(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 879 845**

(51) Int. CI.:

H04L 9/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.08.2005 E 10011885 (0)**

(97) Fecha y número de publicación de la concesión europea: **16.06.2021 EP 2375625**

(54) Título: **Sobre el cifrado de Feistel mediante el uso de mapeos de difusión óptimos a lo largo de múltiples rondas**

(30) Prioridad:

03.09.2004 JP 2004256465

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.11.2021

(73) Titular/es:

SONY GROUP CORPORATION (100.0%)
1-7-1 Konan Minato-ku
Tokyo 108-0075, JP

(72) Inventor/es:

SHIRAI, TAIZO y
PRENEEL, BART

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Sobre el cifrado de Feistel mediante el uso de mapeos de difusión óptimos a lo largo de múltiples rondas

Campo técnico

La presente invención se refiere a un aparato de procesamiento criptográfico, a un método de procesamiento criptográfico y a un programa de ordenador para ello, y, de manera más específica, a un aparato de procesamiento criptográfico con resistencia mejorada al análisis lineal y análisis diferencial conocidos como procesamiento de análisis de descifrado y procesamiento de ataque de criptoanálisis, a un método de procesamiento criptográfico y a un programa de ordenador para ello.

Antecedentes de la técnica

Actualmente, con el desarrollo de las comunicaciones en red y del comercio electrónico, una seguridad que garantice las comunicaciones se ha convertido en una cuestión vital. Un medio de garantizar la seguridad es una tecnología criptográfica y, hoy en día, se están ejecutando, en realidad, comunicaciones que utilizan varias técnicas criptográficas.

Por ejemplo, se ha puesto en práctica un sistema en el cual un módulo de procesamiento criptográfico se incorpora a un pequeño dispositivo como, por ejemplo, una tarjeta IC, la transmisión y recepción de datos se llevan a cabo entre la tarjeta IC y un lector/escritor que actúa como un dispositivo de lectura y escritura de datos, y se lleva a cabo el procesamiento de autenticación o cifrado/descifrado de los datos de envío/recepción.

Existen varios algoritmos en el procesamiento criptográfico, los cuales se dividen ampliamente en el sistema criptográfico de una clave en el cual una clave de cifrado y una clave de descifrado diferentes, por ejemplo, una clave pública y una clave secreta, se establecen y el sistema criptográfico de clave común en el cual una clave común se establece como una clave de cifrado y una clave de descifrado.

Existen también varios algoritmos en el sistema criptográfico de clave común. Uno de ellos es un sistema en el cual múltiples claves se generan mediante el uso de una clave común como una base y el procesamiento de conversión de datos se lleva a cabo de manera repetida para cada unidad de bloque (64 bits, 128 bits, etc.) mediante el uso de las múltiples claves generadas. Un algoritmo típico que aplica dicho método de generación de clave y procesamiento de conversión de datos es un método criptográfico en bloque de clave común.

Como un algoritmo típico de procesamiento criptográfico en bloque de clave común, por ejemplo, existe un algoritmo DES (estándar de cifrado de datos, DES, por sus siglas en inglés) como un cifrado estándar federal de los Estados Unidos y se usa ampliamente en varios campos.

Cualquier algoritmo del procesamiento criptográfico en bloque de clave común tipificado por el DES puede dividirse principalmente en una sección de función de ronda para llevar a cabo la conversión de datos de entrada y una sección de planificación de clave para generar una clave que se aplicará en cada ronda de una parte de función (función F) de ronda. Una clave de ronda (subclave) que se aplicará en cada ronda de la sección de función de ronda se genera en la sección de planificación de clave en la cual se ingresa una clave maestra (clave principal), y se aplica en cada parte de función de ronda.

Sin embargo, en dicho procesamiento criptográfico de clave común, la fuga de la clave por el criptoanálisis se ha convertido en un problema. Como una técnica típica de criptoanálisis o técnica de ataque, se conocen un análisis diferencial (también llamado método de criptoanálisis diferencial o ataque de criptoanálisis diferencial) en el cual una clave de aplicación en cada función de ronda se analiza mediante el análisis de muchos datos de entrada (texto en lenguaje claro) y sus datos de salida (texto cifrado), y un análisis lineal (también llamado método de criptoanálisis lineal o ataque de criptoanálisis lineal) que lleva a cabo un análisis según textos en lenguaje claro y textos cifrados correspondientes.

Que es fácil analizar una clave mediante criptoanálisis significa baja seguridad del procesamiento criptográfico. En el algoritmo DES convencional, existe el problema de que, dado que el procesamiento (matriz de conversión) que se aplicará en una sección de conversión lineal en una sección función de ronda (función F) es equivalente en una ronda de cada etapa, el criptoanálisis es fácil de llevar a cabo y, en consecuencia, resulta en un análisis fácil de la clave.

El documento US 2002/0016773 A1 se refiere a un aparato y método de cifrado, y a un aparato y método de descifrado basado en el cifrado por bloques, en donde cada una de las secciones de cifrado comprende primeras unidades de transformación no lineal configuradas para llevar a cabo un proceso de transformación no lineal en los primeros datos de subbloque, y una primera unidad de difusión lineal configurada para llevar a cabo un proceso de difusión lineal en datos producidos desde las primeras unidades de transformación no lineal con respecto a un rango que es más amplio que un rango de los primeros datos de subbloque y proveer un resultado de difusión a las primeras unidades de transformación no lineal en una sección de cifrado subsiguiente. Cada una de las primeras unidades de transformación no lineal comprende segundas unidades de transformación no lineal configuradas para

llevar a cabo un proceso de transformación no lineal en segundos datos de subbloque que se obtienen mediante la división de los primeros datos de subbloque; y una segunda unidad de difusión lineal configurada para llevar a cabo un proceso de difusión lineal en datos producidos desde las segundas unidades de transformación no lineal con respecto al rango de los primeros datos de subbloque. El documento se centra en la provisión de diferentes cajas-S como unidades de transformación no lineal y solo menciona una única matriz MDS que se utilizará en procesos de transformación lineal. El documento describe diferentes matrices MDS que podrán utilizarse como la única matriz MDS en el proceso.

