradas de diferencia, y el estado de datos puede ser generado analizando una clave (clave de ronda) en el denominado análisis diferencial.

(Estado 1)
Dejar una mitad izquierda de diferencias de entrada para la ronda i consiste de diferencias de entrada de todo ceros (ΔX_{i-1} = (00, 00, 00, 00, 00, 00, 00, 00)) y una mitad derecha de diferencias de entrada consiste de diferencias de entrada todas ceros excepto para una entrada solo a una caja S (ΔX_i = (34, 00, 00, 00, 00, 00, 00)). Este estado de datos indica que estableciendo muchos datos de entrada de diferencia, tal estado de datos puede ser obtenido en la ronda i.

Ocho elementos de ΔX_i = (34, 00, 00, 00, 00, 00, 00, 00) corresponden a diferencias de entrada respectivas para m (m = 8) cajas S establecidas en las funciones F. (34) es introducida en una primera caja S ((S1) en la figura 6), y los (00) son diferencias de entrada a las cajas segunda a octava.

Como se ha descrito antes, cualquier diferencia de salida de la caja S que tiene una diferencia de entrada de cero (00) es

cero (00). En tanto en cuanto la diferencia de salida es afectada, la caja S que tiene una diferencia de entrada de cero no ejecuta ninguna operación, siendo denominada por consiguiente una caja S que no es activa, particularmente una caja S inactiva. Por otro lado, como sólo una caja S (S1) con una diferencia de entrada distinta de cero (en el ejemplo de la figura 6, diferencia = 34) genera un resultado de conversión no lineal correspondiente a la diferencia de entrada distinta de cero como una diferencia de salida, es denominada por consiguiente una caja S activa.

En el ejemplo de la figura 6, una caja S activa (S1) a la que se ha introducido una diferencia de entrada (34) distinta de cero genera una diferencia de salida (b7), y otras cajas S2-S8 inactivas generan diferencias de salida (00) basadas en las diferencias de entrada (00) de ceros, que están asignadas como entradas de diferencia de la sección de conversión lineal.

(Estado 2)
Una diferencia de salida de una caja S (en lo que sigue denominada una caja S activa) que tiene una diferencia de entrada distinta de cero para la ronda i (en el ejemplo de la figura 4, diferencia = 34) es difundida en la capa de conversión lineal, y emitida desde la función F (valor de salida = ΔY_i), resultando una diferencia de entrada ΔX_{i+1} para la siguiente ronda, cuando lo hay.

En el ejemplo de la figura 6, la conversión linear es ejecutada con cierta matriz cuadrada específica 125 que es común a cada ronda, por ejemplo, que está mostrada en la figura 5, y ΔY_i = (98, c4, b4, d3, ac, 72, 0f, 32) como una diferencia de salida de la función F de ronda i es emitida s.

ΔY_i = (98, c4, b4, d3, ac, 72, 0f, 32), como diferencia de salida de la función F de ronda i, es sometida a las operaciones O-exclusiva (XOR) en la sección O-exclusiva 141 mostrada en la figura 6 junto con diferencia de entrada todas ceros (ΔX_{i-1} = (00, 00, 00, 00, 00, 00, 00, 00)), y los resultados de la operación resultan diferencias de entrada para la siguiente ronda i+1.

Como los resultados de las operaciones O-exclusivas (XOR) en ΔY_i = (98, c4, b4, d3, ac, 72, 0f, 32), como diferencias de salida de la función F de ronda i, y diferencias de entrada de todo ceros (ΔX_{i-1} = (00, 00, 00, 00, 00, 00, 00, 00)) son ΔY_i, diferencias de entrada a la siguiente ronda i+1 resultan $\Delta X_{i+1} = \Delta Y_i$ = (98, c4, b4, d3, ac, 72, 0f, 32).

(Estado 3)
Una diferencia de salida ΔY_{i+1} de la función F de ronda i+1 tiene un valor distinto de cero sólo en una posición de la caja S activa en la ronda i. Este estado de datos indica que estableciendo muchos datos de entradas de diferencia, puede obtenerse tal estado de datos.

Es decir, ΔY_{i+1} es ΔY_{i+1} = (34, 00, 00, 00, 00, 00, 00, 00), y tiene un valor distinto de cero sólo en una posición de la caja S (una primera caja S (S1)) que tiene un valor de diferencia distinto de cero (en el ejemplo de la figura 6, diferencia = 34) como con la ronda i.

(Estado 4)
Una entrada a la función F de ronda i+2 es un resultado de la operación O-exclusiva en la sección O-exclusiva 142 en ΔX_i = (34, 00, 00, 00, 00, 00, 00, 00) y ΔY_{i+1} = (34, 00, 00, 00, 00, 00, 00, 00), que son ambos los mismos datos, y resulta una entrada que consiste toda de ceros, ΔX_{i+2} = (00, 00, 00, 00, 00, 00, 00, 00) . Como resultado, una diferencia de salida desde la función F de ronda i+2 también resulta una diferencia de salida que consiste toda de ceros, ΔY_{i+2} = (00, 00, 00, 00, 00, 00, 00, 00).

(Estado 5)
Las entradas a una función F de ronda i+3 son resultados de las operaciones O-exclusivas en la sección O-exclusiva 143 en ΔX_{i+1} = (98, c4, b4, d3, ac, 72, 0f, 32) y ΔY_{i+2} = (00, 00, 00, 00, 00, 00, 00, 00), que son diferencias de salida de la función F de ronda i+2 de todo ceros, y resultan entradas $\Delta X_{i+3} = \Delta X_{i+1}$ = (98, c4, b4, d3, ac, 72, 0f, 32) para la función F de ronda i+3.

(Estado 6)
Las diferencias de salida de la función F de ronda i+3 resultan ΔY_{i+3} = (43, 00, 00, 00, 00, 00, 00, 00). Las operaciones O-exclusivas en la sección O-exclusiva 144 en estas diferencias junto con ΔX_{i+2} = (00, 00, 00, 00, 00, 00, 00, 00) que consiste toda de ceros resulta en $\Delta X_{i+4} = \Delta X_{i+3}$ = (43, 00, 00, 00, 00, 00, 00, 00), que resulta diferencias de entrada de la función F de ronda i+4.

(Estado 7)
Cuando una diferencia de salida de una caja S activa (S1) en la ronda i+4 está de acuerdo con una diferencia de salida de la caja S activa (S1) en la ronda i, una diferencia de salida de la caja S activa (S1) en la ronda i+4 resulta b7, como se ha mostrado en la figura 6, y está de acuerdo con una diferencia de salida (b7) de la caja S activa (S1) en la ronda i. Este

estado de datos indica que estableciendo muchos datos de entradas de diferencia, puede obtenerse tal estado de datos.

Cuando este estado de datos ocurre, la diferencia de salida ΔY_{i+4} = (98, c4, b4, d3, ac, 72, 0f, 32) de una función F de ronda i+4 estará de acuerdo con la diferencia de salida ΔX_{i+3} = (98, c4, b4, d3, ac, 72, 0f, 32) de la sección O-exclusiva 143 de ronda i+2 que es una ronda anterior, pero una.

Como resultado, en la sección O-exclusiva 145, ΔX_{i+3} = (98, c4, b4, d3, ac, 72, 0f, 32) y ΔY_{i+4} (98, c4, b4, d3, ac, 72, 0f, 32), que son ambos el mismo valor, serán sometidos a la operación O-exclusiva, emitiendo valores de todo ceros como un resultado de la operación O-exclusiva.

Por consiguiente, las diferencias de entrada a la siguiente etapa (ronda i+5) son establecidas como ΔX_{i+5} = (00, 00, 00, 00, 00, 00, 00, 00).

Esta entrada izquierda a esta ronda i+5, ΔX_{i+5} = (00, 00, 00, 00, 00, 00, 00, 00) consiste de todo ceros como con la entrada izquierda a la ronda i, ΔX_{i-1} = (00, 00, 00, 00, 00, 00, 00, 00), y existe la posibilidad de que se repetirá el mismo tratamiento como de la ronda i a la ronda i+4 también en la ronda i+5 y en rondas posteriores.

Por consiguiente, un problema es que el número de cajas S activas no aumenta en comparación con el aumento del número de ronda, y la robustez a los ataques de criptoanálisis diferencial no aumenta tanto.

Como se ha descrito antes, el análisis diferencial (ataque de criptoanálisis diferencial) es una técnica para analizar una clave de aplicación en cada función de ronda estableciendo muchos datos de entrada (texto sin codificar) que tienen una cierta diferencia y sus datos de salida (texto cifrado) y analizar esta correspondencia. En este análisis diferencial si el número de cajas S activas puede ser reducido, el análisis resultará fácil y el número de procesos de análisis podrá ser acortado.

En el ejemplo con referencia a la figura 6 antes descrito, en el caso de las funciones F a las que se han proporcionado entradas en una dirección de derecha a izquierda, es decir, en el caso en el que la ronda i, ronda i+2, y ronda i+4 han sido considerados como rondas objetivo de cálculo de caja S activa, el número de cajas S activas es sólo dos, una suma de ronda i = 1, ronda i+2 = 0, y ronda i+4 = 1. En el caso de las funciones F a las que se han proporcionado las entradas en una dirección de izquierda a derecha, es decir, en el caso en el que la ronda i+1 y la ronda i+3 son considerados como rondas objetivo, aunque el número de cajas S activas es ocho, el número de cajas S activas en la ronda i+5 resulta cero debido a la cancelación de diferencia simultánea; por lo tanto, el análisis del tratamiento de conversión no lineal de cada caja S por análisis diferencial y tratamiento de criptoanálisis de una clave de ronda de entrada para la función F resulta relativamente fácil.

Aunque el ejemplo con referencia a la figura 6 presenta un estado de ocurrencia de un diseño en el que sólo la primera caja S (S1) es una caja S activa, con respecto a otras cajas S (S2 a S8), establecer los datos de entrada de análisis diferencial permite a cualquiera de las otras cajas S ser establecida como una caja S activa, por lo tanto, la ejecución de tal proceso de análisis diferencial hará posible analizar el tratamiento de conversión no lineal de cada caja S y además analizar la clave de ronda introducida en la función F.

Aunque el ejemplo de ocurrencia de la cancelación de diferencia simultánea en los casos de tres y cinco rondas se ha explicado con referencia a la figura 4 y a la figura 6, si estos casos son generalizados para que el número de ronda arbitrario defina la cancelación de diferencia simultánea, la definición puede ser dada como sigue. Con referencia a la figura 7, se explicará la definición de la cancelación de diferencia simultánea en un número de ronda arbitrario. La figura 7 muestra rondas en serie, pero uno (i, i+2, i+4, ..., i+2j) de la estructura Feistel que realiza el tratamiento criptográfico de bloque de clave común de la estructura Feistel.

"Definición"
En un proceso en el que una mitad de las diferencias de entrada de la estructura Feistel en la ronda i consiste de ceros (en la figura 7, ΔX_i = (00, 00, 00, 00, 00, 00, 00, 00) y cada uno de ellos y cada una de las diferencias de salida de la función F de ronda i+2j son sometidos a la operación O-exclusiva en la sección O-exclusiva, un caso en el que los resultados de la operación O-exclusiva resultan ceros (en la figura 7, ΔX_{i+2j+1} = (00, 00, 00, 00, 00, 00, 00, 00) es denominado la cancelación de diferencia simultánea.

En este instante, las cajas S activas que existen en las funciones F de rondas i, i+2, i+4, ... i+2k son denominadas cajas S activas que causan la cancelación de diferencia simultánea. Definiendo el número de elementos distintos de cero de un vector A como Peso Hamming hw (A), el número "a" de cajas S activas que causa la cancelación de diferencia simultánea puede ser expresado por la siguiente ecuación.

[Ecuación 1]

$$a = \sum_{j=0}^{k} hw(\Delta X_{i+2j})$$

En los ejemplos de tres rondas y cinco rondas descritos con anterioridad, el número de cajas S activas que causa la cancelación de diferencia simultánea es dos, es decir, a = 2.

Como se ha descrito antes, uno de los índices de robustez a ataques de criptoanálisis diferencial en el código de bloque de clave común es el número mínimo de cajas S activas en la totalidad de las funciones criptográficas, y se ha determinado que cuanto mayor es el número mínimo de cajas S activas, más elevada resulta la resistencia a ataques de criptoanálisis diferencial.

Sin embargo, en la configuración en la que la misma matriz de conversión lineal es utilizada para las funciones F de todas las etapas como en el algoritmo DES, existe la posibilidad de que sólo dos cajas S activas causen la cancelación de diferencia simultánea, como puede comprenderse a partir de la explicación con referencia a la figura 4 y a la figura 6. Existe un problema de que debido a la presencia de tal propiedad, el número mínimo de cajas S activas no aumenta lo suficiente y la robustez a ataques de criptoanálisis diferencial no se ha reforzado tanto.

[2. Tratamiento de análisis lineal en algoritmo criptográfico de bloque de clave común]
El tratamiento de análisis diferencial, como se ha descrito antes, requiere un ejecutor del análisis para preparar datos de entrada (texto sin codificar) que tiene una diferencia constante y analizar sus datos de salida correspondientes (texto cifrado). Para tratamiento de análisis lineal, no es necesario preparar datos de entrada (texto sin codificar) con una diferencia constante y el análisis es ejecutado basado en datos de entrada (texto sin codificar) cuya cantidad es igual o mayor que una cantidad predeterminada y sus datos de salida correspondientes (texto cifrado).

Como se ha descrito antes, en el algoritmo criptográfico de bloque de clave común, cajas S como la sección de conversión no lineal son preparadas y no hay relación lineal entre los datos de entrada (texto sin codificar) y sus datos de salida correspondientes (texto cifrado). En el análisis lineal, el análisis es realizado por aproximación lineal de la entrada/salida de esta caja S, analizando una relación lineal entre muchos datos de entrada (texto sin codificar) y valores de bit constituyentes de los datos de salida correspondientes (texto cifrado), y estrechando hacia abajo las claves que son asumidas como candidatas. En el análisis lineal, no es necesario preparar datos de entrada con una diferencia específica, y el análisis resulta posible preparando sólo un gran número de textos sin formato y sus textos cifrados correspondientes.

[3. Algoritmo criptográfico basado en este invento]
A continuación, se explicará un algoritmo criptográfico de este invento. El algoritmo criptográfico de este invento tiene una estructura que mejora la resistencia a ataques de criptoanálisis lineal, ataques de criptoanálisis diferencial descritos con anterioridad, y similares, es decir, que tiene una estructura que mejora la dificultad en el análisis de clave y mejora la seguridad.

Una de las características del algoritmo criptográfico relativo a este invento es que el algoritmo es construido estableciendo una pluralidad de matrices MDS (Separable por Distancia Máxima) cuadradas en vez de una estructura en la que un tratamiento común (matriz de conversión) es aplicada a la sección de conversión lineal de una función F de cada ronda como con el algoritmo DES convencional. Específicamente, el algoritmo está configurado para realizar un tratamiento de conversión no lineal aplicando matrices MDS cuadradas que son diferentes al menos en las rondas consecutivas de numeración par y en las rondas consecutivas de numeración impar.

El algoritmo criptográfico relativo a este invento pone en práctica una estructura con la que la cancelación de diferencia simultánea basada en un número pequeño de cajas S activas no ocurre o es menos propensa a ocurrir utilizando propiedades de las matrices MDS (Separables por Distancia Máxima) cuadradas, de modo que el número mínimo de cajas S activas es ampliado y el tratamiento criptográfico de bloque de clave común más robusto a los ataques de criptoanálisis diferencial es realizado. Alternativamente, este invento pone en práctica una estructura con la que aumenta la dificultad de un análisis lineal que es ejecutado como un ataque de criptoanálisis de texto sin codificar conocido.

El algoritmo criptográfico de este invento aplica una estructura criptográfica de bloque de clave común típica que es denominada estructura Feistel que tiene funciones F de tipo SPN explicadas con referencia a las figuras 1 y 2, es decir, aplica una estructura que convierte un texto sin codificar en un texto cifrado o convierte un texto cifrado en un texto sin codificar por simple repetición de la función F de tipo SPN que tiene la sección de conversión no lineal y la sección de conversión lineal sobre una pluralidad de rondas.

Por ejemplo, la longitud de un texto sin codificar se ha asumido como 2 mn bits (aquí, siendo m y n números enteros). La estructura divide un texto sin codificar de 2 mn bits en dos datos PL (Perfil-izquierdo y Perfil-derecho) cada uno de mn bits, y ejecuta la función F en cada ronda utilizándolos como valores de entrada. La función F es una función F con un tipo SPN que consiste de la sección de conversión no lineal compuesta de cajas S y la sección de conversión lineal conectadas juntas.

En la configuración de este invento, cuando una matriz para el tratamiento de conversión lineal ha de ser aplicada en la sección de conversión lineal en la función F, la matrices seleccionadas a partir de una pluralidad de diferentes matrices MDS (Separables por Distancia Máxima) cuadradas son establecidas como matrices que han de ser aplicadas en las secciones de conversión lineal de las funciones F de rondas respectivas. Específicamente, se aplican matrices MDS cuadradas que son diferentes al menos en las rondas consecutivas de número par y en las rondas consecutivas de número impar.

La matriz MDS cuadrada será explicada. La matriz cuadrada es una matriz que satisface las propiedades de (a) y (b) de más abajo. (a) La matriz es una matriz cuadrada. (b) Los determinantes de todas las submatrices incluidas en una matriz no son cero, en particular det (submatriz) $\neq 0$.

La matriz que satisface las condiciones de los anteriores (a) y (b) es denominada matriz MDS cuadrada. Las longitudes de los bits de entrada/salida a la función F que son ejecutadas en cada ronda del tratamiento criptográfico de bloque de clave común es mxn bit (m, n: número entero). La figura 8 muestra un ejemplo de la matriz MDS cuadrada en el caso en que la sección de conversión no lineal establecida en la función F está construida con m cajas S cada una de las cuales tiene entrada/salida de n bits, y la sección de conversión no lineal ejecuta el tratamiento de conversión lineal basado en matrices cuadradas emésimas cada una de las cuales tiene elementos en el campo de extensión GF (2^n) de 2 definidos por un polinomio irreducible enésimo como sus elementos. Un ejemplo de la matriz MDS cuadrada mostrada en la figura 8 es un ejemplo de la matriz MDS cuadrada de n = 8 y m = 8.

Designando el número de elementos distintos de cero en el vector A por peso Hamming hw(A), una matriz MDS cuadrada emésima por M, y un vector de entrada a la matriz MDS cuadrada M por x, una matriz MDS cuadrada que satisface las anteriores (a) y (b) satisface la desigualdad siguiente (Ecuación 1).

$$hw(x) + hw(M_x) \geq m+1 \quad \text{..... (Ecuación 1)}$$

La expresión (Ecuación 1) antes mencionada indica que el total del número de elementos hw(x) distintos de cero de los datos de entrada x que han de ser convertidos linealmente con la matriz MDS cuadrada (M) más el número de elementos $hw(M_x)$ distintos de cero de los datos de salida M_x que fueron convertidos linealmente con la matriz MDS cuadrada (M) es mayor que el número de orden m de la matriz MDS cuadrada.

Incidentalmente, el nombre de la matriz MDS cuadrada es proporcionado debido a que una mitad derecha de una forma estándar de una matriz de generación del código-MDS (Código Separable por Distancia Máxima) cuadrado satisface las condiciones antes mencionadas.

Es sabido que, incluso en la configuración convencional en la que se ha incorporado una única matriz en todas las funciones F, la utilización de una matriz MDS cuadrada como una matriz de conversión lineal permite que el número mínimo de cajas S activas sea mantenido a un nivel relativamente elevado comparado con un caso en el que se ha utilizado una matriz diferente de la matriz MDS cuadrada.

Este invento propone un método para utilizar una matriz que satisfaga las condiciones de la matriz MDS cuadrada para la función F de cada ronda y además establecer diferentes matrices para rondas respectivas. Específicamente, son aplicadas matrices MDS cuadradas que son diferentes al menos en las rondas consecutivas de número par y en las rondas consecutivas de número impar.

Se explicará a continuación una pluralidad de ejemplos de configuraciones en cada uno de los cuales la resistencia a ataques de criptoanálisis diferencial es hecha más elevada en el código de bloque de clave común de tipo Feistel de número de etapa 2r (siendo r un número entero).

En la explicación siguiente, MLT_j indica la matriz de conversión lineal que ha de ser aplicada en la sección de conversión lineal de la función F de la etapa j-ésima en la estructura de bloque de clave común de tipo Feistel de número de etapa 2r (número de ronda).

En la configuración de este invento, como una matriz para tratamiento de conversión lineal que ha de ser aplicada en la sección de conversión lineal de la función F de cada etapa en la estructura criptográfica de bloque de clave común de tipo Feistel de número de etapa 2r (número de ronda), matrices seleccionadas de una pluralidad de diferentes matrices MDS

(Separables por Máxima Distancia) cuadradas son establecidas como matrices que han de ser aplicadas en las secciones de conversión lineal de las funciones F de rondas respectivas. Específicamente, son aplicadas matrices MDS cuadradas que son diferentes al menos en las rondas consecutivas de número par y en las rondas consecutivas de número impar.

Específicamente, conforme a la estructura criptográfica de bloque de clave común de número de etapa (número de ronda) 2r, se han generado q matrices MDS cuadradas L_1, L_2, ..., L_q ($q \leq r$). A continuación, como matrices para el tratamiento de conversión lineal que ha de ser aplicado en las secciones de conversión lineal en las funciones F de etapas de número impar en la estructura criptográfica de bloque de clave común de tipo Feistel de número de etapa (número de ronda) 2r, q matrices MDS cuadradas son establecidas repetidamente designando L_q, L_1, L_2, ... desde su etapa superior de las funciones F. Además, para las funciones F de etapas de número par, q matrices MDS cuadradas son establecidas repetidamente designando L_1, L_2, ..., L_q, L_1, L_2, ... desde su etapa inferior de las funciones F.

La figura 9 muestra un ejemplo de configuración al que se ha aplicado esta configuración. Como un ejemplo de configuración en el que están dispuestos tres tipos de matrices MDS cuadradas diferentes en la estructura criptográfica de bloque de clave común de tipo Feistel de q = 3, en particular el número de ronda 12 en el caso en el que se ha definido una estructura como la estructura criptográfica de bloque de clave común de tipo Feistel de número de etapa (número de ronda) 2r = 12, en particular r = 6, se han mostrado en la figura 9 las matrices MDS cuadradas (L_1, L_2. L_3) que han de ser establecidas en las secciones de conversión lineal de las funciones F en rondas respectivas.

La configuración de la figura 9 es una estructura que divide un texto sin codificar de 2 mn bit en dos datos de PL (Perfil-Izquierdo) y PR (Perfil-Derecho) cada uno de mn bit, y ejecuta una Función F en cada ronda utilizándolos como valores de entrada. La función F de la primera ronda así como las funciones F de otras rondas son funciones F cada una con el tipo SPN consistente de la sección de conversión no lineal compuesta de cajas S y la sección de conversión lineal conectadas juntas.

El ejemplo de configuración de la figura 9 es de r = 6 y q = 3, dónde un símbolo L_n mostrado en cada función F indica una matriz MDS cuadrada 402. Es decir, L_1, L_2. y L_3 indican tres clases de matrices MDS cuadradas diferentes, cada una de las cuales es una matriz MDS cuadrada que ha de ser aplicada al tratamiento de conversión lineal en la sección de conversión de cada función F.

Una secuencia de tratamiento de configuración de la matriz de conversión lineal MLT_j será explicada con referencia a la figura 10.

[Operación S21]
Un número q igual o menor que una mitad r del número de ronda 2r, en particular se ha seleccionado q que satisface $q \leq r$. Aquí, q es un entero de dos o más.

[Operación S22]
Se generan q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q en GF (2^n). Detalles de las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q en GF (2^n) serán explicadas en un párrafo posterior.
Después las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q en GF(2^n) son generadas en la Operación S22, el tratamiento de configuración de la matriz MDS cuadrada es ejecutado a continuación.

[Operación S23]
La matriz de conversión lineal MLT_{2i-1} de número de etapa 2i-1 ($1 \leq i \leq r$) es establecida a $L_{(i-1 \bmod q)+1}$.

[Operación S24]
La matriz de conversión lineal MLT_{2j} de número de etapa 2i ($1 \leq i \leq r$) es establecida a $MLT_{2r-2i+1}$.

Por ejemplo, en el caso en una configuración ejemplar mostrada en la figura 9, es decir, en el caso en el que el aparato de tratamiento criptográfico tiene 12 etapas (r = 6) y q = 3, la configuración será:

$MLT_1 = L_1$, $MLT_2 = L_3$, $MLT_3 = L_2$, $MLT_4 = L_2$, $MLT_5 = L_3$, $MLT_6 = L_1$, $MLT_7 = L_1$, $MLT_8 = L_3$, $MLT_9 = L_2$, $MLT_{10} = L_2$, $MLT_{11} = L_3$, $MLT_{12} = L_1$.

Así, el aparato de tratamiento criptográfico de este invento utiliza la siguiente estructura. Conforme a la estructura criptográfica de bloque de clave común de tipo Feistel de número de etapa (número de ronda) 2r, se generan q matrices MDS cuadradas, en las que $q \leq r$. Para las funciones F de etapas de número impar, q matrices MDS cuadradas son establecidas repetidamente designando L_1, L_2, ..., L_q, L_1, L_2, ... secuencialmente desde la función F de la etapa superior, y para las funciones F de etapas de número par, q matrices MDS cuadradas son establecidas repetidamente designando L_1, L_2, ..., L_q, L_1, L_2, ... secuencialmente desde la función F de la etapa inferior.

A continuación, se explicarán los detalles de las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q en GF(2^n) en la Operación S22 en el flujo de tratamiento de la figura 10 y configurándolas a las funciones F. La explicación será dada a lo largo de los artículos siguientes.

(3-a) Ejemplo de generación de matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis diferencial y configurándolas a las funciones F
(3-b) Ejemplo de generación de matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis lineal y configurándolas a las funciones F
(3-c) Ejemplo de generación de matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis diferencial y ataques de criptoanálisis lineal, y configurándolas a las funciones F.

(3-a) Ejemplo de generación de matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis diferencial y configurándolas a las funciones F. En primer lugar, como un ejemplo de generación de matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis diferencial y configurándolas a las funciones F, se explicarán tres ejemplos de tratamiento a2, a2, y a3.

(Ejemplo de tratamiento a1)
Se explicará un primer ejemplo de generación de matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis diferencial y configurándolas a las funciones F. En primer lugar, la explicación será dada para el tratamiento de generación de una matriz MDS cuadrada con referencia a un diagrama de flujo mostrado en la figura 11.

[Operación S101]
Designar entrada: el número de matrices MDS cuadradas necesarias por q, un orden de extensión por n, y un tamaño de matriz por m, las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q son generadas aleatoriamente en GF(2^n). El diagrama de flujo mostrado en la figura 11 muestra un ejemplo de tratamiento como con el número de matrices MDS q = 6, el orden de extensión n = 8, y el tamaño de matriz m = 8.

[Operación S102]
Se ha comprobado si vectores de columna qm arbitrarios sacados de los qm vectores de columna incluidos en las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q son independientes linealmente. Si el flujo ha pasado la comprobación, el flujo prosigue a la Operación S103; si no lo ha hecho, el flujo vuelve a la Operación S101.

[Operación S103]
Las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q son emitidas como matrices MDS cuadradas que han de ser aplicadas al código de bloque de clave común de tipo Feistel de número de ronda 2r.

Mediante el proceso anterior, se generan las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q. Aquí, q satisface $q \leq r$.

Las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q generadas de este modo son establecidas como matrices que han de ser aplicadas al tratamiento de conversión lineal en la sección de conversión lineal de la función F de cada etapa en la estructura criptográfica de bloque de clave común de tipo Feistel de número de etapa (número de ronda) 2r, de acuerdo con el tratamiento de [Operación S23] y [Operación S24] explicados previamente con referencia a la figura 10. Es decir, para etapas de número impar, q matrices MDS cuadradas son designadas como L_1, L_2, ..., L_q, L_1, L_2, ... secuencialmente y repetidamente a partir de la función F de la etapa superior, y para etapas de número par, q matrices MDS cuadradas son designadas como L_1, L_2, ..., L_q, L_1, L_2, ... secuencial y repetidamente desde la función F de la etapa inferior.

Así, las matrices MDS cuadradas de rondas de número par y las matrices MDS cuadradas de rondas de número par están dispuestas en órdenes mutuamente inversos, respectivamente, por lo que se garantiza que el tratamiento de cifrado y el tratamiento de descifrado son iguales excepto para el tratamiento de reemplazar una secuencia de claves.

Esta configuración garantiza lo siguiente. (a) La matriz de conversión lineal de cada función F es una MDS cuadrada. (b) m vectores de columna arbitrarios de las matrices de conversión lineal incluidos en al menos q funciones F consecutivas y rondas de número impar en una función criptográfica son linealmente independientes. (c) m vectores de columna arbitrarios de las matrices de conversión lineal incluidos en al menos q funciones F consecutivas en rondas de número par son linealmente independientes. Como se garantiza el respeto a (a) y (c), se garantiza que, en la estructura criptográfica de bloque de clave común de tipo Feistel que tiene una pluralidad de rondas, no tiene lugar la cancelación de diferencia simultánea por contribución de m cajas S o menos activas. Por lo tanto, aumentará el valor mínimo del número de cajas S activas en la totalidad de la función criptográfica.

Así, este ejemplo de tratamiento hace posible ampliar el número mínimo de cajas S activas en la totalidad de la función criptográfica que es uno de los índices de robustez a ataques de criptoanálisis de diferencia en el código de bloque de clave común. Como resultado, aumentará el número de cajas S activas cuando el análisis diferencial (ataque de

criptoanálisis diferencial) es intentado y la dificultad en el análisis será mejorada. Por lo tanto, se produce el tratamiento criptográfico de alta seguridad cuya clave es difícil de analizar.

(Ejemplo de tratamiento a2)

Se explicará un segundo ejemplo de generación de matrices cuadradas MDS que produce una resistencia mejorada a ataques de criptoanálisis diferencial y configurándolas a las funciones F. El tratamiento de generación de las matrices MDS cuadradas será explicado con referencia al diagrama de flujo de la figura 12.

[Operación S201]

Designación de entrada: el número de matrices MDS necesarias por q, el orden de extensión por n, y el tamaño de matriz por m, las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q son generadas aleatoriamente en $GF(2^n)$. El diagrama de flujo mostrado en la figura 12 muestra un ejemplo de tratamiento como con el número de matrices MDS q = 6, el orden de extensión n = 8, y el tamaño de matriz m = 8.

[Operación S202]

Se ha comprobado si una matriz compuesta de m columnas seleccionada arbitrariamente de qm columnas incluidas en las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q es una MDS cuadrada. Si el flujo ha pasado la comprobación, el flujo prosigue a la Operación S203; si no, el flujo vuelve a la Operación S201. Aquí, la matriz MDS cuadrada significa una matriz que satisface las propiedades siguientes, como se ha descrito antes. (a) Es una matriz cuadrada. (b) Los determinantes de todas las submatrices incluidas en la matriz no son cero, es decir, det(submatriz) $\neq 0$.

[Operación S203]

Las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q son emitidas como matrices MDS cuadradas que han de ser aplicadas al código de bloque de clave común de tipo Feistel de número de ronda 2r.

Mediante el proceso anterior, son generadas las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q. Aquí, q satisface $q \leq r$.

En el tratamiento de generación de la matriz MDS cuadrada en el ejemplo a1 de tratamiento antes mencionado, como se ha explicado en la secuencia de tratamiento de la figura 11, se ha determinado la independencia lineal de una matriz compuesta de m columnas arbitrarias sacadas de las qm columnas incluidas en las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q en la Operación S102. En el tratamiento de generación de matriz MDS cuadrada en este ejemplo a2 de tratamiento, se ha comprobado si una matriz compuesta de m columnas arbitrarias sacadas de las qm columnas incluidas en las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q es una matriz MDS cuadrada. Es decir, se ejecutará una comprobación más severa.

De manera similar al ejemplo a1 de tratamiento explicado con anterioridad, las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q generadas por el tratamiento de generación de la matriz MDS cuadrada que ha seguido una secuencia de tratamiento mostrada en esta figura 12 son establecidas como matrices que han de ser aplicadas al tratamiento de conversión lineal de las secciones de conversión lineal de las funciones F de etapas respectivas en la estructura criptográfica de bloque de clave común de tipo Feistel de número de etapa (número de ronda) 2r, de acuerdo con el tratamiento de [Operación S23] y [Operación S24] explicado previamente con referencia a la figura 10. Es decir, para etapas de número impar, q matrices MDS cuadradas han sido designadas repetidamente como L_1, L_2, ..., L_q, L_1, L_2, ... secuencialmente desde la función F de la etapa superior, y para etapas de número par, q matrices MDS cuadradas son designadas repetidamente como L_1, L_2, ..., L_q, L_1, L_2, ... secuencialmente desde la función F de la etapa inferior.

Así, las matrices MDS cuadradas de las rondas de número par y las matrices MDS cuadradas de las rondas de número par están dispuestas en órdenes mutuamente inversos, respectivamente, por lo que se garantiza que el tratamiento de cifrado y el tratamiento de descifrado son los mismos excepto para el tratamiento de reemplazar una secuencia de claves.

Esta configuración garantiza lo siguiente:

(a) La matriz de conversión lineal de cada función F es una MDS cuadrada.
(b) m vectores de columna arbitrarios de las matrices de conversión lineal incluidos en al menos q funciones F consecutivas en rondas de número impar constituyen una matriz MDS cuadrada.
(c) m vectores de columna arbitrarios de las matrices de conversión lineal incluidas en al menos q funciones F consecutivas en rondas de número par constituyen una matriz MDS cuadrada.

Por ello, en la estructura criptográfica de bloque de clave común de tipo Feistel con número de ronda de una pluralidad de etapas, se garantiza que la cancelación de diferencia simultánea por contribución de m cajas S activas o menos no ocurre en las rondas 2q-1 consecutivas. Además, se garantiza lo siguiente.

(d) El número de elementos distintos de cero en los valores de diferencia obtenidos por contribución de "a" ($a \leq m$) cajas S activas resulta m+1-a o más, a partir de la propiedad de la matriz MDS cuadrada. Por lo tanto, el valor mínimo del número de cajas S activas en la totalidad de la función criptográfica aumenta.

Así, por este ejemplo de tratamiento, resulta posible ampliar el número mínimo de cajas S activas en la totalidad de la función criptográfica que es uno de los índices de robustez a ataques de criptoanálisis diferencial en el código de bloque de clave común, y como resultado el número de cajas S activas en el caso en que se intente el análisis diferencial (ataque de criptoanálisis diferencial) aumentará y se mejorará la dificultad en el análisis. Por tanto, se produce el tratamiento criptográfico de alta seguridad cuya clave es difícil de analizar.

(Ejemplo de tratamiento a3)
Se explicará el tercer ejemplo de generación de matrices MDS cuadradas que produce una resistencia mejorada a ataques de criptoanálisis diferencial y las configura a las funciones F. El tratamiento de generación de matrices MDS cuadradas será explicado con referencia al diagrama de flujo de la figura 13.

[Operación S301]
Designación de entrada: el número de matrices MDS necesarias por q, el orden de extensión por n, y el tamaño de matriz por m, una q matriz MDS cuadrada emésima es generada en GF (2^n). El diagrama de flujo mostrado en la figura 1 muestra un ejemplo de tratamiento como con el número de matrices MDS q = 6, el orden de extensión n = 8, y el tamaño de matriz m = 8.

[Operación S302]
m filas son seleccionadas y extraídas arbitrariamente de una matriz MDS cuadrada emésima M y una matriz M' de m-filas y qm-columnas es compuesta.

[Operación S303]
Los qm vectores de columna incluidos en la matriz M' de m filas y qm columnas son divididos arbitrariamente en q grupos cada uno compuesto de m vectores de columna sin presencia de ningún vector de columna en dos o más grupos. Las matrices cuadradas emésimas L_1, L_2, ..., L_q son emitidas a partir de los vectores de columna incluidos en los grupos respectivos como matrices MDS cuadradas que han de aplicarse al código de bloque de clave común de tipo Feistel de número de ronda 2r.

Mediante el proceso anterior, se generan las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q. Aquí, q satisface $q \leq r$.