En el artículo de TAIZO SHIRAI *ET AL.*: "*Improving Immunity of Feistel Ciphers against Differential Cryptanalysis by Using Multiple MDS matrices*", 14 de julio de 2004, *FAST SOFTWARE ENCRYPTION*; *[LECTURE NOTES IN COMPUTER SCIENCE;;LNCS]*, SPRINGER-VERLAG, BERLIN/HEIDELBERG, PÁGINA(S) 260-278, XP019007568, ISBN: 978-3-540-22171-5, los autores comienzan con el descubrimiento de que el porcentaje de cajas-S activas en Cifrados de Feistel es más bajo que en otros procesos. Los autores proponen una nueva estrategia de diseño para evitar propiedades de cancelación de diferencias de estructuras Feistel mediante el empleo de mújltiples matrices basadas en MDS en la capa de difusión de la función F.

Descripción de la invención

Problema a resolver mediante la invención

La presente invención se lleva a cabo teniendo en cuenta los problemas descritos más arriba, y tiene como objeto proveer un aparato de procesamiento criptográfico que realice un algoritmo criptográfico en bloques de clave común altamente resistente al análisis lineal y al análisis diferencial, un método de procesamiento criptográfico, y un respectivo aparato de procesamiento para ello.

Medios para resolver el problema

El problema se resuelve por el objeto de las reivindicaciones independientes. Un primer aspecto de los ejemplos se dirige a un aparato de procesamiento criptográfico para llevar a cabo el procesamiento criptográfico en bloques de clave común tipo Feistel, que se configura para ejecutar una función F del tipo SPN con una sección de conversión no lineal y la sección de conversión lineal en múltiples rondas, en donde la sección de conversión lineal de la función F correspondiente a cada una de las múltiples rondas tiene una configuración para llevar a cabo el procesamiento de conversión lineal para n bits producidos desde cada una de las m secciones de conversión no lineal, en total mn bits, como procesamiento de conversión lineal que aplica matrices MDS (distancia máxima separable, MDS, por sus siglas en inglés) cuadradas, y al menos en las rondas consecutivas numeradas con pares y en las rondas consecutivas numeradas con impares, se aplican diferentes matrices MDS cuadradas L_a, L_b, y una matriz compuesta de m vectores de columna seleccionados de forma arbitraria de los vectores de columna que constituyen matrices inversas de las matrices MDS cuadradas L_a^{-1}, L_b^{-1} es linealmente independiente.

Además, en una realización del aparato de procesamiento criptográfico de un ejemplo, el aparato de procesamiento criptográfico se caracteriza por que una matriz compuesta de m vectores de columna seleccionados de forma arbitraria de los vectores de columna que constituyen las matrices inversas L_a^{-1}, L_b^{-1} es una matriz MDS cuadrada.

Además, en una realización del aparato de procesamiento criptográfico de un ejemplo, su algoritmo se caracteriza por que el algoritmo del procesamiento criptográfico en bloques de clave común tipo Feistel es un algoritmo criptográfico de número de ronda 2r, y la sección de conversión lineal de la función F se configura para llevar a cabo el procesamiento de conversión lineal que aplica q tipos ($2 \leq q < r$) de diferentes matrices MDS cuadradas de manera secuencial y repetida en todas las r rondas numeradas con pares y en todas las r rondas numeradas con impares.

Además, en una realización del aparato de procesamiento criptográfico de un ejemplo, el aparato de procesamiento criptográfico se caracteriza por que cada una de las múltiples matrices MDS cuadradas que se aplicarán en la sección de conversión lineal de la función F es una matriz MDS cuadrada que está compuesta de m vectores de columna seleccionados de forma arbitraria de los vectores de columna que constituyen las múltiples matrices MDS cuadradas y es linealmente independiente.

Además, en una realización del aparato de procesamiento criptográfico de un ejemplo, el aparato de procesamiento criptográfico se caracteriza por que cada una de las múltiples matrices MDS cuadradas que se aplicarán en la sección de conversión lineal de la función F es una matriz MDS cuadrada de modo que una matriz compuesta de m vectores de columna seleccionados de forma arbitraria de los vectores de columna que constituyen las múltiples matrices MDS cuadradas también constituye una matriz MDS cuadrada.

Además, en una realización del aparato de procesamiento criptográfico de un ejemplo, el aparato de procesamiento criptográfico se caracteriza por que cada una de las múltiples matrices MDS cuadradas que se aplicarán en la sección de conversión lineal de la función F está compuesta de una matriz que está compuesta de vectores de columna extraídos de una matriz M' compuesta de vectores de fila seleccionados de un vector MDS cuadrado M que incluye todos los elementos que constituyen las múltiples matrices MDS cuadradas.

Un segundo aspecto de los ejemplos es un método criptográfico para llevar a cabo el procesamiento criptográfico por bloque de clave común tipo Feistel, caracterizado por que la función F del tipo SPN para llevar a cabo el procesamiento de conversión no lineal y el procesamiento de conversión lineal se lleva a cabo de manera repetida en múltiples rondas, el procesamiento de conversión lineal de la función F correspondiente a las múltiples rondas lleva a cabo el procesamiento de conversión lineal de n bits producidos desde las m secciones de conversión no lineal, en total mn bits, como procesamiento de conversión lineal que aplica matrices MDS (distancia máxima separable) cuadradas, al menos en las rondas consecutivas numeradas con pares y en las rondas consecutivas numeradas con impares se aplican diferentes matrices MDS cuadradas L_a^{-1}, L_b^{-1}, y se lleva a cabo el procesamiento de conversión lineal con matrices MDS cuadradas de modo que una matriz compuesta de m vectores de columna seleccionados de forma arbitraria de los vectores de columna que constituyen las matrices inversas L_a^{-1}, L_b^{-1} de las matrices MDS cuadradas es linealmente independiente.

Además, en una realización del método de procesamiento criptográfico de un ejemplo, el aparato de procesamiento criptográfico se caracteriza por que lleva a cabo el procesamiento de conversión lineal con matrices MDS cuadradas de modo que una matriz compuesta de m vectores de columna seleccionados de forma arbitraria de los vectores de columna que constituyen las matrices inversas L_a^{-1}, L_b^{-1} es una matriz MDS cuadrada.

Además, en una realización del método de procesamiento criptográfico de un ejemplo, el algoritmo del procesamiento criptográfico por bloque de clave común tipo Feistel se caracteriza por que es un algoritmo criptográfico de número de ronda 2r, en donde el procesamiento de conversión lineal de la función F es la ejecución del procesamiento de conversión lineal mediante la aplicación de q ($2 \leq q < r$) tipos de diferentes matrices MDS cuadradas de manera secuencial y repetida en todas las r rondas numeradas con pares y en todas las r rondas numeradas con impares.

Además, en una realización del método de procesamiento criptográfico de un ejemplo, el método de procesamiento criptográfico se caracteriza por que cada una de las múltiples matrices MDS cuadradas diferentes que se aplicarán al procesamiento de conversión lineal en la función F es una matriz MDS cuadrada que está compuesta de m vectores de columna seleccionados de forma arbitraria de los vectores de columna que constituyen las múltiples matrices MDS cuadradas y es linealmente independiente.

Además, en una realización del método de procesamiento criptográfico de un ejemplo, el método de procesamiento criptográfico se caracteriza por que cada una de las múltiples matrices MDS cuadradas diferentes que se aplicarán al procesamiento de conversión lineal de la función F es una matriz MDS cuadrada de modo que una matriz compuesta de m vectores de columna seleccionados de forma arbitraria de los vectores de columna que constituyen las múltiples matrices MDS cuadradas también es una matriz MDS cuadrada.

Además, en una realización del método de procesamiento criptográfico de un ejemplo, el método de procesamiento criptográfico se caracteriza por que cada una de las múltiples matrices MDS cuadradas diferentes que se aplicarán al procesamiento de conversión lineal de la función F está compuesta de una matriz compuesta de vectores de columna seleccionados de una matriz M' compuesta de vectores de fila seleccionados de una matriz MDS cuadrada que incluye todos los elementos que constituyen las múltiples matrices MDS cuadradas.

Un tercer aspecto de los ejemplos es un programa de ordenador para llevar a cabo el procesamiento criptográfico por bloque de clave común tipo Feistel, el cual comprende la etapa de ejecutar, de forma repetida, la función F del tipo SPN de llevar a cabo el procesamiento de conversión no lineal y el procesamiento de conversión lineal en múltiples rondas, en donde el procesamiento de conversión lineal de la función F correspondiente a cada una de las múltiples rondas es una etapa de conversión lineal de llevar a cabo el procesamiento de conversión lineal de una entrada de n bits producidos desde cada una de las m secciones de conversión no lineal, en total mn bit, como procesamiento de conversión lineal que aplica matrices MDS (distancia máxima separable) cuadradas. En la etapa de conversión lineal, al menos en las rondas consecutivas numeradas con pares y en las rondas consecutivas numeradas con impares, se aplican diferentes matrices MDS cuadradas L_a, L_b, y cada una de las matrices MDS cuadradas es tal que una matriz compuesta de m vectores de columna seleccionados de forma arbitraria de los vectores de columna que constituyen las matrices inversas L_a^{-1}, L_b^{-1} de las matrices MDS cuadradas es linealmente independiente.

Es preciso observar que el programa de ordenador de un ejemplo es un programa de ordenador que puede proveerse, por ejemplo, a un sistema de ordenador que puede ejecutar varios códigos de programa por medio de cualquier medio de almacenamiento y medio de comunicación en una forma legible por ordenador (por ejemplo, medio de almacenamiento de un CD, FD, MO, etc., o medio de comunicación de una red, etc.). Mediante la provisión de dicho programa en la forma legible por ordenador, el procesamiento que corresponde al programa se lleva a cabo en un sistema de ordenador.

Otros objetos, características y ventajas adicionales de la presente invención serán aparentes a partir de la siguiente descripción de las realizaciones preferidas de la presente invención según se ilustra en los dibujos anexos. Es preciso observar que, en la presente descripción, el sistema es uno que tiene una estructura de combinación lógica de múltiples dispositivos, pero no se encuentra limitado a sistemas que tienen, cada uno, sus propios dispositivos en el mismo recinto.

Según la configuración de un ejemplo, el procesamiento criptográfico se configura de la siguiente manera en el procesamiento criptográfico por bloque de clave común tipo Feistel de ejecución de la función F del tipo SPN que tiene la sección de conversión no lineal y la sección de conversión lineal de forma repetida en múltiples rondas: El procesamiento de conversión lineal de la función F correspondiente a cada una de las múltiples rondas se ejecuta como procesamiento de conversiones lineales que aplica matrices MDS (distancia máxima separable) cuadradas. Y se configura para ejecutar el procesamiento de conversión lineal con matrices MDS cuadradas en donde se aplican matrices MDS cuadradas L_a, L_b que son diferentes al menos en las rondas consecutivas numeradas con pares y en las rondas consecutivas numeradas con impares, y una matriz compuesta de m vectores de columna seleccionados de forma arbitraria de los vectores de columna que constituyen las matrices inversas L_a^{-1}, L_b^{-1} de las matrices MDS cuadradas es linealmente independiente o constituye una matriz MDS cuadrada. Por consiguiente, la resistencia a ataques de criptoanálisis lineal en el cifrado por bloque de clave común se mejora y la dificultad para analizar una clave de cifrado, etc., aumenta; por lo tanto, se lleva a cabo un procesamiento criptográfico de alta seguridad.

Además, según la configuración de un ejemplo, en el procesamiento del procesamiento criptográfico por bloque de clave común tipo Feistel en el cual la función F del tipo SPN que tiene la sección de conversión no lineal y la sección de conversión lineal se ejecuta de manera repetida en múltiples rondas, el procesamiento de conversión lineal de la función F correspondiente a cada una de las múltiples rondas se ejecuta como procesamiento de conversión lineal que aplica matrices MDS (distancia máxima separable) cuadradas, mientras el procesamiento se configura de manera tal que se aplican las matrices MDS cuadradas que son diferentes al menos en las rondas consecutivas numeradas con impares y en las rondas consecutivas numeradas con pares, y dichas matrices MDS cuadradas se configuran para exhibir independencia lineal o constituir matrices MDS cuadradas. Por lo tanto, es posible garantizar que no ocurra la cancelación simultánea de diferencias por contribución de cajas-S activas y, en consecuencia, ampliar un número mínimo de las cajas-S activas en toda una función criptográfica que es uno de los índices de la resistencia a ataques de criptoanálisis diferencial en un cifrado por bloque de clave común. La presente configuración mejora la resistencia tanto a ataques de criptoanálisis lineal como a ataques de criptoanálisis diferencial, y se lleva a cabo un procesamiento criptográfico de mayor seguridad.