La técnica 3 e generación de matriz MDS cuadrada en el ejemplo a3 de tratamiento será explicada más concretamente con referencia a la figura 14.

[Operación S301]
Una q matriz MDS cuadrada emésima M es generada en GF (2^n). Como se ha mostrado en la figura 14, una matriz MDS cuadrada M de qmxqm ha sido generada. Nótese que el orden de la matriz M generada en esta operación S301 puede ser mayor que qm (orden).

[Operación S302]
Como se ha mostrado en la figura 14, m columnas seleccionadas y extraídas arbitrariamente de la q matriz MDS cuadrada M emésima y una matriz M' de m filas y qm columnas es compuesta. Nótese que aunque el ejemplo en la figura se ha mostrado como un ejemplo en el que m filas consecutivas son seleccionadas y extraídas, una matriz M' de m filas y qm columnas puede ser compuesta seleccionando y extrayendo m filas arbitrarias que tienen un espacio o tolerancia entre ellas que constituirá la matriz MDS cuadrada emésima M.

[Operación S303]
qm vectores de columna incluidos en la matriz M' de m filas y qm columnas son divididos en x grupos que tienen cada uno m vectores de columna sin presencia de ningún vector de columna en dos o más grupos, y matrices cuadradas emésimas L_1, L_2, ..., L_x son generadas a partir de los vectores de columna incluidos en grupos respectivos.

Como los ejemplos de tratamiento a1 y a2 explicados previamente, las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q, generadas por el tratamiento de generación de matriz MDS cuadrada que han seguido una secuencia de tratamiento explicada con referencia a las figuras 13 y 14 son establecidas como matrices que han de ser aplicadas al tratamiento de conversión lineal de las secciones de conversión lineal de las funciones F de etapas respectivas en la estructura criptográfica de bloque de clave común de tipo Feistel de número de etapa (número de ronda) 2r, de acuerdo con el tratamiento de [Operación S23] y [Operación S24] explicado previamente con referencia a la figura 10. Es decir, para etapas de número impar, q matrices MDS cuadradas son designadas repetidamente como L_1, L_2, ..., L_q, L_1, L_2, ... secuencialmente desde la función F de la etapa superior, y para etapas de número par, q matrices MDS cuadradas son

designadas repetidamente como L_1, L_2, ..., L_q, L_1, L_2, ... secuencialmente desde la función F de la etapa inferior.

Así, las matrices MDS cuadradas de las rondas de número par y las matrices MDS cuadradas de rondas de número par están dispuestas en órdenes mutuamente inversos, respectivamente, por lo que se garantiza que el tratamiento de cifrado y el tratamiento de descifrado son iguales excepto para el tratamiento de reemplazar una secuencia de claves.

Esta configuración garantiza lo siguiente. (a) La matriz de conversión lineal de cada función F es una matriz MDS cuadrada. (b) m vectores de columna arbitrarios de la matriz de conversión lineal incluidos en el menos q funciones F consecutivas en las rondas de número impar en la función criptográfica son linealmente independientes. (c) m vectores de columna arbitrarios de la matriz de conversión lineal incluidos en al menos q funciones F consecutivas en las rondas de número par en ella son linealmente independientes. Como estos aspectos (a) a (c) son garantizados, se garantizado que la cancelación de diferencia simultánea por contribución de m cajas S activas o menos no tiene lugar en las rondas 2q-1 consecutivas en la estructura criptográfica de bloque de clave común de tipo Feistel con el número de ronda de una pluralidad de etapas. Además, se garantiza lo siguiente. (d) A partir de la propiedad de la matriz MDS cuadrada, el número de elementos distintos de cero en los valores de diferencia obtenidos por contribución de "a" ($a \leq m$) cajas S activas resulta m+1-a o más. Por ello, el valor mínimo del número de cajas S activas en la totalidad de la función criptográfica aumenta.

Un caso en el que el ejemplo a3 de tratamiento produce especialmente un efecto es un caso en el que m y r resultan grandes, un coste de tiempo requerido en un sistema de tratamiento de determinación de matriz de los ejemplos a1 y a2 de tratamiento antes mencionados resulta enorme, y por ello es difícil determinar una matriz dentro de un tiempo realista. Incluso en tal caso, si se utiliza la técnica de generación de matriz MDS cuadrada de este ejemplo de tratamiento a3, el tratamiento de generación de matriz en un tiempo relativamente corto resultará posible.

Esto es debido a que resulta posible en el ejemplo a3 de tratamiento aplicar un sistema capaz de tratar para m y r suficientemente grandes en un tiempo realista, por ejemplo, un método de generación para generar una matriz con el código Reed-Solomon.

También en este ejemplo de tratamiento a3, como se ha descrito antes, resulta posible ampliar el número mínimo de cajas S activas en la totalidad de la función criptográfica que es uno de los índices de robustez a ataques de criptoanálisis diferencial en el código de bloque de clave común. Como resultado, cuando el análisis diferencial (ataque de criptoanálisis diferencial) es intentado, el número de cajas S activas aumenta, lo que mejorará la dificultad en el análisis. Por ello, es realizado un tratamiento criptográfico de alta seguridad cuya clave es difícil de analizar.

[(3-b) Ejemplo de generación de matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis lineal y las ajusta a las funciones F]

A continuación, se explicarán dos ejemplos de tratamiento b1, b2 como ejemplos de generación de las matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis lineal, y las ajusta a las funciones F.

(Ejemplo de tratamiento b1)
Se explicará un primer ejemplo de generación de las matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis lineal y las ajusta a las funciones F. El tratamiento de generación de las matrices MDS cuadradas será explicado con referencia al diagrama de flujo mostrado en la figura 15.

[Operación S401]
Designación de entrada: el número de matrices MDS cuadradas por q, el orden de extensión por n, y el tamaño de matriz por m, las q matrices MDS cuadradas emésimas M_1, M_2, ..., M_q son generadas aleatoriamente en GF (2^n). El diagrama de flujo mostrado en la figura 14 muestra un ejemplo de tratamiento como con el número de matrices MDS cuadradas q = 6, el orden de extensión n = 8, y el tamaño de matriz m = 8.

[Operación S402]
Se ha comprobado si m vector de fila arbitrarios sacados de los 2m vectores de fila incluidos en dos matrices inversas adyacentes después de calcular matrices inversas M_1^{-1}, M_2^{-1}, ..., M_q^{-1}, de q matrices MDS cuadradas emésimas M_1, M_2, ..., M_q son linealmente independientes. t^R en la figura 15 indica un vector transpuesto de un vector de fila. Si el flujo ha pasado la comprobación, el flujo prosigue a la Operación S403; si no lo ha hecho, el flujo vuelve a la Operación S401. Aquí, las matrices $M1^{-1}$, Mq^{-1} deben ser consideradas como matrices adyacentes.

[Operación S403]
Las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q son emitidas como matrices MDS cuadradas que han de ser aplicadas al código de bloque de clave común de tipo Feistel de número de ronda 2r.

Mediante el proceso anterior, se generan las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q. Aquí, q satisface $q \leq r$.

Las q matrices MDS cuadradas emésimas generadas de este modo L_1, L_2, ..., L_q son establecidas como matrices que han de ser aplicadas al tratamiento de conversión lineal de las secciones de conversión lineal de las funciones F de etapas respectivas en la estructura criptográfica de bloque de clave común de tipo Feistel de número de etapas (número de ronda) 2r, de acuerdo con el tratamiento de [Operación S23] y [Operación S24] explicados previamente con referencia a la figura 10. Es decir, para etapas de número impar, las q matrices MDS cuadradas han sido designadas repetidamente como L_1, L_2, ..., L_q, L_1, L_2, ... secuencialmente desde la función F de la etapa superior, y para las etapas de número par, las q matrices MDS cuadradas son designadas repetidamente L_1, L_2, ..., L_q, L_1, L_2, ... secuencialmente desde la función F de la etapa inferior.

Las matrices MDS cuadradas de las rondas de número par y las matrices MDS cuadradas de rondas de número par están dispuestas en órdenes mutuamente inversos, respectivamente, de este modo, por lo cual se garantiza que el tratamiento de cifrado y el tratamiento de descifrado son el mismo excepto para reemplazar una secuencia de claves.

Esta configuración garantiza lo siguiente. (a) Una matriz de conversión lineal de cada función F es una MDS cuadrada, (b) m vectores de columna en una matriz inversa incluida consecutivamente en rondas de número impar en una función criptográfica y en una matriz inversa incluida consecutivamente en rondas de número par en ella son linealmente independientes. Estas propiedades permiten que la dificultad en el análisis por aproximación lineal en ataques de criptoanálisis lineal sea aumentada, y se produzca un tratamiento criptográfico de alta seguridad con dificultad acrecentada en el análisis, es decir, cuya clave es difícil de analizar.

(Ejemplo de tratamiento b2)
Se explicará un segundo ejemplo de generación de las matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis lineal y las ajusta a las funciones F. La explicación será dada para el tratamiento de generación de la matriz MDS cuadrada que se refiere al diagrama de flujo mostrado en la figura 16.

[Operación S501]
Designación de entrada: el número de matrices MDS cuadradas necesarias por q, un orden de ampliación por n, y un tamaño de matriz por m, las q matrices MDS cuadradas emésimas M_1, M_2, ..., M_q son generadas aleatoriamente en GF (2^n). El diagrama de flujo mostrado en la figura 16 muestra un ejemplo de tratamiento como con el número de matrices MDS cuadradas q = 6, el orden de extensión n = 8, y el tamaño de matriz M = 8.

[Operación S502]
Se comprueba si m vectores de fila arbitrarios sacados de los vectores de fila 2m incluidos en dos matrices inversas adyacentes después de calcular las matrices inversas M_1^{-1}, M_2^{-1}, ..., M_q^{-1}, de las q matrices MDS emésimas M_1, M_2, ..., M_q constituyen una matriz MDS cuadrada. ${}^tR$ en la figura 16 indica un vector transpuesto de un vector de fila. Si el flujo ha pasado la comprobación, el flujo prosigue a la Operación S503; si no lo ha hecho, el flujo vuelve a la Operación 401. Aquí, las matrices $M1^{-1}$, Mq^{-1} deben ser consideradas como matrices adyacentes. La matriz MDS cuadrada es una matriz que satisface las propiedades siguientes. (a) Es una matriz cuadrada. (b) Los determinantes de todas las submatrices incluidas en la matriz no son cero, en particular, det(submatriz) $\neq 0$.

[Operación S503]
Las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q son emitidas como matrices MDS cuadradas que han de ser aplicadas al código de bloque de clave común de tipo Feistel de número de ronda 2r.

Mediante el proceso anterior, son generadas las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q. Aquí, q satisface $q \leq r$.

En el tratamiento de generación de matriz MDS cuadrada en el ejemplo b1 de tratamiento antes descrito, como se ha explicado en la secuencia de tratamiento de la figura 15, lo que se ha determinado es la independencia lineal cuando se sacan m vectores de columna arbitrarios de los qm vectores de columna incluidos en las matrices inversas M_1^{-1}, M_2^{-1}, ..., M_q^{-1} de las q matrices MDS cuadradas emésimas M_1, M_2, ..., M_q en la Operación S402. En el tratamiento de generación de la matriz MDS cuadrada en este ejemplo de tratamiento b2, se ha comprobado si m vectores de columna arbitrarios sacados de los m vectores de columna incluidos en matrices inversas M_1^{-1}, M_2^{-1}, ..., M_q^{-1} de las q matrices MDS cuadradas emésimas M_1, M_2, ..., M_q constituyen una matriz MDS cuadrada. Es decir, se ejecutará una comprobación más severa.

Como el ejemplo b1 de tratamiento descrito previamente, las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q generadas por el tratamiento de generación de matriz MDS cuadrada que cumple con una secuencia de tratamiento mostrada en esta figura 16 son establecidas como matrices que han de ser aplicadas al tratamiento de conversión lineal

de las secciones de conversión lineal de las funciones F de etapas respectivas en la estructura criptográfica de bloque de clave común de tipo Feistel de número de etapa (número de ronda) 2r, de acuerdo con el tratamiento [Operación S23] y [Operación S24] explicado previamente con referencia a la figura 10. Es decir, para etapas de número impar, las q matrices MDS cuadradas han sido designadas como L_1, L_2, ..., L_q, L_1, L_2, ... secuencial y repetidamente desde las funciones F de la etapa superior, y para etapas de número par, las q matrices MDS cuadradas han sido designadas como L_1, L_2, ..., L_q, L_1, L_2, ... secuencial y repetidamente desde la función F de la etapa inferior.

Así, las matrices MDS cuadradas de las rondas de número par y las matrices MDS cuadradas de las rondas de número par están dispuestas en órdenes mutuamente inversos, respectivamente, por lo que se garantiza que el tratamiento de cifrado y el tratamiento de descifrado son el mismo excepto para el tratamiento de reemplazar una secuencia de claves.

Esta configuración garantiza lo siguiente. (a) La matriz de conversión lineal de cada función F es una matriz MDS cuadrada. (b) m vectores de columna arbitrarios de las matrices inversas de la matriz de conversión lineal incluidos consecutivamente en rondas de número impar en la función criptográfica y de la matriz de conversión lineal incluida consecutivamente en rondas de número par en ella constituyen una matriz MDS cuadrada. Estas propiedades permiten que la dificultad en el análisis por aproximación lineal en ataques de criptoanálisis lineal sea incrementada, y se produzca un tratamiento criptográfico de alta seguridad con dificultad aumentada en el análisis, es decir, cuya clave es difícil de analizar.

[(3-c) Ejemplo de generación de matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis diferencial y ataques de criptoanálisis lineal y las ajusta a las funciones F]

A continuación, se explicará un ejemplo de generación de matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis diferencial y ataques de criptoanálisis lineal y las ajusta a las funciones F.

El algoritmo criptográfico con la resistencia a ataques de criptoanálisis diferencial es producido aplicando el tratamiento explicado con referencia a las figuras 10 a 13 previamente, es decir, estableciendo las matrices MDS cuadradas que han de ser aplicadas a conversión lineal en las secciones de tratamiento lineal de las funciones F aplicando cualquiera de los ejemplos de tratamiento antes mencionados a1 (figura 11) a a3 (figura 13). Además, el algoritmo criptográfico con la resistencia a ataques de criptoanálisis lineal es producido aplicando el tratamiento explicado con referencia a la figura 10 y figuras 14 y 15 previamente, es decir, ajustando las matrices MDS cuadradas que han de ser aplicadas a conversión lineal en las secciones de tratamiento lineal de las funciones F por aplicación de cualquiera de los ejemplos de tratamiento antes mencionados b1 (figura 14) y b2 (figura 15).

El algoritmo que utiliza matrices MDS cuadradas que producen una resistencia mejorada a ataques de criptoanálisis diferencial y ataques de criptoanálisis lineal es puesto en práctica estableciendo matrices MDS cuadradas generadas realizando tanto un tratamiento de ambos ejemplos de tratamiento a1 (figura 11) a a3 (figura 12) como uno de los tratamientos de ejemplos de tratamiento b1 (figura 14) y b2 (figura 15) como matrices que han de ser aplicadas al tratamiento de conversión lineal de las secciones de conversión lineal de las funciones F de etapas respectivas en la estructura criptográfica de bloque de clave común de tipo Feistel de número de etapa (número de ronda) 2r.

Es decir, se generan q matrices MDS cuadradas por cualquiera de las combinaciones siguientes: un ejemplo a1 de tratamiento y un ejemplo de tratamiento b1; un ejemplo a1 de tratamiento y un ejemplo de tratamiento b2; un ejemplo a2 de tratamiento y un ejemplo de tratamiento b1; un ejemplo a2 de tratamiento y un ejemplo de tratamiento b2; un ejemplo a3 de tratamiento y un ejemplo de tratamiento b1; un ejemplo a3 de tratamiento y un ejemplo de tratamiento b2; y son establecidas como matrices que han de ser aplicadas al tratamiento de conversión lineal de las secciones de conversión lineal de las funciones F de etapas respectivas en la estructura criptográfica de bloque de clave común de tipo Feistel de número de ronda 2r. Es decir, para etapas de número impar, las q matrices MDS cuadradas han sido designadas repetidamente como L_1, L_2, ..., L_q, L_1, L_2, ... secuencialmente desde la función F de la etapa superior, y para etapas de número par, las q matrices MDS cuadradas han sido designadas repetidamente como L_1, L_2, ..., L_q, L_1, L_2, ... secuencialmente desde la función F de la etapa inferior. Mediante este ajuste, resulta posible el tratamiento criptográfico que produce una resistencia mejorada a ataques de criptoanálisis diferencial y ataques de criptoanálisis lineal.

Se explicará con referencia a la figura 17 un ejemplo de tratamiento de generación de matrices MDS cuadradas para poner en práctica el tratamiento criptográfico que produce una resistencia mejorada a ataques de criptoanálisis diferencial y a ataques de criptoanálisis lineal. Este tratamiento es una combinación del ejemplo a2 de tratamiento y del ejemplo b2 de tratamiento antes descritos.

[Operación S601]
Designación de entrada: el número de matrices MDS cuadradas necesarias por q, el orden de extensión por n, y el tamaño de matriz por m, las q matrices MDS cuadradas emésimas han sido generadas aleatoriamente en GF (2^n). El diagrama de flujo mostrado en la figura 17 muestra un ejemplo de tratamiento como con el número de matrices MDS

cuadradas q = 6, el orden de extensión n = 8, y el tamaño de matriz m = 8.

[Operación S602]
Cuando m columnas son sacadas de las qm columnas incluidas en las q matrices MDS cuadradas emésimas, M_1, M_2, ..., M_q, se comprueba si constituyen una matriz MDS cuadrada. Si el flujo ha pasado la comprobación, el flujo prosigue a la Operación S603; si no lo ha hecho, el flujo vuelve a la operación S601. Aquí, la matriz MDS cuadrada significa una matriz que satisface las siguientes propiedades. (a) Es una matriz cuadrada. (b) Un determinante de cualquier submatriz incluida en la matriz es distinto de cero, en particular det(submatriz) $\neq 0$.