Breve descripción de los dibujos

La Figura 1 es un diagrama que muestra una configuración de un cifrado por bloque de clave común típico que tiene una estructura Feistel.

Las Figuras 2A y 2B son diagramas que explican una estructura de una función F configurada 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 se aplicará al procesamiento de conversión lineal.

La Figura 4 es un diagrama que explica la cancelación simultánea de diferencias de tres etapas en un cifrado por bloque de 128 bits de m = 8 y n = 8.

La Figura 5 es un diagrama que explica un ejemplo concreto de generación de una diferencia de salida de función F ΔY_i llevando a cabo la conversión lineal con una matriz MDS cuadrada.

La Figura 6 es un diagrama que explica la cancelación simultánea de diferencias de cinco etapas en un cifrado por bloque de 128 bits de m = 8 y n = 8.

La Figura 7 es un diagrama que explica una definición de la cancelación simultánea de diferencias de etapa arbitraria en el procesamiento criptográfico por 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 configuración de matrices MDS cuadradas como matrices de conversión lineal de las funciones F de las respectivas rondas en un algoritmo criptográfico por bloque de clave común según la presente invención.

La Figura 10 es un diagrama de flujo que explica una secuencia de procesamiento de configuración de matrices MDS cuadradas como las matrices de conversión lineal de las funciones F de las respectivas rondas en el algoritmo criptográfico por bloque de clave común según la presente invención.

La Figura 11 es un diagrama de flujo que explica un ejemplo de procesamiento a1 de generación de matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis diferencial como una técnica de generación de matrices MDS cuadradas que son las matrices de conversión lineal que se establecerán en las funciones F de las respectivas rondas.

La Figura 12 es un diagrama de flujo que explica un ejemplo de procesamiento a2 de generación de matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis diferencial como una técnica de

generación de matrices MDS cuadradas que son las matrices de conversión lineal que se establecerán en las funciones F de las respectivas rondas.

La Figura 13 es un diagrama de flujo que explica un ejemplo de procesamiento a3 de generación de matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis diferencial como una técnica de generación de matrices MDS cuadradas que son las matrices de conversión lineal que se establecerán en las funciones F de las respectivas rondas.

La Figura 14 es un diagrama que explica una técnica concreta del ejemplo de procesamiento a3 de generación de matrices MDS cuadradas que son las matrices de conversión lineal que se establecerán en las funciones F de las respectivas rondas.

La Figura 15 es un diagrama de flujo que explica un ejemplo de procesamiento b1 de generación de matrices MDS cuadradas que llevan a cabo 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 se establecerán en las funciones F de las respectivas rondas.

La Figura 16 es un diagrama de flujo que explica un ejemplo de procesamiento de generación de matrices MDS cuadradas que llevan a cabo 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 se establecerán en las funciones F de las respectivas rondas.

La Figura 17 es un diagrama de flujo que explica un ejemplo de procesamiento de generación de matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis diferencial y ataques de criptoanálisis lineal como una técnica de generación de matrices MDS cuadradas que son las matrices de conversión lineal que se establecerán en las funciones F de las respectivas rondas.

La Figura 18 es un diagrama que muestra un ejemplo de una configuración de un módulo CI como un aparato de procesamiento criptográfico para llevar a cabo el procesamiento criptográfico según la presente invención.

Mejor modo de llevar a cabo la invención

De aquí en adelante, se explicarán detalles de un aparato de procesamiento criptográfico de la presente invención, un método de procesamiento criptográfico y un programa de ordenador para ello. La explicación se proveerá en el siguiente orden de artículos.

1. Procesamiento de análisis diferencial en un algoritmo criptográfico por bloque de clave común

2. Procesamiento de análisis lineal en el algoritmo criptográfico por bloque de clave común

3. Algoritmo criptográfico según la presente invención

(3-a) Ejemplo de generación de matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis diferencial y su establecimiento en las funciones F

(3-b) Ejemplo de generación de matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis lineal y su establecimiento en las funciones F

(3-c) Ejemplo de generación de matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis diferencial y a ataques de criptoanálisis lineal y su establecimiento en las funciones F.

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

Primero, se explicará un resumen del procesamiento de análisis diferencial en el algoritmo criptográfico por bloque de clave común tipificado por el procesamiento criptográfico DES (estándar de cifrado de datos) mediante el uso de un modelo generalizado de procesamiento criptográfico por bloque de clave común.

El algoritmo del procesamiento criptográfico por bloque de clave común puede dividirse principalmente en una sección de función de ronda para llevar a cabo la conversión de datos de entrada y una sección de planificación de clave para generar una clave que se aplicará en cada ronda de la parte de función de ronda. Una clave (subclave) aplicada en cada ronda de la función de ronda se genera por la sección de planificación de clave en la cual se ingresa una clave maestra (clave principal) y, según esta, se aplica en cada ronda. Entre los sistemas típicos del presente sistema criptográfico de clave común, existe un DES (estándar de cifrado de datos) como un sistema estándar federal de los Estados Unidos.

Una estructura del procesamiento criptográfico por bloque de clave común típico llamada estructura Feistel se explicará con referencia a la Figura 1.

La estructura Feistel tiene una configuración de conversión de un texto en lenguaje claro en un texto cifrado mediante la simple repetición de una función de conversión. La longitud de un texto en lenguaje claro se establece en 2 mn (2×m×n) bits. Aquí, m y n son, ambos, enteros. Primero, un texto en lenguaje claro de 2 mn bits se divide en dos datos de entrada, un P_L (Texto en lenguaje claro-Izquierda) 101 de mn bits y un P_R (Texto en lenguaje claro-Derecha) 102 de mn bits, y estos se usan como valores de entrada.

La estructura Feistel se expresa por la repetición de una estructura básica llamada función de ronda, y una función de conversión de datos que se incluye en cada ronda se llama una función F 120. La Figura 1 muestra una configuración a modo de ejemplo compuesta de las funciones F (funciones de ronda) 120 repetidas para r etapas.

Por ejemplo, en la primera ronda, los datos de entrada X de mn bits y una clave de ronda K_1 103 de mn bits ingresada desde una unidad de generación de clave (no se muestra en la figura) se ingresan en la función F 120, la cual produce datos Y de mn bits después del procesamiento de conversión de datos allí. Una sección OR exclusiva 104 ejecuta una operación OR exclusiva en la salida y los otros datos de entrada de la etapa precedente, y produce un resultado de operación de mn bits a la siguiente función de ronda. El procesamiento criptográfico se completa aplicando dicho procesamiento, a saber, la función F de manera repetida para un número predeterminado de rondas (r), y produce datos divididos CL (Cifrado-Izquierda) y datos CR (Cifrado-Derecha) de un texto cifrado. La configuración de más arriba lleva al hecho de que, con el fin de llevar a cabo el descifrado con la estructura Feistel, solo es necesario invertir una secuencia de inserción de claves de ronda, no es necesario configurar una función inversa.

La estructura de la función F 120 que se configura como una función de cada ronda se explicará 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 así llamada estructura del tipo SPN que consiste en una capa de conversión no lineal y en una capa de conversión lineal conectadas juntas, como se muestra en la Figura 2B.

La función F 120 del tipo SPN tiene múltiples cajas-S 121 para llevar a cabo el procesamiento de conversión no lineal, como se muestra en la Figura 2B. La operación OR exclusiva se ejecuta en un valor de entrada X de mn bits de una etapa precedente de la sección de función de ronda junto con una clave de ronda K_i ingresada desde la sección de planificación de clave, y su salida se ingresa en múltiples (m) cajas-S, cada una de las cuales ejecuta el procesamiento de conversión no lineal en n bits. Cada una de las cajas-S lleva a cabo el procesamiento de conversión no lineal que aplica, por ejemplo, una tabla de conversión.

Un valor de salida Z de mn bits que son datos de salida de la caja-S 121 se ingresa en una sección de conversión lineal 122 para llevar a cabo el procesamiento de conversión lineal, que ejecuta el procesamiento de conversión lineal, por ejemplo, el procesamiento de intercambio de posiciones de bits, etc., y produce un valor de salida Y de mn bits. El valor de salida Y junto con los datos de entrada de la etapa precedente se someten a la operación OR exclusiva, y su resultado se asigna a un valor de entrada de la función F de la siguiente ronda.

En la función F 120 que se muestra en la Figura 2, la longitud de bit de una entrada/salida es mxn (m, n: entero), la capa de conversión no lineal tiene una configuración en la cual m cajas-S 121, cada una de las cuales sirve como la capa de conversión no lineal cuya entrada y salida son n bits, se disponen en paralelo, y la sección de conversión lineal 122 como la capa de conversión lineal ejecuta el procesamiento de conversión lineal según una m-ésima matriz cuadrada que tiene elementos en un campo de extensión $GF(2^n)$ definido por un n-ésimo polinomio irreducible como sus elementos.

La Figura 3 muestra un ejemplo de una matriz cuadrada que se aplicará al procesamiento de conversión lineal en la sección de conversión lineal 122. Una matriz cuadrada 125 que se muestra en la Figura 3 es un ejemplo de n = 8 y m = 8. La conversión lineal se ejecuta en datos de mn bits Z[1], Z[2], ..., Z [m] producidos desde la sección de conversión no lineal (caja-S 121) que aplica la matriz cuadrada 125 predeterminada, e Y[1], Y[2], ..., Y[m] se determinan como salidas de la función F (función de ronda) producida. Es preciso observar que la operación lineal de elementos de una matriz de cada dato se ejecuta en el campo de extensión $GF(2^n)$ predeterminado de 2.

Dado que el cifrado tipo Feistel hasta ahora usado utiliza la misma capa de conversión lineal para las funciones F de todas las etapas, existe una propiedad de que múltiples diferencias se anulan simultáneamente cuando las diferencias se propagan. Según se explica en el párrafo de los antecedentes de la técnica, como una técnica de criptoanálisis típica, existe un análisis diferencial conocido (o técnica de descifrado de diferencias) en el cual una clave de aplicación para cada función de ronda se analiza mediante el análisis de muchos datos de entrada (texto en lenguaje claro) y sus datos de salida (texto cifrado). En el procesamiento criptográfico por bloque de clave común convencional como, por ejemplo, el algoritmo criptográfico DES, dado que el procesamiento (matriz de conversión) que se aplicará en la sección de conversión lineal 122 de las funciones F 120 se establece para ser equivalente en una ronda de cada etapa, es fácil llevar a cabo el análisis diferencial y, como resultado, el análisis de una clave es fácil.

Un ejemplo donde múltiples diferencias se anulan simultáneamente al momento de propagación de las diferencias se explicará con referencia a la Figura 4. En la presente descripción, cuando se expresa una diferencia, la diferencia se indica mediante adición de un símbolo Δ (delta).

La Figura 4 es un diagrama que explica la cancelación simultánea de diferencias de tres etapas en un cifrado por bloque de 128 bits de m = 8 y n = 8. Es preciso observar que, en la figura, datos de 64 bits se dividirán por byte, cada uno se expresará como un vector, y cada elemento se representará en hexadecimal.

La cancelación simultánea de diferencias en la función F que tiene una estructura de tres etapas ocurre, por ejemplo, según un mecanismo de configuración de los siguientes estados de datos 1-4. Los estados de datos generados por un mecanismo que se explicará más abajo son estados de datos que pueden generarse configurando muchos datos de entradas de diferencia, es decir, esto puede generarse al analizar una clave (clave de ronda) en el así llamado análisis diferencial.