[Operación S603]
Se calculan matrices inversas M_1^{-1}, M_2^{-1}, ..., M_q^{-1} de las q matrices MDS cuadradas emésimas M_1, M_2, ..., M_q, y se comprueba si m vectores de fila arbitrarios son sacados de 2m vectores de fila incluidos en dos matrices inversas adyacentes constituyen una matriz MDS cuadrada. tR en la figura 17 indica un vector transpuesto de un vector de fila. Si el flujo ha pasado la comprobación, el flujo prosigue a la Operación S604; si no lo ha hecho, el flujo vuelve a la Operación S601. Aquí, matrices M1-1, Mq-1 serán consideradas como matrices adyacentes.

[Operación S604]
Las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q son emitidas como matrices MDS cuadradas que han de ser aplicadas al código de bloque de clave común de número de ronda 2r.

Mediante el proceso anterior, se generan las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q. Aquí, satisface $q \leq r$.

Las q matrices MDS cuadradas emésimas L_1, L_2, ..., L_q generadas por el tratamiento de generación de matriz MDS cuadrada que ha seguido una secuencia de tratamiento mostrada en la figura 17 son establecidas como matrices que han de ser aplicadas al tratamiento de conversión lineal de las secciones de conversión lineal de las secciones de funciones F de etapas respectivas en la estructura criptográfica de bloque de clave común de tipo Feistel de número de etapa (número de ronda) 2r, de acuerdo con el tratamiento de la [Operación S23] y la [Operación S24] explicado previamente con referencia a la figura 10. Es decir, para etapas de número impar, q matrices MDS cuadradas son designadas repetidamente como L_1, L_2, ..., L_q, L_1, L_2, ... secuencialmente desde la función F de la etapa superior, y para etapas de número par, q matrices MDS cuadradas son designadas repetidamente como L_1, L_2, ..., L_q, L_1, L_2, ... secuencialmente desde la función F de la etapa inferior.

Así, matrices MDS cuadradas de las rondas de número par y matrices MDS cuadradas de las rondas de número impar están dispuestas en órdenes mutuamente inversos, respectivamente, por lo que se garantiza que el tratamiento de cifrado y el tratamiento de descifrado son el mismo excepto para el tratamiento de reemplazar una secuencia de claves.

Esta configuración garantiza los siguientes aspectos (a) a (c). (a) La matriz de conversión lineal de cada función F es una matriz MDS cuadrada. (b) m vectores de columna arbitrarios de la matriz de conversión lineal incluida en al menos q funciones F consecutivas en rondas de número impar en la función criptográfica constituyen una matriz MDS cuadrada. (c) m vectores de columna arbitrarios de la matriz de conversión lineal incluida en el menos q funciones F consecutivas en rondas de número par en ella constituyen una matriz MDS cuadrada. Como estos respetos a (a) a (c) están garantizados, en la estructura criptográfica de bloque de clave común de tipo Feistel con número de ronda de la pluralidad de operaciones, se garantiza que la cancelación de diferencia simultánea por contribución de m cajas S activas o menos no ocurre en las rondas 2q-1 consecutivas. Además, (d) a partir de la propiedad de la matriz MDS cuadrada, se garantiza que el número de elementos distintos de cero en valores de diferencia obtenidos por contribución de “a” ($a \leq m$) cajas S activas resulta m+1-a o más. Por tanto, el valor mínimo del número de cajas S activas en la totalidad de la función criptográfica aumenta. Además, se garantiza lo siguiente. (e) m vectores de columna arbitrarios de las matrices inversas de las matrices de conversión lineal incluidas consecutivamente en rondas de número impar y de las matrices de conversión lineal incluidas consecutivamente en las rondas de número par ambas en la función criptográfica constituyen una matriz MDS cuadrada. Estas propiedades permiten que la dificultad en el análisis por aproximación lineal en ataques de criptoanálisis lineal sea aumentada, y se produzca el tratamiento criptográfico de alta seguridad con dificultad aumentada en el análisis, es decir, cuya clave es difícil de analizar.

Así, mediante este ejemplo de tratamiento, es aumentada la dificultad en el análisis tanto a los ataques de criptoanálisis diferencial como a los ataques de criptoanálisis lineal, y se produce el tratamiento de criptoanálisis de alta seguridad cuya clave es difícil de analizar. El ejemplo mostrado en la figura 17 fue, como se ha descrito antes, un ejemplo de generación de las matrices MDS cuadradas por la combinación del ejemplo a2 de tratamiento y del ejemplo b2 de tratamiento explicado previamente. Sin embargo, puede adoptarse otra generación. Es decir, q matrices MDS cuadradas son generadas combinando uno de los siguientes pares: el ejemplo a1 de tratamiento y el ejemplo b1 de tratamiento, el ejemplo a1 de tratamiento y el ejemplo b2 de tratamiento, el ejemplo a2 de tratamiento y el ejemplo b1 de tratamiento, el ejemplo a3 de tratamiento y el ejemplo b1 de tratamiento, y el ejemplo a3 de tratamiento y el ejemplo b2 de tratamiento. Para etapas de número impar, q matrices MDS cuadradas son designadas repetidamente como L_1, L_2, ..., L_q, L_1, L_2, ...

secuencialmente desde la función F de la etapa superior, y para etapas de número par, q matrices MDS cuadradas son designadas repetidamente como L_1, L_2, ..., L_q, L_1, L_2, ... secuencialmente desde la función F de la etapa inferior, como una matriz que ha de ser aplicada en las secciones de conversión lineal de las funciones F de etapas respectivas en la estructura criptográfica de bloque de clave común de tipo Feistel de número de etapa (número de ronda) 2r; por lo que puede realizarse un tratamiento criptográfico de alta seguridad que tiene una dificultad realzada en el análisis tanto de ataques de criptoanálisis diferencial como de ataques de criptoanálisis lineal y cuya clave es difícil de analizar.

Aunque la explicación hasta este punto haya asumido que la matriz de conversión lineal es una matriz de mxm definida en GF (2^n) y utilizada en una operación de conversión de datos desde mn bits hasta mn bits, el efecto similar a ataques de criptoanálisis diferencial y ataques de criptoanálisis lineal puede ser obtenido incluso en el caso en el que se ha utilizado una matriz de mnxmn definida en GF (2). Realmente, la matriz arbitraria en GF (2^n) puede ser llevada a una correspondencia unívoca con una matriz en GF (2) que muestra la misma conversión. Por ello, puede decirse que la matriz en GF (2) muestra una representación más general. La matriz en GF (2) tiene mn columna y mn filas, que son n-veces las del caso de GF (2^n). Por esta razón, la primera columna de la matriz en GF (2^n) corresponde a las columnas primera a enésima de la matriz en GF (2), y la primera fila de la matriz en GF (2^n) corresponde a las filas primera a enésima de la misma. Es decir, la fila iésima corresponde a las filas [(i-1)+1]-ésima a [(i-1)+n]-ésima, y la columna iésima corresponde a las columnas [(i-1)+1]-ésima a [(i-1)+n]-ésima. Por tanto, con el fin de realizar una operación de extracción de una columna o fila en GF (2^n), si se utiliza una matriz definida en GF (2), es necesario realizar una operación de extracción de n filas o n columnas que corresponden a la columna o fila en GF (2) de manera correspondiente. La operación de extraer m filas o columnas en GF (2) requiere extraer n filas o columnas durante m veces en GF (2), y como resultado puede obtenerse una matriz mnxmn. La coordinación anterior permite que las matrices sean fácilmente extendidas o prolongadas a matrices definidas en GF (2).

Finalmente, la figura 18 muestra una configuración ejemplar de un módulo IC 600 como un aparato de tratamiento criptográfico para realizar un tratamiento criptográfico. El tratamiento antes mencionado puede ser ejecutado en diferentes aparatos de tratamiento de información, por ejemplo, un PC, una tarjeta IC, un lector/escritor, etc. y el módulo IC 600 mostrado en la figura 18 puede ser utilizado como un constituyente para estos distintos aparatos.

Una CPU (Unidad de Tratamiento Central) 601 mostrada en la figura 18 es un procesador para ejecutar distintos programas, tales como iniciar un tratamiento criptográfico, terminarlo, controlar la transmisión/recepción de datos, controlar la transferencia de datos entre secciones de configuración, y ejecutar distintos programas. La memoria 602 consiste de ROM (Memoria Sólo de Lectura) para almacenar un programa que la CPU 601 ejecuta o datos fijos como parámetros de funcionamiento, RAM (Memoria de Acceso Aleatorio) utilizada como un área de almacenamiento del programa ejecutado en el tratamiento de la CPU 601, parámetros siempre variables en tratar el programa, y un área de trabajo, etc. La memoria 602 también puede ser utilizada como áreas de almacenamiento de datos clave necesarios para el tratamiento criptográfico, etc. Es preferible que un área de almacenamiento de datos etc., construida como memoria con una estructura resistente a las manipulaciones indebidas.

Una sección 603 de tratamiento criptográfico realiza cifrado, descifrado, etc. que sigue, por ejemplo, el algoritmo de tratamiento criptográfico de bloque de clave común de tipo Feistel descrito con anterioridad. Aunque se ha mostrado el ejemplo en el que los medios de tratamiento criptográfico están hechos como un módulo individual, puede configurarse que, por ejemplo, un programa criptográfico sea almacenado en la ROM y la CPU 601 lea y ejecute el programa almacenado en la ROM sin proporcionar tal módulo criptográfico independiente.

Un generador 604 de número aleatorio ejecuta el tratamiento de generar números aleatorios que son necesarios en la generación de una clave que es requerida para tratamiento criptográfico y similar.

Una sección 605 de transmisión/recepción es una sección de comunicación de datos para realizar la comunicación de datos externamente, que ejecuta comunicación de datos con, por ejemplo, un lector-escritor, etc. y un módulo IC, que emite un texto cifrado generado en el módulo IC o que introduce en él datos etc., desde el lector-escritor externo etc.

Nótese que una serie de tratamiento explicada en la descripción puede ser puesta en práctica mediante hardware, mediante software, o mediante una combinación de ambos. Cuando se realiza el tratamiento mediante software, puede ejecutarse un programa que graba o registra una secuencia de tratamiento instalándolo en la memoria integrada en un hardware exclusivo en un ordenador, o puede ser ejecutado instalándolo en un ordenador de propósito general capaz de realizar distintos tratamientos.

Por ejemplo, un programa puede ser grabado de antemano en un disco duro o ROM (Memoria Sólo de Lectura) como un medio de grabación. Alternativamente, el programa puede ser almacenado temporalmente o de manera permanente en un medio de grabación que se puede retirar, tal como un disco flexible, un CD-ROM (Disco Compacto de Memoria Sólo de Lectura), un disco MO (Magneto óptico), un DVD (Disco Versátil Digital), un disco magnético, y una memoria de semiconductor. Tal medio de grabación que puede retirarse puede ser proporcionado como el denominado paquete de

software.

Además de instalar el programa en el ordenador desde un medio de grabación que se puede retirar como se ha descrito antes, puede adoptarse el siguiente esquema. El programa es transferido de modo inalámbrico al ordenador desde un sitio de descarga, o es transferido por cable al ordenador a través de una red, tal como una LAN (Red de Área Local) y la Internet, mientras el ordenador recibe el programa que está siendo transferido de tal forma y lo instala en un medio de grabación, tal como un disco duro interno.

Nótese que pueden ser ejecutados distintas clases de tratamiento escritos en la descripción en paralelo o individualmente de acuerdo con la capacidad de tratamiento del aparato que realiza el tratamiento o si se necesitara también siendo ejecutados en la secuencia de tiempo de acuerdo con la descripción. Obsérvese que en esta descripción, el sistema es uno que tiene una estructura de combinación lógica de una pluralidad de dispositivos, pero que no está limitado a sistemas, cada uno de los cuales tiene sus propios dispositivos en el mismo recinto o envolvente.

REIVINDICACIONES

1.- Un aparato de tratamiento criptográfico para realizar un tratamiento criptográfico de bloque de clave común que tiene una estructura de Feistel, que tiene
una estructura que ejecuta repetidamente una función F (120) que incluye un SPN que tiene una sección de conversión no lineal (121) y una sección de conversión lineal (122) sobre una pluralidad de rondas, incluyendo la sección de conversión no lineal (121) m Casa S, siendo m un número entero, en el que cada una de las m cajas emite n bits en paralelo, siendo n un número entero, en el que
cada una de las secciones de conversión lineal (122) de una función F correspondiente a cada una de la pluralidad de rondas está establecida para realizar un tratamiento de conversión lineal de una entrada de mxn bits emitidos en paralelo desde las m cajas S como tratamiento de conversión lineal que aplica una matriz (402) MDS (Separable por Distancia Máxima) cuadrada, siendo la matriz MDS cuadrada una matriz cuadrada enésima que tiene elementos en un campo de extensión GF(2^n), multiplicando la matriz MDS cuadrada con la entrada de mxn bits, en que se aplican directamente al menos en las rondas de número impar consecutivos matrices MDS cuadradas diferentes y en las rondas de número par consecutivos, se aplican directamente matrices MDS cuadradas diferentes,
el tratamiento criptográfico de bloque de clave común incluye un algoritmo criptográfico de número de ronda 2r,
la sección de conversión lineal (122) de la función F (120) está establecida para ejecutar una conversión lineal aplicando q clases de diferentes matrices MDS cuadradas ($2 \leq q < r$) secuencial y repetidamente en todas las rondas de número par r y en todas las rondas de número impar r,
la matriz de conversión lineal de número de ronda 2i-1 ($1 \leq i \leq r$) es ajustada a $L_{[i-1 \bmod o]+1}$, donde L_i indica una de las q matrices MDS,
la matriz de conversión lineal de número de ronda 2i-1 ($1 \leq i \leq r$) es ajustada a $L_{2r-21+1}$, y **caracterizado porque**:

m vectores de fila seleccionados arbitrariamente a partir de vectores de fila de dos matrices secuenciales que constituyen matrices inversas de las matrices MDS cuadradas son linealmente independientes.

2.- El aparato de tratamiento criptográfico para realizar el tratamiento criptográfico de bloque de clave común según la reivindicación 1en el que:
una matriz compuesta de m vectores de fila seleccionados arbitrariamente de vectores de fila que constituyen las matrices inversas es una matriz MDS cuadrada.

3. Un método de tratamiento criptográfico para realizar un tratamiento criptográfico de bloque de clave común que tiene una estructura Feistel, que comprende las operaciones de:

ejecutar una función F (120) que incluye un SPN para realizar tratamiento de conversión no lineal y tratamiento de conversión lineal repetidamente sobre una pluralidad de rondas; y
en el tratamiento de conversión de una función F (120) que corresponde a cada uno de la pluralidad de rondas, realizar la conversión lineal para una entrada de mxn bits emitida en paralelo desde m secciones de conversión no lineal, en la que cada una de las secciones de conversión no lineal emite n bits, siendo n y m números enteros, como tratamiento de conversión lineal aplicar matrices MDS (Separable por Máxima Distancia) cuadradas (402) multiplicando la matriz MDS cuadrada (402), siendo la matriz MDS cuadrada una matriz cuadrada emésima que tiene elementos en un campo de extensión GF (2^n), con la entrada de mxn bits; en la que
el tratamiento de conversión lineal con matrices MDS cuadrada (402) es realizado de tal forma que al menos se aplican directamente en las rondas de número par consecutivas matrices MDS cuadradas diferentes y en las rondas de número impar consecutivas, se aplican directamente matrices MDS cuadradas diferentes,
el tratamiento criptográfico de bloque de clave común incluye un algoritmo criptográfico de número de ronda 2r,
la sección de conversión lineal (122) de la función F (120) está establecida para ejecutar conversión lineal aplicando q clases de matrices MDS cuadradas diferentes ($2 \leq q < r$) secuencial y repetidamente en todas las rondas de número par r y en todas las rondas de número impar r,
la matriz de conversión lineal de número de ronda 2i-1 ($1 \leq i \leq r$) es ajustada a $L_{(i-1 \bmod q)+1}$, en el que L_i indica una de las q matrices MDS,
la matriz de conversión lineal de número de ronda 2i ($1 \leq i \leq r$) es ajustada a $L_{2r-2i+1}$, y **caracterizado porque**
m vectores de fila seleccionados arbitrariamente a partir de los vectores de fila de dos matrices secuenciales que constituyen matrices inversas de las matrices MDS cuadradas son linealmente independientes.

4. Un programa de ordenador para realizar el tratamiento criptográfico de bloque de clave común que tienen una estructura Feistel, que comprende la operación de:

ejecutar una función F (120) que incluye un SPN para realizar un tratamiento de conversión no lineal y un tratamiento de conversión lineal sobre una pluralidad de rondas, en el que
el tratamiento de conversión lineal de la función F (120) que corresponde a cada uno de la pluralidad de rondas es una operación de conversión lineal para realizar un tratamiento de conversión lineal para una entrada de mxn bits

emitida en paralelo desde m secciones de conversión no lineal, en el que cada una de las secciones de conversión no lineal emite n bits, como un tratamiento de conversión lineal que aplica una matriz MDS (Separable por Distancia Máxima) cuadrada multiplicando la matriz MDS cuadrada (402), siendo la matriz MDS cuadrada una matriz cuadrada emésima que tiene elementos en un campo de extensión GF (2^n), con la entrada de mxn bits, y
en la operación de conversión lineal, es ejecutado un tratamiento de conversión lineal por matrices MDS cuadradas (402)
de tal forma que al menos en las rondas de número par consecutivas se aplican directamente matrices MDS cuadradas (402) diferentes y en las rondas de número impar consecutivas, se aplican directamente diferentes matrices MDS cuadradas (402),
el tratamiento criptográfico de bloque de clave común incluye un algoritmo criptográfico de número de ronda 2r,
la sección de conversión lineal (122) de la función F (120) está establecida para ejecutar conversión lineal aplicando q clases de matrices MDS cuadradas diferentes ($2 \leq q < r$) secuencial y repetidamente en todas las rondas de número par r y en todas las rondas de número impar r,
la matriz de conversión lineal de número de ronda 2i-1 ($1 \leq i \leq r$) es establecida a $L_{(i-1 \bmod q)+1}$, en el que L_i indica una de las q matrices MDS,
la matriz de conversión lineal de número de ronda 2i ($1 \leq i \leq r$) es ajustada a $L_{2r-2i+1}$, y **caracterizado porque**:

m vectores de fila seleccionados arbitrariamente a partir de los vectores de fila de dos matrices secuenciales que constituyen matrices inversas de las matrices MDS cuadradas son linealmente independientes.