(Estado 1)

Supongamos que la mitad izquierda de la diferencia de entrada con respecto a la ronda i consiste en diferencias de entrada de todos ceros (ΔX_{i-1}, = (00, 00, 00, 00, 00, 00, 00, 00)) y la mitad derecha de aquella consiste en diferencias de entrada de todos ceros excepto una entrada a una caja-S solamente (ΔX_{i-1}, = (34, 00, 00, 00, 00, 00, 00, 00)). El presente estado de datos indica que, mediante la configuración de muchos datos de entradas de diferencia, dicho estado de datos puede obtenerse 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 respectivas m cajas-S (m = 8) estructuradas en la función F. Una diferencia (34) se ingresa en la primera caja-S ((S1) en la Figura 4), y (00)'s son diferencias de entrada con respecto a la segunda a octava cajas.

Aquí, una diferencia de salida de una caja-S que tiene una diferencia de entrada de cero (00) es cero (00). Con respecto a los datos de diferencia, la caja-S que tiene una diferencia de entrada de cero (00) no provoca efecto alguno, por consiguiente, se llama una caja-S que no es activa, a saber, una caja-S inactiva. Por otro lado, una caja-S que tiene una diferencia de entrada diferente de cero (en el ejemplo de la Figura 4, diferencia = 34) genera un resultado de conversión no lineal correspondiente a la diferencia de entrada diferente de cero, por consiguiente, llamada una caja-S activa.

En el ejemplo de la Figura 4, se genera la diferencia de salida (b7) de una caja-S activa (S1) en la cual se ingresa la diferencia de entrada (34) diferente de cero. Las otras cajas-S inactivas S2-S8 generan diferencias de salida (00) según las diferencias de entrada (00) de ceros, respectivamente, y provistas como entradas de diferencia de la sección de conversión lineal.

(Estado 2)

Una diferencia de salida de una caja-S que tiene una diferencia de entrada diferente de cero con respecto a la ronda i (de aquí en adelante, llamada caja-S activa) se dispersa en la capa de conversión lineal, y se produce a partir de la función F (valor de salida = ΔY_i) y, de esta manera, se convierte en una diferencia de entrada ΔX_{i+1} con respecto a la siguiente ronda, tal como está.

La conversión lineal en el ejemplo de la Figura 4 es tal que la conversión lineal con cierta matriz cuadrada 125 específica, por ejemplo, como se muestra en la Figura 5, común en las funciones F de las respectivas rondas se ejecuta para producir una diferencia ΔY_i = (98, c4, b4, d3, ac, 72, 0f, 32) como una diferencia de salida de una función F de la ronda i. Como puede comprenderse a partir de la estructura de conversión lineal que se muestra en la Figura 5, la diferencia de salida ΔY_i = (98, c4, b4, d3, ac, 72, 0f, 32) se determina como un valor solo dependiente de un elemento de salida Z[1] = b7 de una caja-S activa (S1).

Dicho ΔY_i = (98, c4, b4, d3, ac, 72, 0f, 32) como diferencias de salida de la función F de la presente ronda i junto con diferencias de entrada de todos ceros (ΔX_{i-1}, = (00, 00, 00, 00, 00, 00, 00, 00)) se someten a la operación OR exclusiva (XOR) en una sección OR exclusiva 131 que se muestra en la Figura 4, y un resultado de operación se provee como ΔX_{i+1} a la siguiente ronda i+1.

Dado que los resultados de las operaciones OR exclusivas (XOR) en ΔY_i = (98, c4, b4, d3, ac, 72, 0f, 32), como diferencias de salida de la función F de la ronda i, y diferencias de entrada de todos los ceros ΔX_{i-1} = (00, 00, 00, 00, 00, 00, 00, 00) son ΔY_i, las diferencias de entrada ΔX_{i+1} a la siguiente ronda i+1 son iguales 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 la ronda i+1 tiene un valor diferente de cero solo en una posición de la caja-S activa en la ronda i. Dicho estado de datos indica que, mediante la configuración de muchos datos de entradas de diferencia, puede obtenerse dicho estado de datos.

Es decir, ΔY_{i+1} = (ad, 00, 00, 00, 00, 00, 00, 00), y la diferencia de salida ΔY_{i+1} tiene un valor diferente de cero solo en una posición de la caja-S (primera caja-S (S1)) que tiene un valor de diferencia diferente de cero, de manera similar a la ronda i. De manera incidental, es evidente que ad ≠ 00.

(Estado 4)

En el caso donde 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 muestra en la Figura 4, una diferencia de salida de la caja-S activa (S1) en la ronda i+2 se convierte en b7 y concuerda con la diferencia de salida (b7) de la caja-S activa (S1). El presente estado de datos indica que, mediante la configuración de muchos datos de entradas de diferencia, puede obtenerse dicho estado de datos.

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

Como resultado, una sección OR exclusiva 133 ejecutará la operación OR exclusiva en $\Delta X_{i+1} = \Delta Y_i$ = (98, c4, b4, d3, ac, 72, 0f, 32) y ΔY_{i+2} = (98, c4, b4, d3, ac, 72, 0f, 32), los cuales son, ambos, el mismo valor, y producirá valores de todos ceros como resultado de la operación OR exclusiva.

Como resultado, la diferencia de entrada izquierda ΔX_{i+3} de la etapa precedente (ronda i+2) que produce la diferencia de salida a la siguiente etapa (ronda i+3) se convierte en 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 la presente ronda i+3 consiste en todos ceros como con la diferencia de entrada izquierda ΔX_{i-1} = (00, 00, 00, 00, 00, 00, 00, 00) con respecto a la ronda i, y existe la posibilidad de que el mismo procesamiento que el de las rondas i a i+2 se repita también en la ronda i+3 y rondas posteriores.

Como resultado, existe el problema de que el número de cajas-S activas no aumentará en comparación con un aumento de número de rondas, y la robustez frente a ataques de criptoanálisis diferencial tampoco mejorará tanto.

En el cifrado por bloque de clave común, un número mínimo de cajas-S activas en toda la función criptográfica se conoce como uno de los índices de robustez al ataque de criptoanálisis diferencial. Cuanto mayor es el número mínimo de cajas-S activas, se determina que más alta es la resistencia a ataques de criptoanálisis diferencial.

Según se describe más arriba, el análisis diferencial (ataque de criptoanálisis diferencial) es una técnica de análisis de una clave de aplicación en cada función de ronda mediante la configuración de muchos datos de entradas (textos en lenguaje claro) con cierta diferencia y sus datos de salidas (textos cifrados) y de análisis de la presente correspondencia. Si el número de cajas-S activas puede reducirse en el presente análisis diferencial, el análisis se convertirá en fácil y el número de procesos de análisis podrá reducirse.