FIG. 1

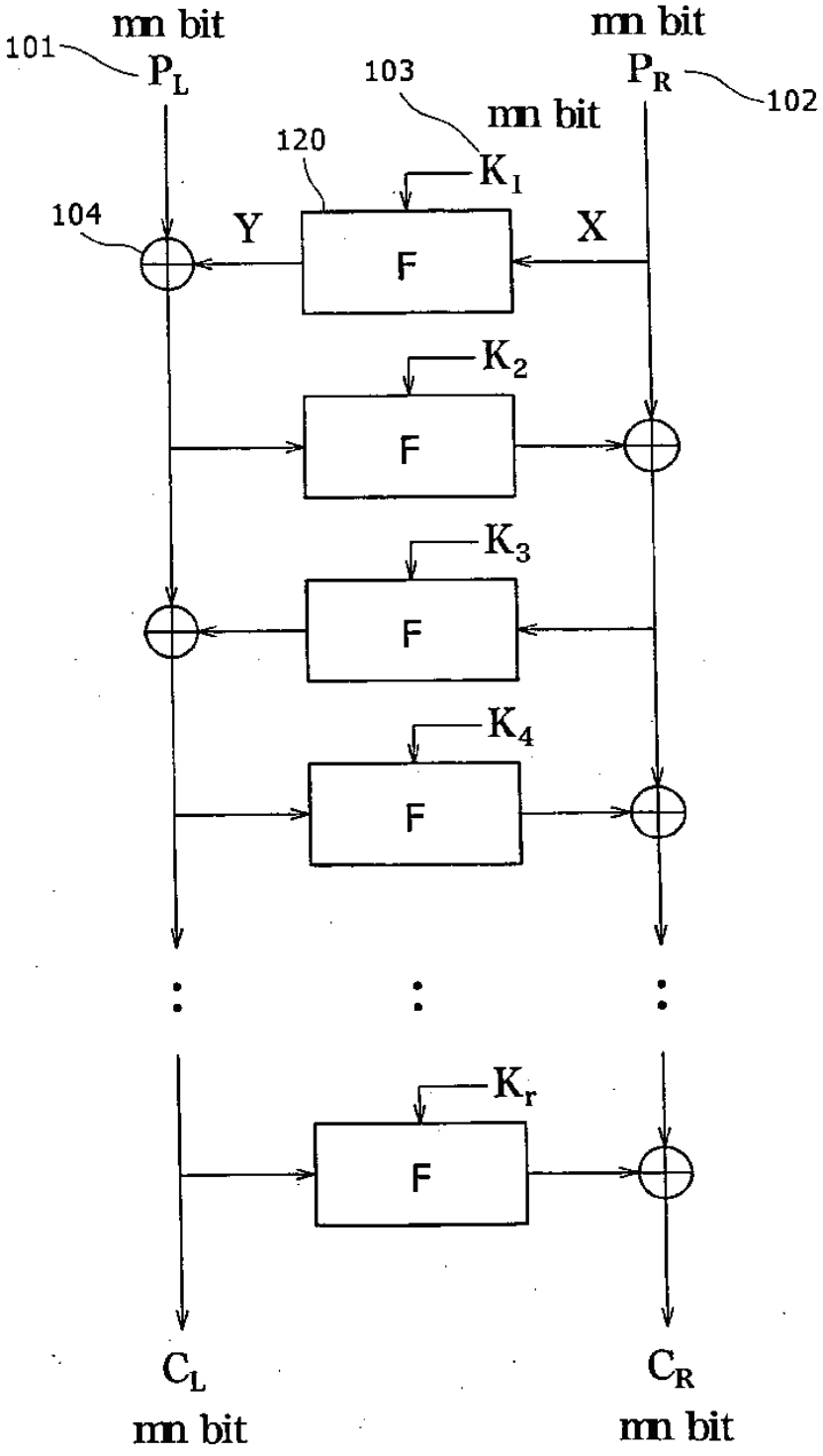

mn bit
101
P_L
mn bit
P_R
102
103
mn bit
120
K_1
104
Y
X
F
K_2
F
K_3
F
K_4
F
K_r
F
C_L
mn bit
C_R
mn bit

FIG. 2A

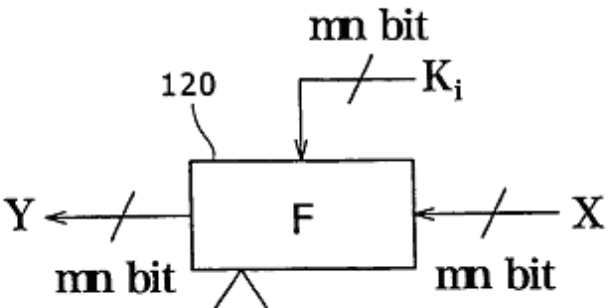

mn bit
K_i
120
F
Y
X
mn bit
mn bit

FIG. 2B

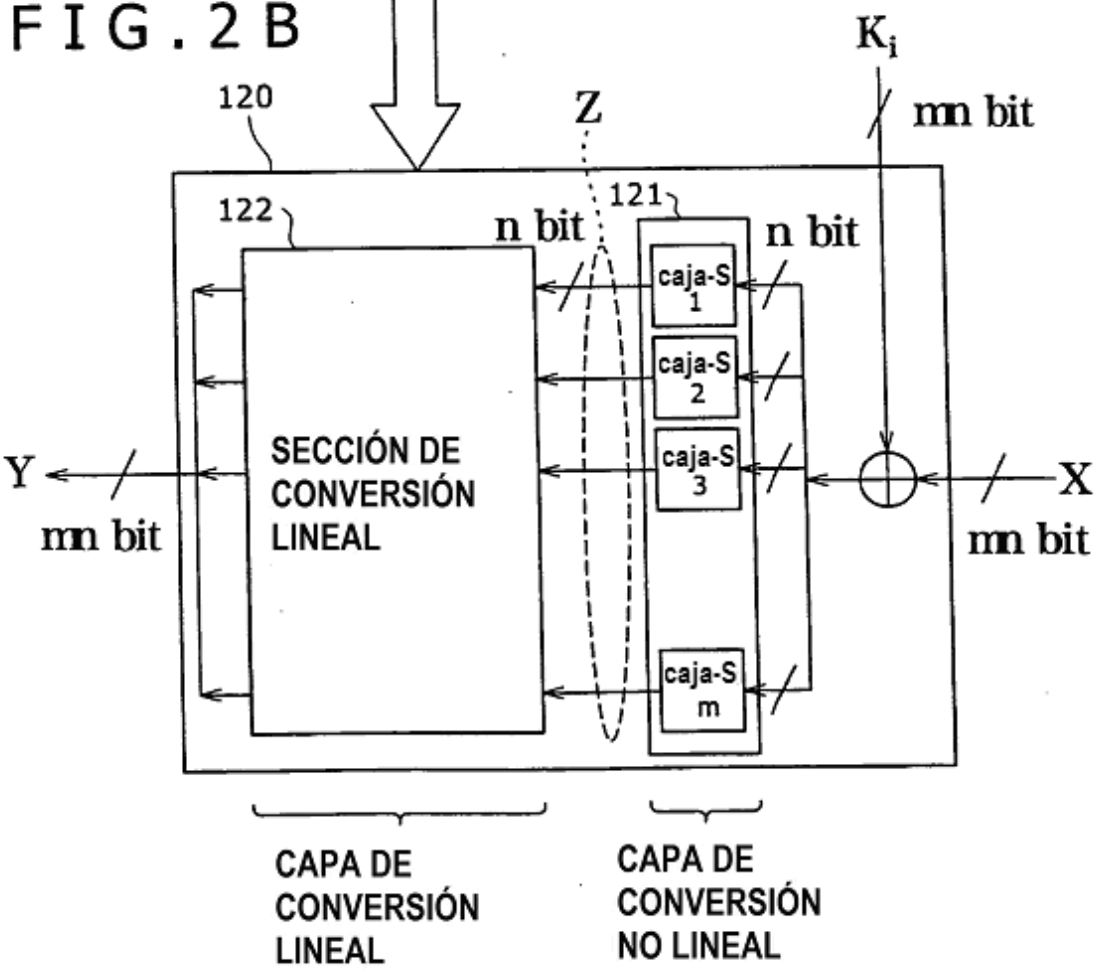

120
Z
K_i
mn bit
122
n bit
121
n bit
caja-S 1
caja-S 2
caja-S 3
caja-S m
SECCIÓN DE CONVERSIÓN LINEAL
Y
mn bit
X
mn bit
CAPA DE CONVERSIÓN LINEAL
CAPA DE CONVERSIÓN NO LINEAL

FIG. 3

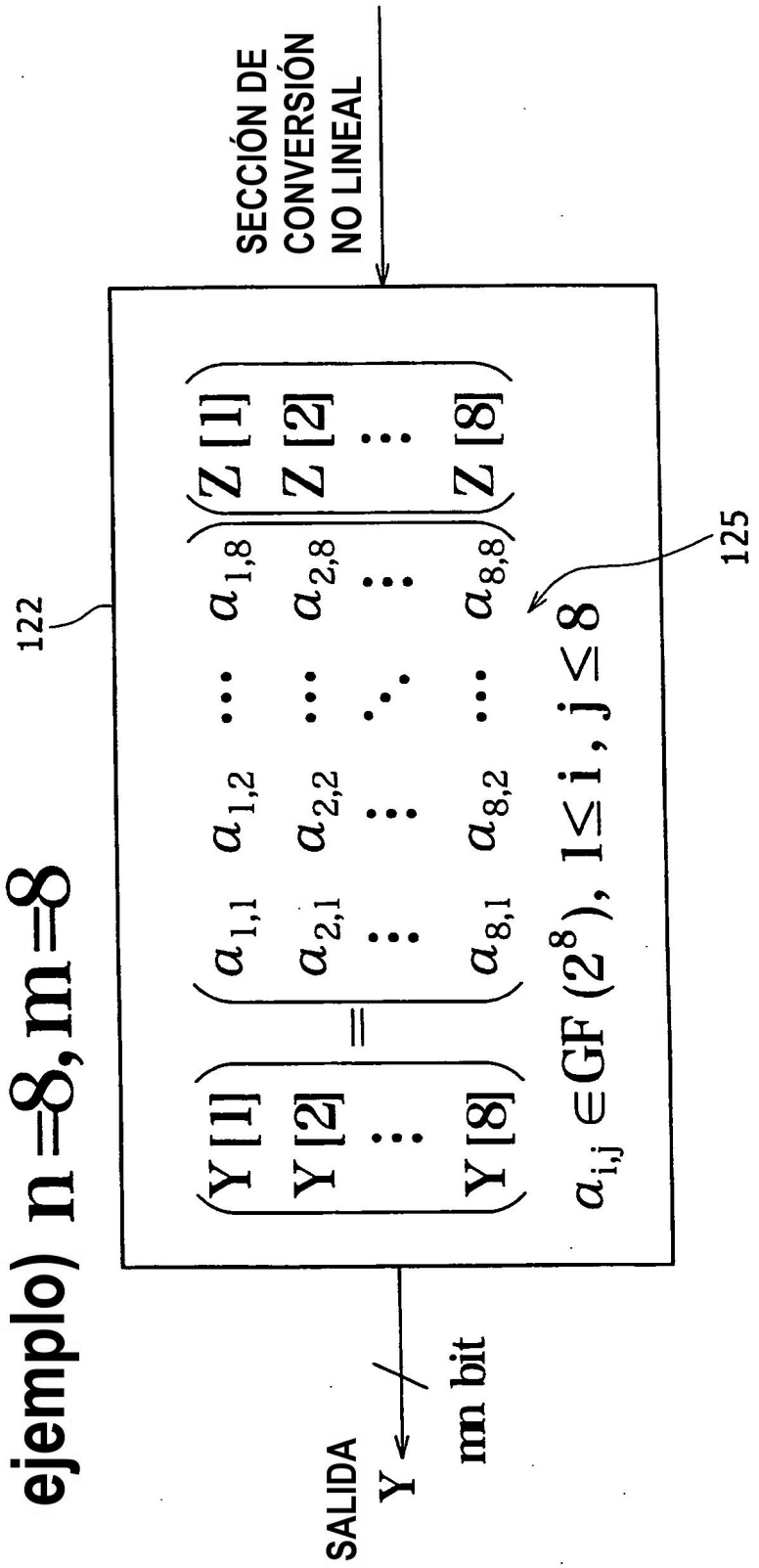

ejemplo) n=8, m=8
122
SECCIÓN DE CONVERSIÓN NO LINEAL
$\begin{pmatrix} Y[1] \\ Y[2] \\ \vdots \\ Y[8] \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,8} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,8} \\ \vdots & \vdots & \ddots & \vdots \\ a_{8,1} & a_{8,2} & \cdots & a_{8,8} \end{pmatrix} \begin{pmatrix} Z[1] \\ Z[2] \\ \vdots \\ Z[8] \end{pmatrix}$
$a_{i,j} \in GF(2^8),\ 1 \le i, j \le 8$
125
SALIDA
Y
m bit

FIG. 4

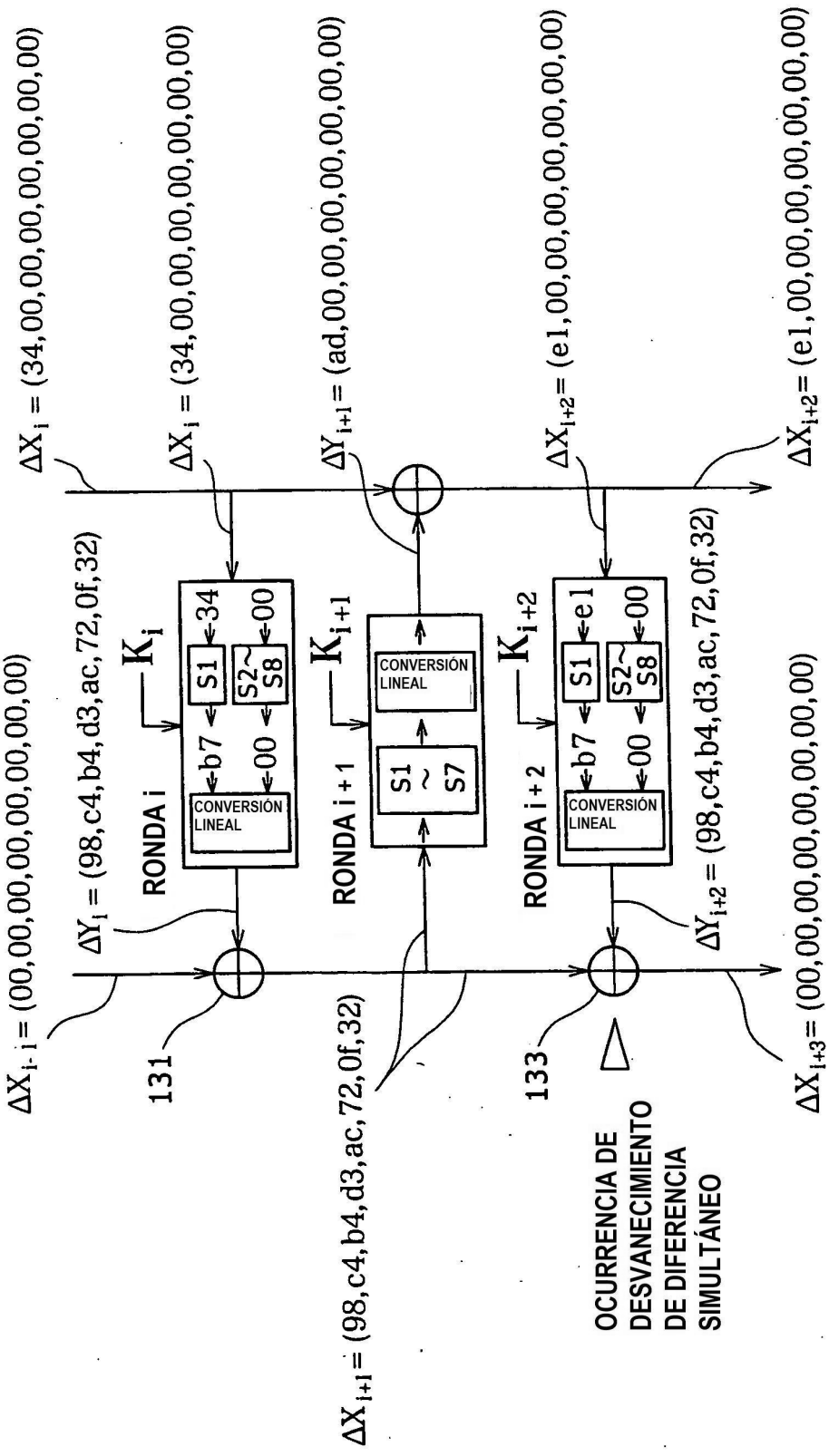

ΔXi = (34,00,00,00,00,00,00,00)
ΔXi = (34,00,00,00,00,00,00,00)
ΔYi+1 = (ad,00,00,00,00,00,00,00)
ΔXi+2 = (e1,00,00,00,00,00,00,00)
ΔXi+2 = (e1,00,00,00,00,00,00,00)
ΔYi = (98,c4,b4,d3,ac,72,0f,32)
ΔXi-1 = (00,00,00,00,00,00,00,00)
RONDA i
Ki
34
S1
S2~S8
00
b7
00
CONVERSIÓN LINEAL
RONDA i+1
Ki+1
CONVERSIÓN LINEAL
S1 ~ S7
RONDA i+2
Ki+2
e1
S1
S2~S8
00
b7
00
CONVERSIÓN LINEAL
ΔYi+2 = (98,c4,b4,d3,ac,72,0f,32)
ΔXi+1 = (98,c4,b4,d3,ac,72,0f,32)
ΔXi+3 = (00,00,00,00,00,00,00,00)
131
133
OCURRENCIA DE DESVANECIMIENTO DE DIFERENCIA SIMULTÁNEO