Aunque en el ejemplo que se refiere a la Figura 4 descrita más arriba, un estado de ocurrencia de un patrón donde solo una primera caja-S (S1) es una caja-S activa, para otras cajas-S (S2-S8), es posible una configuración en la cual cada caja-S se configura para ser una caja activa mediante la configuración de datos de entrada del análisis diferencial. Por lo tanto, al llevar a cabo un proceso de análisis diferencial como este, es posible analizar el procesamiento de conversión no lineal de cada caja-S, y además analizar una clave de ronda ingresada para la función F.

Con el fin de aumentar la resistencia al análisis diferencial como este, es necesario mantener un estado donde el número de cajas-S activas sea siempre grande, es decir, que el número mínimo de cajas-S activas sea grande.

En el ejemplo explicado con referencia a la Figura 4, en el caso de la función F a la cual se provee una entrada en una dirección de derecha a izquierda, es decir, cuando se considera solo la ronda i y la ronda i+2 como rondas de objeto de un procesamiento de cálculo de caja-S activa, el número de cajas-S activas es solo dos, en las funciones F a las cuales se proveen entradas 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 se convierte en cero por la cancelación simultánea de diferencias y, en consecuencia, el procesamiento de análisis del procesamiento de conversión no lineal de cada caja-S por el análisis diferencial se convierte en fácil.

El algoritmo criptográfico por bloque de clave común que se muestra en la Figura 4 es que las matrices de conversión lineal aplicadas en las secciones de conversión lineal en las respectivas rondas son iguales, y dicha configuración particular lleva a la posibilidad de que la cancelación simultánea de diferencias se provoque por solo dos cajas-S activas, especialmente en las funciones F a las cuales se provee una entrada en una dirección de derecha a izquierda. Por lo tanto, existe el problema de que el número mínimo de cajas-S activas no aumenta totalmente en comparación con el crecimiento del número de rondas, y la robustez frente a ataques de criptoanálisis diferencial no aumenta tanto.

A continuación, de manera similar, en la configuración en la cual se usa la misma matriz de conversión lineal para las funciones F de todas las etapas (rondas), un mecanismo de ocurrencia de la cancelación simultánea de diferencias en cinco rondas se explicará con referencia a la Figura 6.

La Figura 6 es un diagrama que explica la cancelación simultánea de diferencias de cinco etapas en un cifrado por bloque de 128 bits de m = 8 y n = 8. Es preciso observar que, en la figura, datos de 64 bits se representarán como vectores mediante su división para un byte, y cada elemento se representará en hexadecimal.

La cancelación simultánea de diferencias en la función F con una configuración de cinco etapas ocurre, por ejemplo, según el siguiente mecanismo de configuración de los estados de datos 1-7. El estado de datos generado por un mecanismo explicado más abajo es un estado de datos que puede generarse configurando muchos datos de entradas de diferencia, y el estado de datos puede generarse al analizar una clave (clave de ronda) en el así llamado análisis diferencial.

(Estado 1)

Supongamos que la mitad izquierda de las diferencias de entrada con respecto a la ronda i consiste en diferencias de entrada de todos ceros (ΔX_{i-1} = (00, 00, 00, 00, 00, 00, 00, 00)) y la mitad derecha de las diferencias de entrada consiste en diferencias de entrada de todos ceros excepto una entrada a una caja-S solamente (ΔX_i = (34, 00, 00, 00, 00, 00, 00, 00)). El presente estado de datos indica que, mediante la configuración de muchos datos de entradas de diferencia, dicho estado de datos puede obtenerse en la ronda i.

Ocho elementos de ΔX_i = (34, 00, 00, 00, 00, 00, 00, 00) corresponden a respectivas diferencias de entrada a m (m = 8) cajas-S configuradas en las funciones F. (34) se ingresa en una primera caja-S ((S1) en la Figura 6), y (00)'s son diferencias de entrada con respecto a la segunda a octava cajas.

Según se describe más arriba, cualquier diferencia de salida de caja-S que tiene una diferencia de entrada de cero (00) es cero (00). Con respecto a la diferencia de salida, la caja-S que tiene una diferencia de entrada de cero no ejecuta la operación, por consiguiente, se llama una caja-S que no es activa, a saber, una caja-S inactiva. Por otro lado, dado que solo una caja-S (S1) con una diferencia de entrada diferente de cero (en el ejemplo de la Figura 6, diferencia = 34) genera un resultado de conversión no lineal correspondiente a la diferencia de entrada diferente de cero como una diferencia de salida, por consiguiente, llamada una caja-S activa.

En el ejemplo de la Figura 6, una caja-S activa (S1) a la cual una diferencia de entrada (34) diferente de cero se ingresa genera una diferencia de salida (b7), y otras cajas-S inactivas S2-S8 generan diferencias de salida (00) según las diferencias de entrada (00) de ceros, que se asignan como entradas de diferencia de la sección de conversión lineal.

(Estado 2)

Una diferencia de salida de una caja-S (de aquí en adelante, llamada una caja-S activa) que tiene una diferencia de entrada diferente de cero con respecto a la ronda i (en el ejemplo de la Figura 4, diferencia = 34) se dispersa en la capa de conversión lineal, y se produce a partir de la función F (valor de salida = ΔY_i) y, de esta manera, se convierte en una diferencia de entrada ΔX_{i+1} a la siguiente ronda, tal como está.

En el ejemplo de la Figura 6, la conversión lineal se ejecuta con cierta matriz cuadrada 125 específica que es común a cada ronda, por ejemplo, aquello que se muestra en la Figura 5, y ΔY_i = (98, c4, b4, d3, ac, 72, 0f, 32) se produce como una diferencia de salida de función F de la ronda i.

ΔY_i = (98, c4, b4, d3, ac, 72, 0f, 32), como diferencias de salida de la función F de la ronda i, se somete a las operaciones OR exclusivas (XOR) en la sección OR exclusiva 141 que se muestra en la Figura 6 junto con diferencias de entrada de todos ceros (ΔX_{i-1} = (00, 00, 00, 00, 00, 00, 00, 00)), y los resultados de la operación se convierten en diferencias de entrada a la siguiente ronda i+1.