FIG. 5

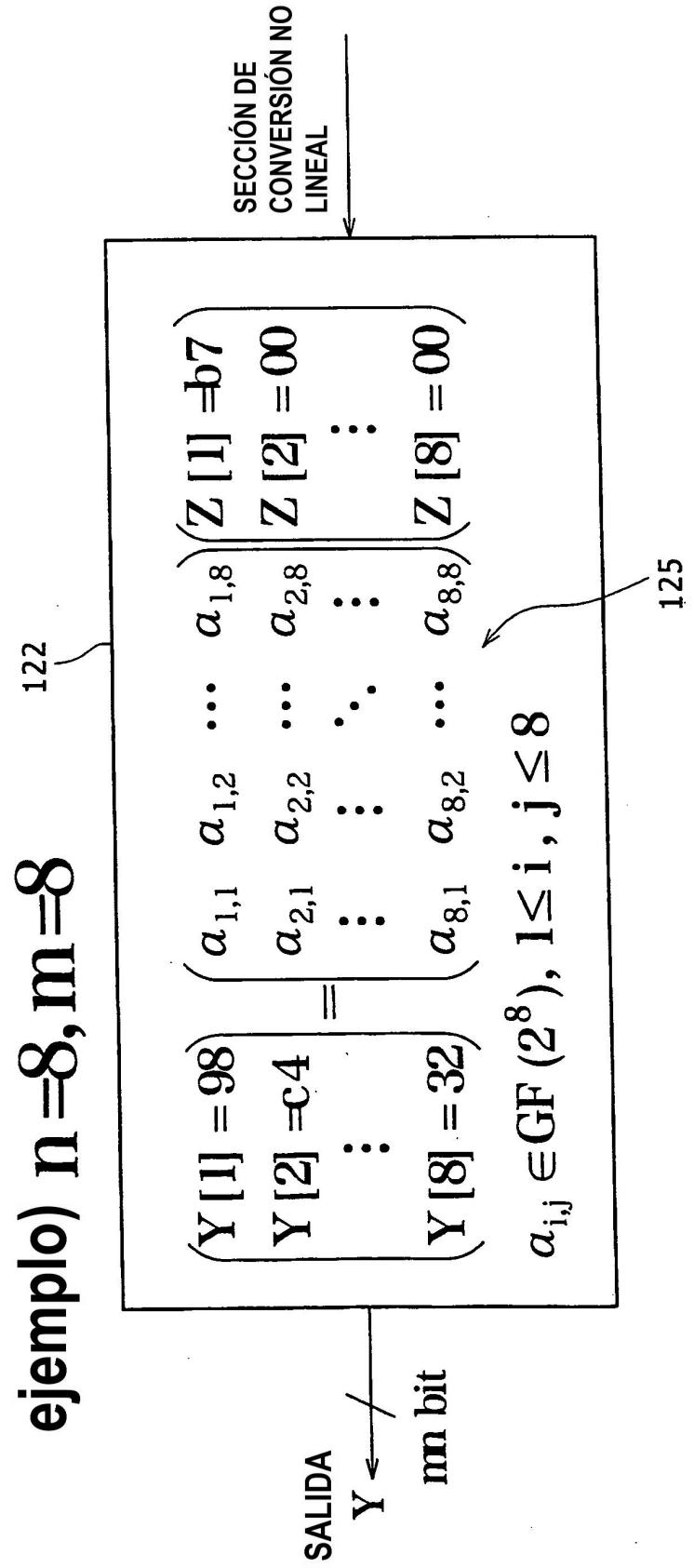

ejemplo) n=8, m=8
122
SECCIÓN DE CONVERSIÓN NO LINEAL
125
SALIDA
Y
m bit

FIG. 6

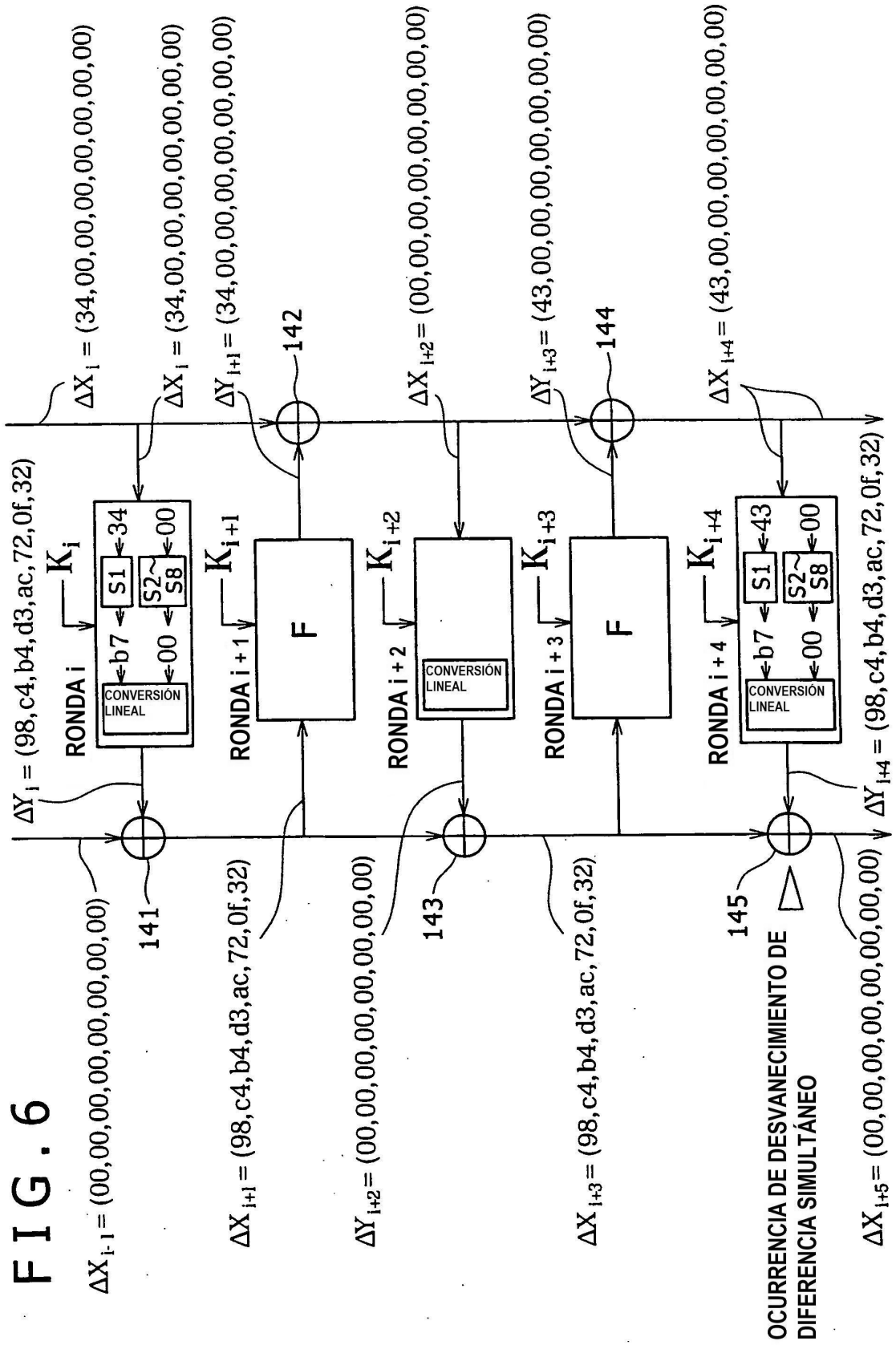

ΔX i-1 = (00,00,00,00,00,00,00,00)
ΔY i = (98,c4,b4,d3,ac,72,0f,32)
ΔX i = (34,00,00,00,00,00,00,00)
RONDA i
Ki
S1
34
S2~S8
00
b7
00
CONVERSIÓN LINEAL
141
ΔY i+1 = (34,00,00,00,00,00,00,00)
142
RONDA i + 1
Ki+1
F
ΔX i+1 = (98,c4,b4,d3,ac,72,0f,32)
ΔX i+2 = (00,00,00,00,00,00,00,00)
RONDA i + 2
Ki+2
CONVERSIÓN LINEAL
143
ΔY i+2 = (00,00,00,00,00,00,00,00)
ΔY i+3 = (43,00,00,00,00,00,00,00)
144
RONDA i + 3
Ki+3
F
ΔX i+3 = (98,c4,b4,d3,ac,72,0f,32)
ΔX i+4 = (43,00,00,00,00,00,00,00)
RONDA i + 4
Ki+4
S1
43
S2~S8
00
b7
00
CONVERSIÓN LINEAL
145
OCURRENCIA DE DESVANECIMIENTO DE DIFERENCIA SIMULTÁNEO
ΔY i+4 = (98,c4,b4,d3,ac,72,0f,32)
ΔX i+5 = (00,00,00,00,00,00,00,00)

FIG. 7

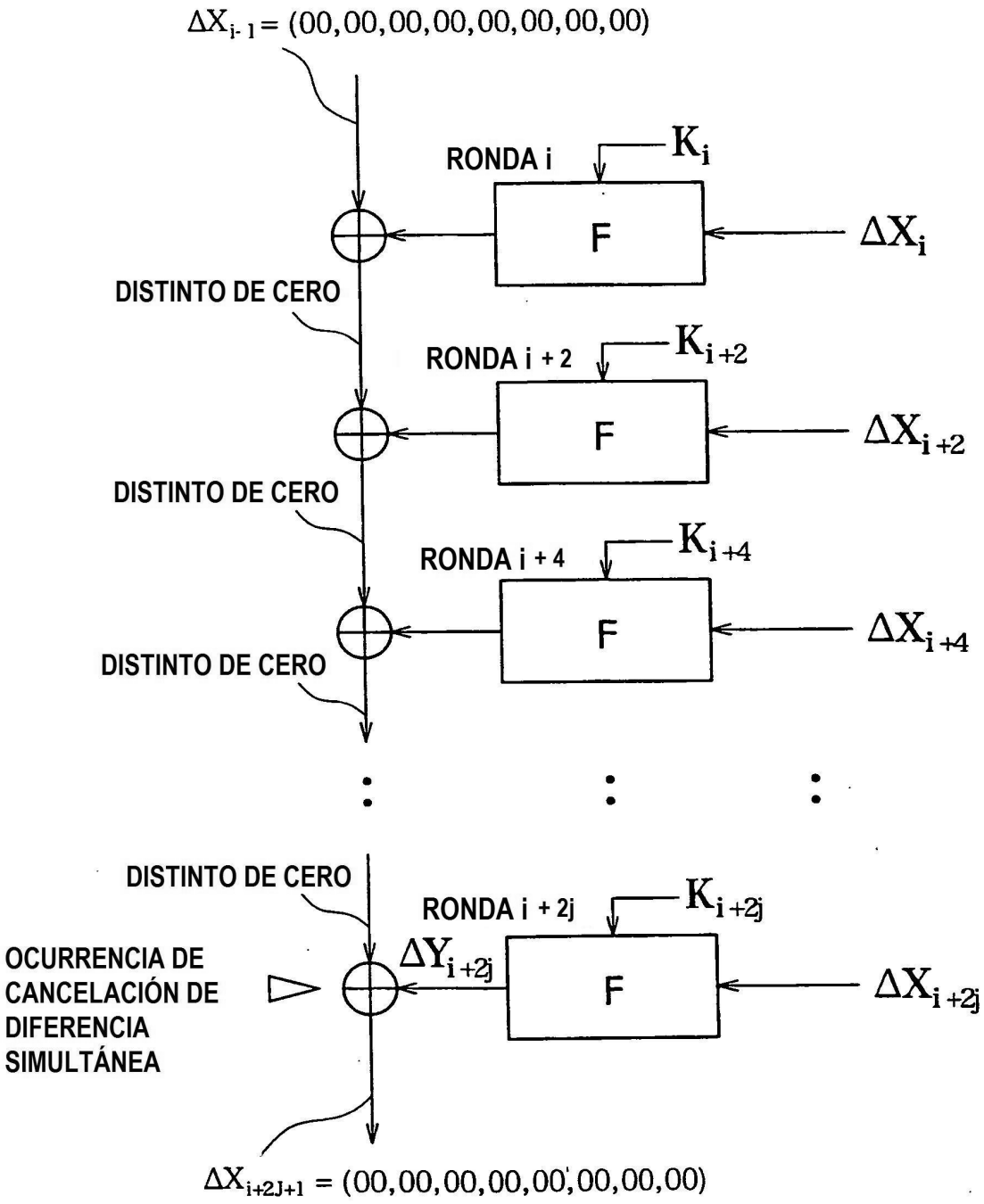

ΔX_{i-1} = (00,00,00,00,00,00,00,00)
RONDA i
K_i
F
ΔX_i
DISTINTO DE CERO
RONDA i + 2
K_{i+2}
F
ΔX_{i+2}
DISTINTO DE CERO
RONDA i + 4
K_{i+4}
F
ΔX_{i+4}
DISTINTO DE CERO
DISTINTO DE CERO
RONDA i + 2j
K_{i+2j}
ΔY_{i+2j}
F
ΔX_{i+2j}
OCURRENCIA DE CANCELACIÓN DE DIFERENCIA SIMULTÁNEA
ΔX_{i+2J+1} = (00,00,00,00,00,00,00,00)

FIG. 8

ejemplo) $n=8, m=8$

$$\begin{pmatrix} 9d & b4 & d3 & 5d & 84 & ae & ec & b9 \\ 29 & 34 & 39 & 60 & 5c & 81 & 25 & 13 \\ 67 & 6a & d2 & e3 & 4b & db & 9d & 4 \\ 8e & d7 & e6 & 1b & 8b & 9e & 3a & 91 \\ d9 & e5 & 4d & dd & c6 & 5 & f0 & ad \\ 2a & f7 & 67 & 72 & b1 & 7 & f2 & 27 \\ 42 & e6 & a0 & 4 & f1 & 4 & 7d & 8c \\ 55 & 63 & fa & 51 & c & d9 & 28 & d6 \end{pmatrix}$$

FIG. 9

EJEMPLO DE CONFIGURACIÓN DE r=6 Y q=3

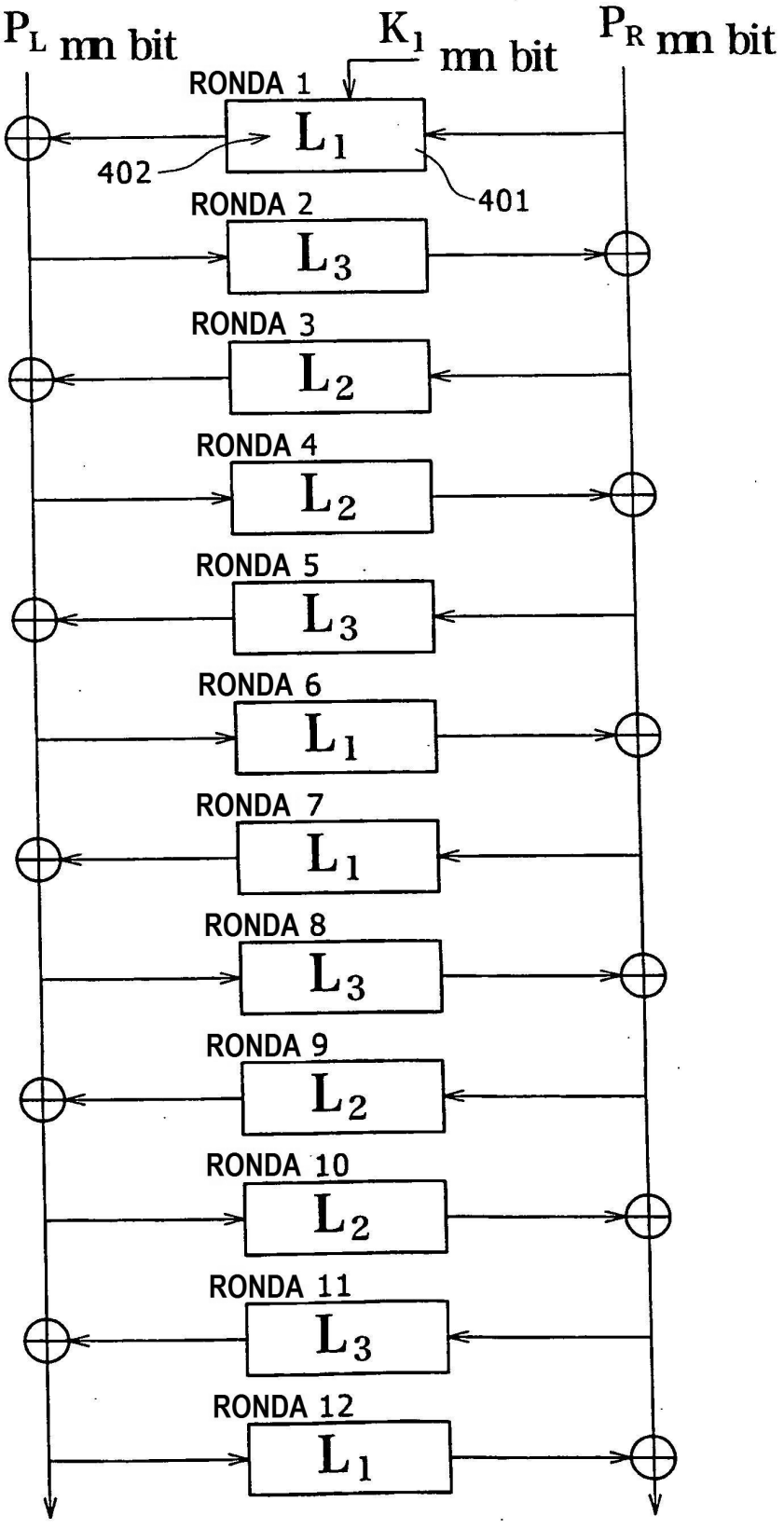


FIG. 10

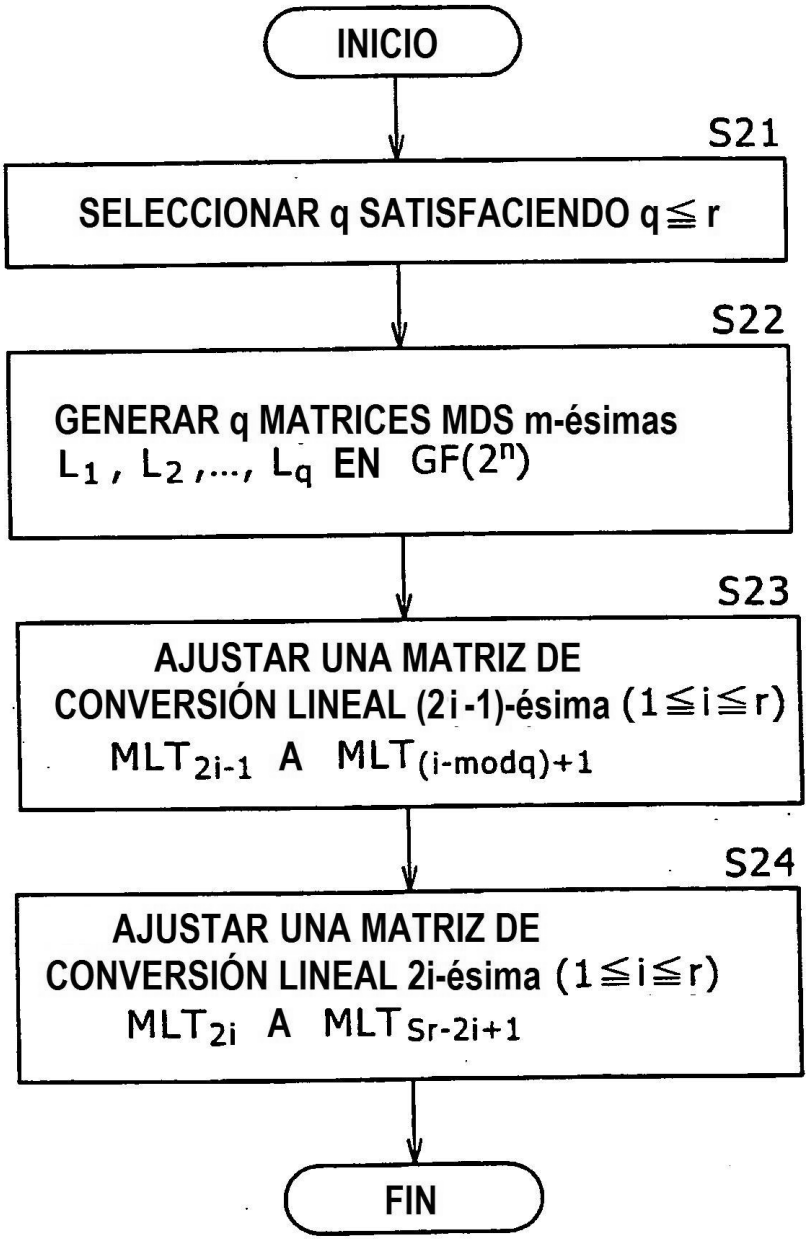

INICIO
S21
SELECCIONAR q SATISFACIENDO q≦r
S22
GENERAR q MATRICES MDS m-ésimas
L1 , L2 ,..., Lq EN GF(2n)
S23
AJUSTAR UNA MATRIZ DE
CONVERSIÓN LINEAL (2i-1)-ésima (1≦i≦r)
MLT2i-1 A MLT(i-modq)+1
S24
AJUSTAR UNA MATRIZ DE
CONVERSIÓN LINEAL 2i-ésima (1≦i≦r)
MLT2i A MLTSr-2i+1
FIN

FIG. 11

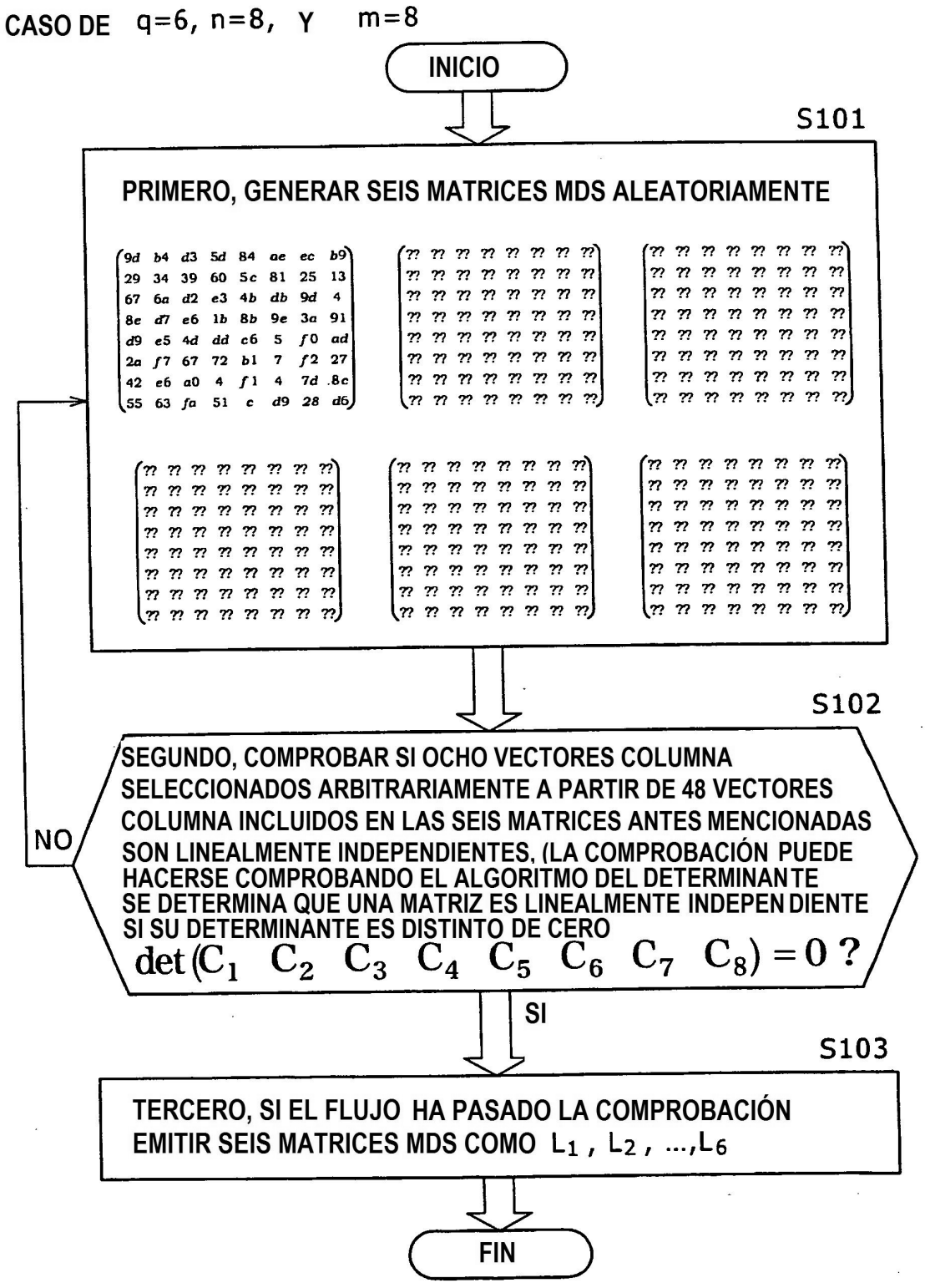

CASO DE q=6, n=8, Y m=8
INICIO
S101
PRIMERO, GENERAR SEIS MATRICES MDS ALEATORIAMENTE
9d b4 d3 5d 84 ae ec b9
29 34 39 60 5c 81 25 13
67 6a d2 e3 4b db 9d 4
8e d7 e6 1b 8b 9e 3a 91
d9 e5 4d dd c6 5 f0 ad
2a f7 67 72 b1 7 f2 27
42 e6 a0 4 f1 4 7d 8c
55 63 fa 51 c d9 28 d6
S102
SEGUNDO, COMPROBAR SI OCHO VECTORES COLUMNA SELECCIONADOS ARBITRARIAMENTE A PARTIR DE 48 VECTORES COLUMNA INCLUIDOS EN LAS SEIS MATRICES ANTES MENCIONADAS SON LINEALMENTE INDEPENDIENTES, (LA COMPROBACIÓN PUEDE HACERSE COMPROBANDO EL ALGORITMO DEL DETERMINANTE SE DETERMINA QUE UNA MATRIZ ES LINEALMENTE INDEPENDIENTE SI SU DETERMINANTE ES DISTINTO DE CERO
det(C1 C2 C3 C4 C5 C6 C7 C8) = 0 ?
NO
SI
S103
TERCERO, SI EL FLUJO HA PASADO LA COMPROBACIÓN EMITIR SEIS MATRICES MDS COMO L1, L2, ..., L6
FIN

FIG. 12

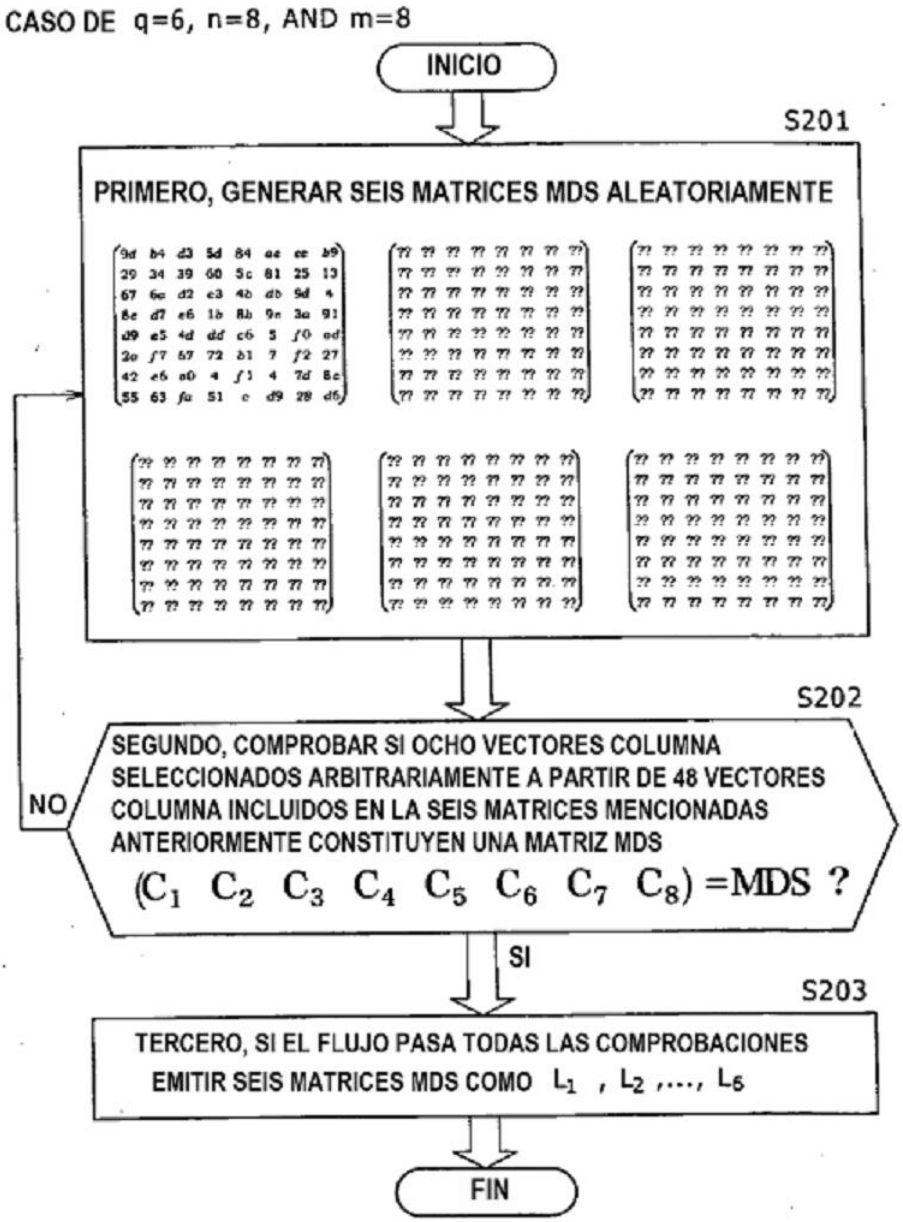

CASO DE q=6, n=8, AND m=8
INICIO
S201
PRIMERO, GENERAR SEIS MATRICES MDS ALEATORIAMENTE
S202
SEGUNDO, COMPROBAR SI OCHO VECTORES COLUMNA SELECCIONADOS ARBITRARIAMENTE A PARTIR DE 48 VECTORES COLUMNA INCLUIDOS EN LA SEIS MATRICES MENCIONADAS ANTERIORMENTE CONSTITUYEN UNA MATRIZ MDS
(C1 C2 C3 C4 C5 C6 C7 C8) =MDS ?
NO
SI
S203
TERCERO, SI EL FLUJO PASA TODAS LAS COMPROBACIONES EMITIR SEIS MATRICES MDS COMO L1 , L2 ,..., L6
FIN

FIG. 13

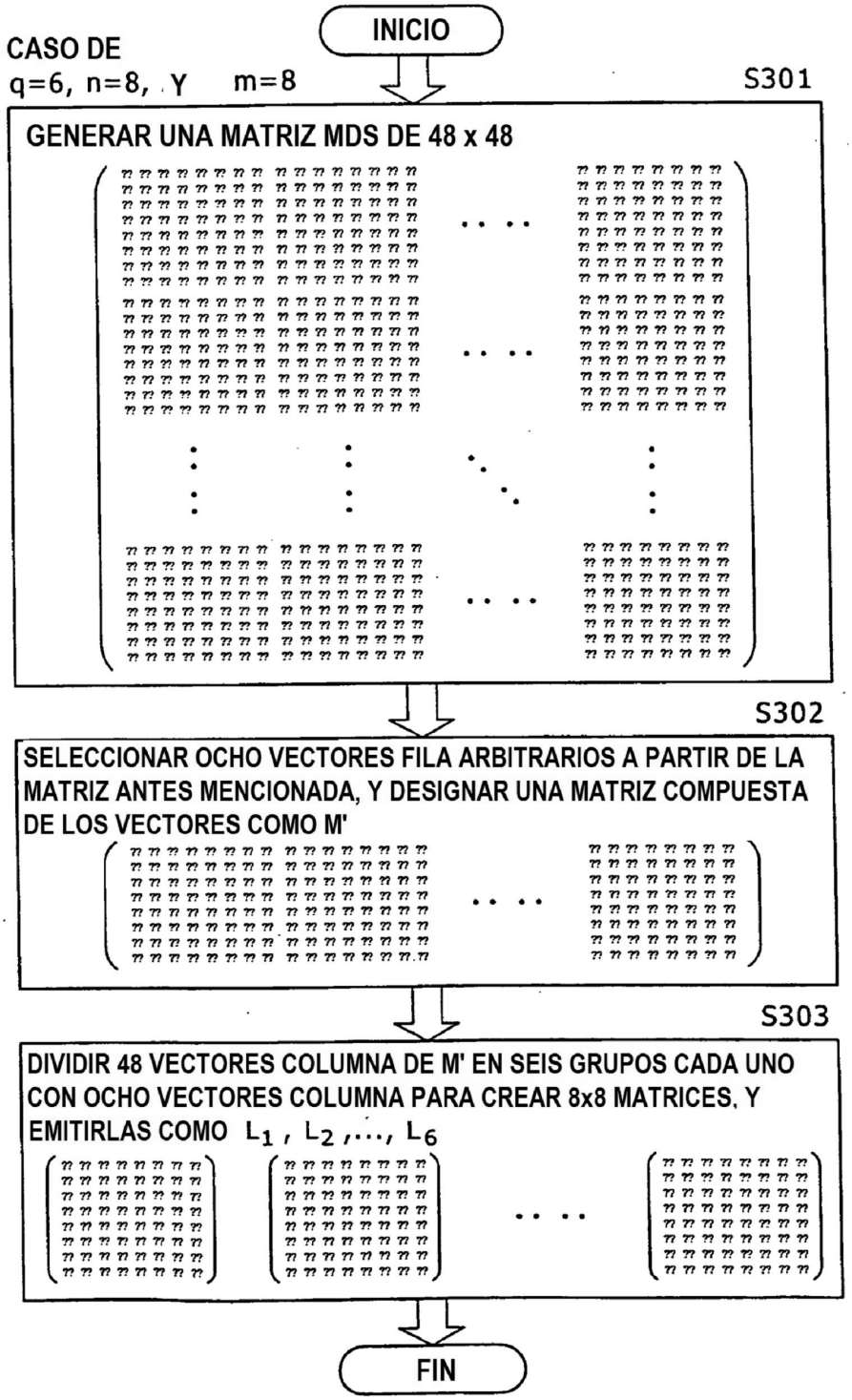

INICIO
CASO DE
q=6, n=8, Y m=8
S301
GENERAR UNA MATRIZ MDS DE 48 x 48
S302
SELECCIONAR OCHO VECTORES FILA ARBITRARIOS A PARTIR DE LA MATRIZ ANTES MENCIONADA, Y DESIGNAR UNA MATRIZ COMPUESTA DE LOS VECTORES COMO M'
S303
DIVIDIR 48 VECTORES COLUMNA DE M' EN SEIS GRUPOS CADA UNO CON OCHO VECTORES COLUMNA PARA CREAR 8x8 MATRICES, Y EMITIRLAS COMO L1 , L2 ,..., L6
FIN

FIG. 14

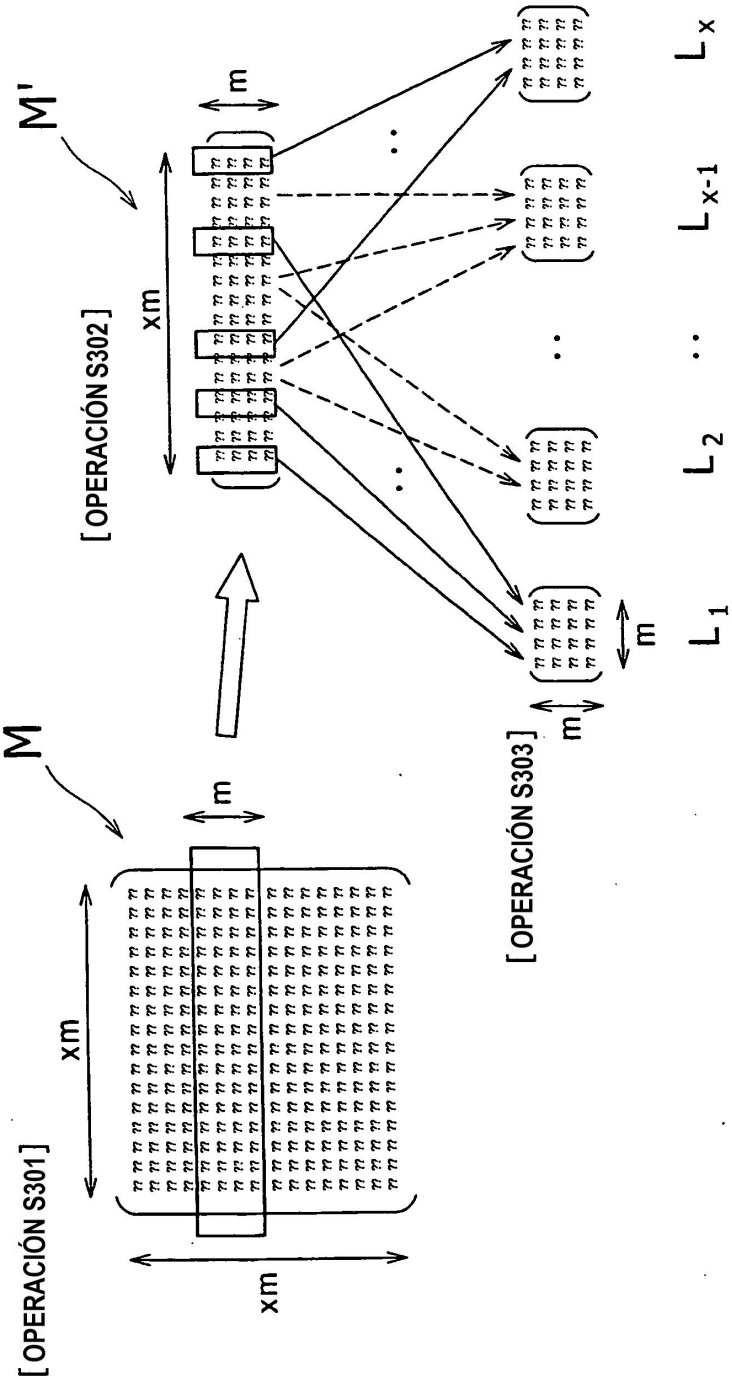

M
M'
m
xm
[OPERACIÓN S301]
[OPERACIÓN S302]
[OPERACIÓN S303]
L1
L2
Lx-1
Lx

FIG. 15

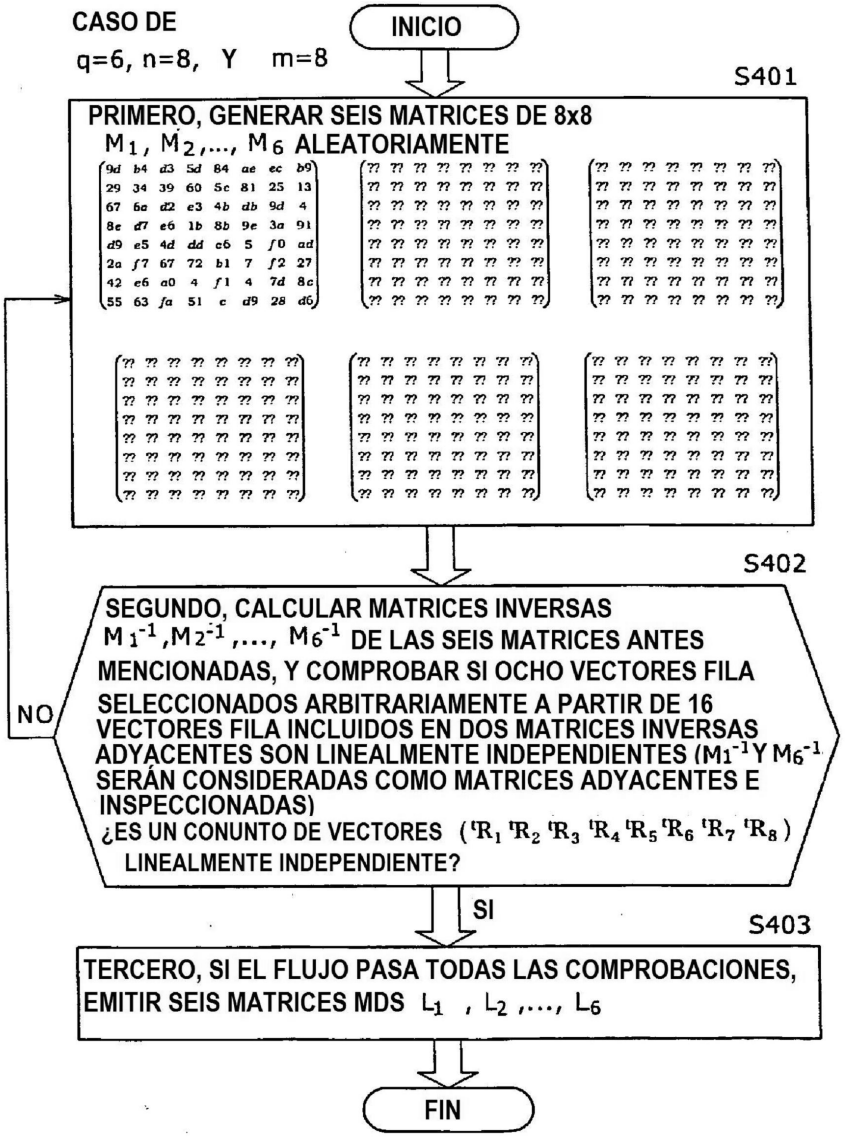

CASO DE
q=6, n=8, Y m=8
INICIO
S401
PRIMERO, GENERAR SEIS MATRICES DE 8x8
M1, M2,..., M6 ALEATORIAMENTE
S402
SEGUNDO, CALCULAR MATRICES INVERSAS
M1-1, M2-1,..., M6-1 DE LAS SEIS MATRICES ANTES MENCIONADAS, Y COMPROBAR SI OCHO VECTORES FILA SELECCIONADOS ARBITRARIAMENTE A PARTIR DE 16 VECTORES FILA INCLUIDOS EN DOS MATRICES INVERSAS ADYACENTES SON LINEALMENTE INDEPENDIENTES (M1-1 Y M6-1 SERÁN CONSIDERADAS COMO MATRICES ADYACENTES E INSPECCIONADAS)
¿ES UN CONUNTO DE VECTORES (tR1 tR2 tR3 tR4 tR5 tR6 tR7 tR8) LINEALMENTE INDEPENDIENTE?
NO
SI
S403
TERCERO, SI EL FLUJO PASA TODAS LAS COMPROBACIONES, EMITIR SEIS MATRICES MDS L1 , L2 ,..., L6
FIN

FIG. 16

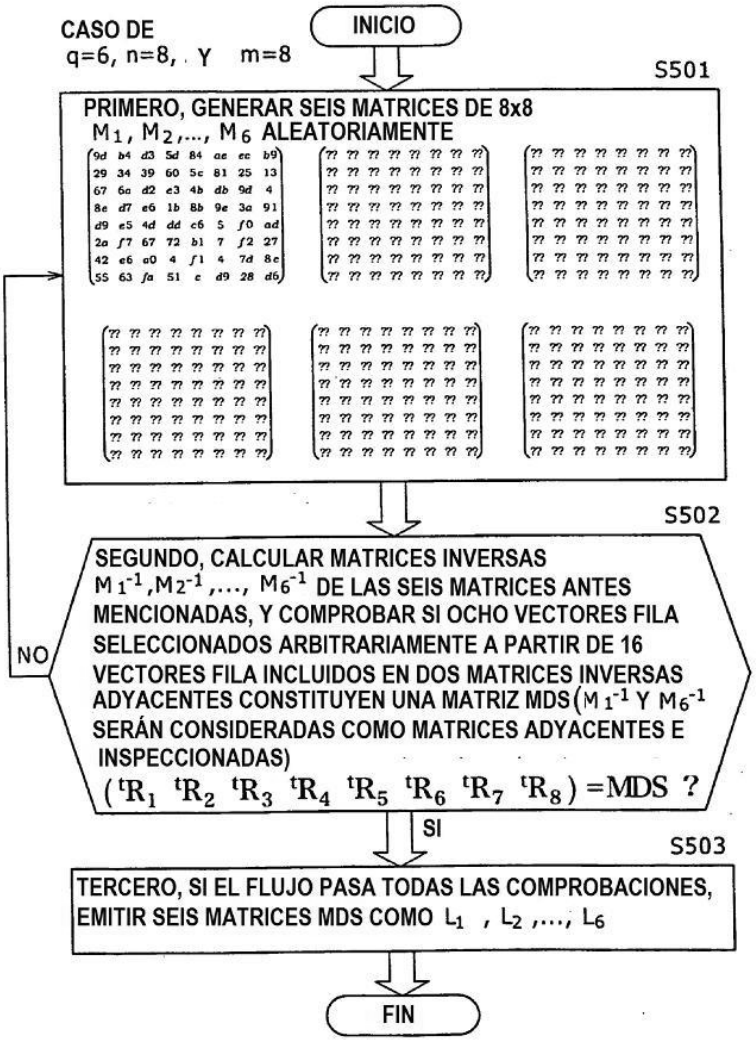

CASO DE
q=6, n=8, Y m=8
INICIO
S501
PRIMERO, GENERAR SEIS MATRICES DE 8x8
M1, M2,..., M6 ALEATORIAMENTE
S502
SEGUNDO, CALCULAR MATRICES INVERSAS
M1-1, M2-1,..., M6-1 DE LAS SEIS MATRICES ANTES MENCIONADAS, Y COMPROBAR SI OCHO VECTORES FILA SELECCIONADOS ARBITRARIAMENTE A PARTIR DE 16 VECTORES FILA INCLUIDOS EN DOS MATRICES INVERSAS ADYACENTES CONSTITUYEN UNA MATRIZ MDS (M1-1 Y M6-1 SERÁN CONSIDERADAS COMO MATRICES ADYACENTES E INSPECCIONADAS)
(tR1 tR2 tR3 tR4 tR5 tR6 tR7 tR8) =MDS ?
NO
SI
S503
TERCERO, SI EL FLUJO PASA TODAS LAS COMPROBACIONES, EMITIR SEIS MATRICES MDS COMO L1 , L2 ,..., L6
FIN

FIG. 17

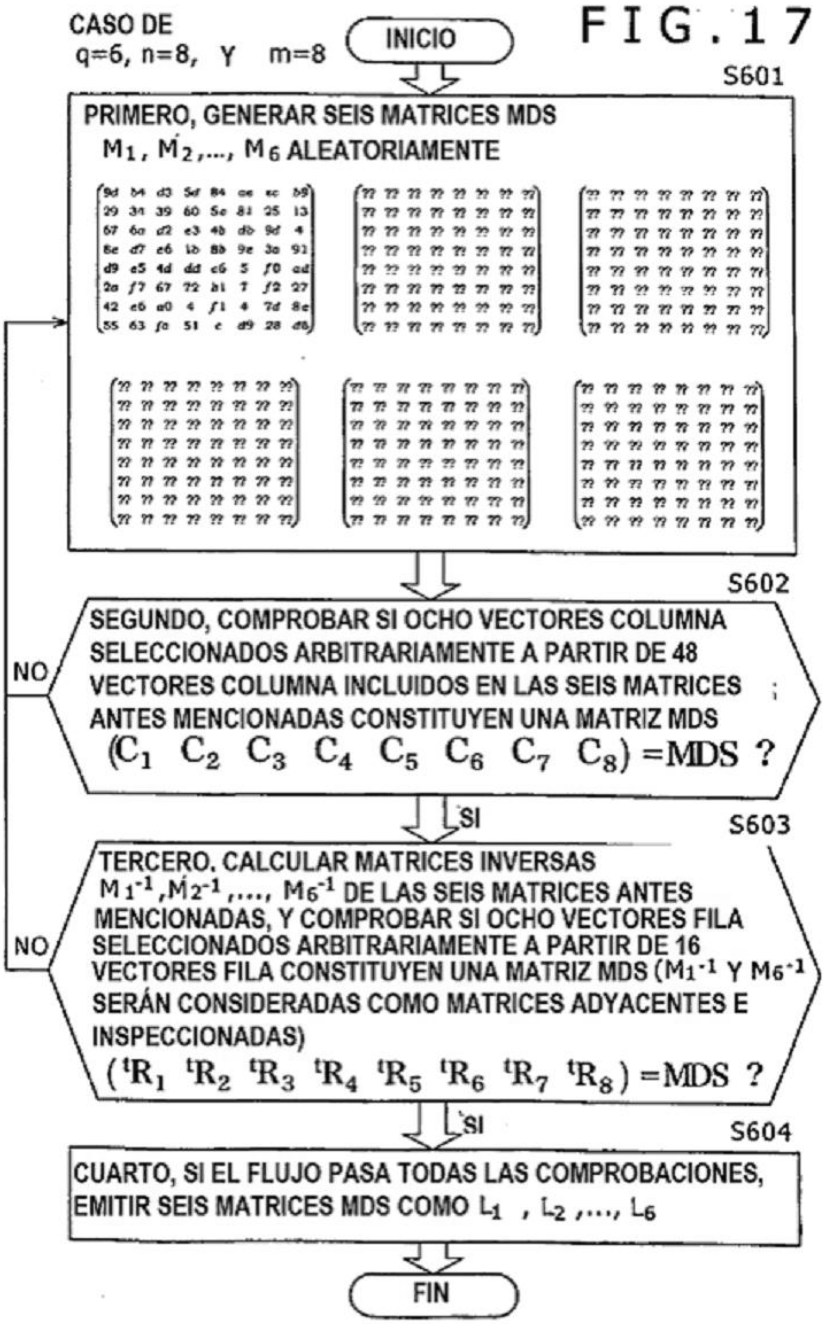
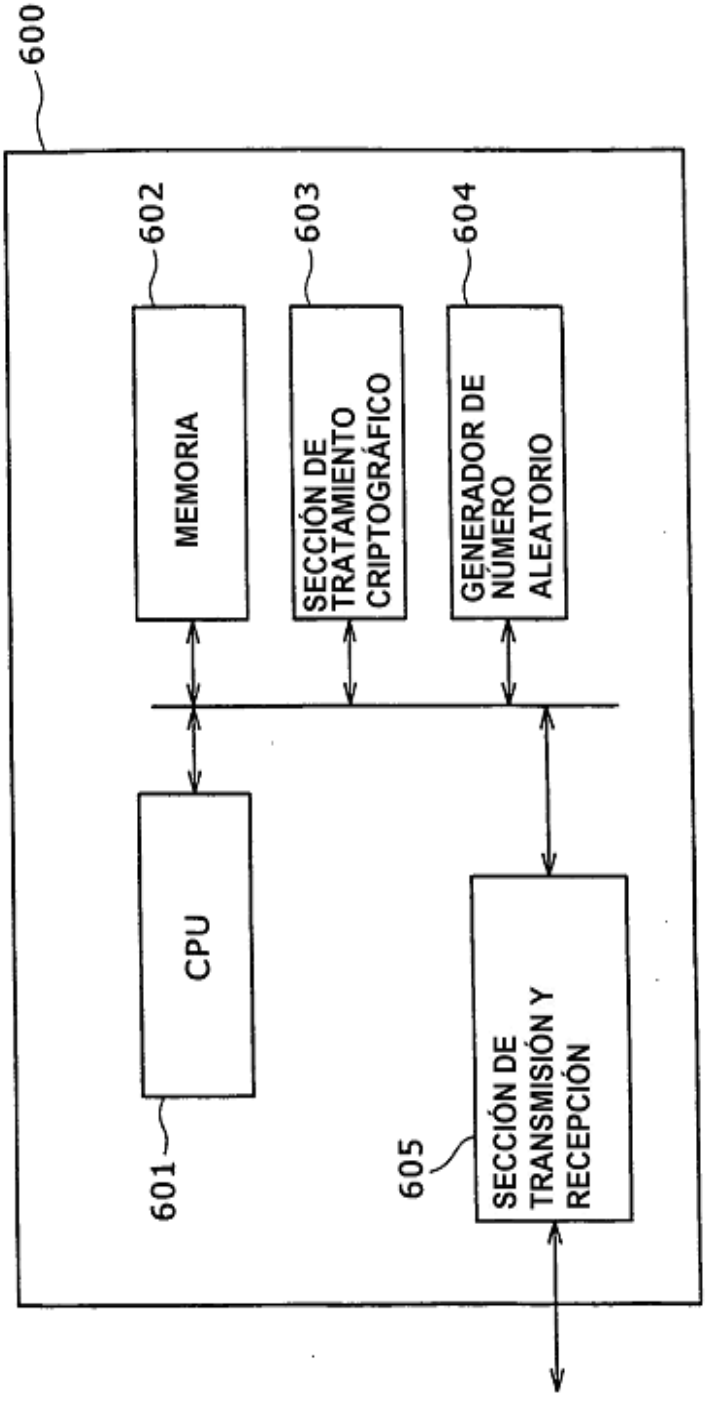

CASO DE
q=6, n=8, Y m=8
INICIO
S601
PRIMERO, GENERAR SEIS MATRICES MDS
M1, M2,..., M6 ALEATORIAMENTE
S602
SEGUNDO, COMPROBAR SI OCHO VECTORES COLUMNA SELECCIONADOS ARBITRARIAMENTE A PARTIR DE 48 VECTORES COLUMNA INCLUIDOS EN LAS SEIS MATRICES ANTES MENCIONADAS CONSTITUYEN UNA MATRIZ MDS
(C1 C2 C3 C4 C5 C6 C7 C8) =MDS ?
NO
SI
S603
TERCERO. CALCULAR MATRICES INVERSAS M1-1, M2-1,..., M6-1 DE LAS SEIS MATRICES ANTES MENCIONADAS, Y COMPROBAR SI OCHO VECTORES FILA SELECCIONADOS ARBITRARIAMENTE A PARTIR DE 16 VECTORES FILA CONSTITUYEN UNA MATRIZ MDS (M1-1 Y M6-1 SERÁN CONSIDERADAS COMO MATRICES ADYACENTES E INSPECCIONADAS)
(tR1 tR2 tR3 tR4 tR5 tR6 tR7 tR8) =MDS ?
NO
SI
S604
CUARTO, SI EL FLUJO PASA TODAS LAS COMPROBACIONES, EMITIR SEIS MATRICES MDS COMO L1 , L2 ,..., L6
FIN

FIG.18


600
602
603
604
MEMORIA
SECCIÓN DE TRATAMIENTO CRIPTOGRÁFICO
GENERADOR DE NÚMERO ALEATORIO
CPU
601
605
SECCIÓN DE TRANSMISIÓN Y RECEPCIÓN