Dado que los resultados de las operaciones OR exclusivas (XOR) en ΔY_i = (98, c4, b4, d3, ac, 72, 0f, 32), como diferencias de salida de la función F de la ronda i, y diferencias de entrada de todos los ceros (ΔX_{i-1}, = (00, 00, 00, 00, 00, 00, 00, 00)) son ΔY_i, las diferencias de entrada a la siguiente ronda i+1 se convierten en $\Delta X_{i+1} = \Delta Y_i$ = (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 diferente de cero solo en una posición de la caja-S activa en la ronda i. Dicho estado de datos indica que, mediante la configuración de muchos datos de entradas de diferencia, puede obtenerse un estado de datos.

Es decir, ΔY_{i+1} es ΔY_{i+1} = (34, 00, 00, 00, 00, 00, 00, 00), y tiene un valor diferente de cero solo en una posición de la caja-S (una primera caja-S (S1)) que tiene un valor de diferencia diferente 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 la ronda i+2 es un resultado de la operación OR exclusiva en la sección OR 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 se convierte en una entrada que consiste en todos ceros, ΔX_{i+2} = (00, 00, 00, 00, 00, 00, 00, 00). Como resultado, una diferencia de salida de la función F de la ronda i+2 también se convierte en una diferencia de salida que consiste en todos ceros, ΔY_{i+2} = (00, 00, 00, 00, 00, 00, 00, 00).

(Estado 5)

Entradas a una función F de la ronda i+3 son resultados de las operaciones OR exclusivas en la sección OR 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 la ronda i+2 de todos ceros, y se convierten en entradas $\Delta X_{i+3} = \Delta X_{i+1}$ = (98, c4, b4, d3, ac, 72, 0f, 32) a la función F de la ronda i+3.

(Estado 6)

Las diferencias de salida de la función F de la ronda i+3 se convierten en ΔY_{i+3} = (43, 00, 00, 00, 00, 00, 00, 00). Las operaciones OR exclusivas en la sección OR exclusiva 144 en dichas diferencias junto con ΔX_{i+2} = (00, 00, 00, 00, 00, 00, 00, 00) que consisten en todos ceros resultan en $\Delta X_{i+4} = \Delta Y_{i+3}$ = (43, 00, 00, 00, 00, 00, 00, 00), que se convierten en diferencias de entrada de la función F de la ronda i+4.

(Estado 7)

Cuando una diferencia de salida de una caja-S activa (S1) en la ronda i+4 concuerda 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 se convierte en b7, como se muestra en la Figura 6, y concuerda con una diferencia de salida (b7) de la caja-S activa (S1) en la ronda i. Dicho estado de datos indica que, al configurar muchos datos de entradas de diferencia, puede obtenerse dicho estado de datos.

Cuando ocurre el presente estado de datos, la diferencia de salida ΔY_{i+4} = (98, c4, b4, d3, ac, 72, 0f, 32) de una función F de la ronda i+4 coincidirá con la diferencia de salida ΔX_{i+3} = (98, c4, b4, d3, ac, 72, 0f, 32) de la sección OR exclusiva 143 de la ronda i+2 que es una ronda previa, pero una.

Como resultado, en la sección OR 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, se someterán a la operación OR exclusiva, y producirán valores de todos ceros como resultado de la operación OR exclusiva.

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

La presente entrada izquierda a la presente ronda i+5, ΔX_{i+5} = (00, 00, 00, 00, 00, 00, 00, 00) consiste en todos 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 el mismo procesamiento que el de la ronda i a la ronda i+4 se repita también en la ronda i+5 y rondas posteriores.

Por lo tanto, existe el problema de que el número de cajas-S activas no aumenta en comparación con el aumento de número de rondas, y la robustez frente a ataques de criptoanálisis diferencial no aumenta tanto.

Según se describe más arriba, el análisis diferencial (ataque de criptoanálisis diferencial) es una técnica de análisis de una clave de aplicación en cada función de ronda mediante la configuración de muchos datos de entradas (textos en lenguaje claro) con cierta diferencia y sus datos de salida (texto cifrado) y de análisis de la presente correspondencia. En el presente análisis diferencial, si el número de cajas-S activas puede reducirse, el análisis se convertirá en fácil y el número de procesos de análisis podrá reducirse.

En el ejemplo con referencia a la Figura 6 descrito más arriba, en el caso de las funciones F a las cuales se proveen entradas en una dirección de derecha a izquierda, es decir, en el caso donde la ronda i, ronda i+2, y ronda i+4 se consideran rondas objetivo del cálculo de caja-S activa, el número de cajas-S activas es solo 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 cuales se proveen entradas en una dirección de izquierda a derecha, es decir, en el caso donde ronda i+1 y ronda i+3 se consideran rondas objetivo, aunque el número de cajas-S activas es ocho, el número de cajas-S activas en ronda i+5 se convierte en cero debido a la cancelación simultánea de diferencias; por lo tanto, el análisis del procesamiento de conversión no lineal de cada caja-S por el análisis diferencial y procesamiento de criptoanálisis de una clave de ronda de entrada para la función F se convierte, en comparación, en fácil.

Aunque el ejemplo con referencia a la Figura 6 presenta un estado de ocurrencia de un patrón donde solo la primera caja-S (S1) es una caja-S activa, con respecto a otras cajas-S (S2 a S8), el establecimiento de los datos de entrada del análisis diferencial permite que cualquiera de las otras cajas-S se establezca como una caja-S activa, por lo tanto, la ejecución de dicho proceso de análisis diferencial posibilitará el análisis del procesamiento de conversión no lineal de cada caja-S y además el análisis de la clave de ronda ingresada en la función F.

Aunque el ejemplo de ocurrencia de la cancelación simultánea de diferencias en los casos de tres y cinco rondas se ha explicado con referencia a la Figura 4 y a la Figura 6, si dichos casos se generalizan para el número arbitrario de rondas para definir la cancelación simultánea de diferencias, la definición puede proveerse de la siguiente manera. Con referencia a la Figura 7, se explicará la definición de la cancelación simultánea de diferencias en un número arbitrario de rondas. La Figura 7 muestra rondas en serie excepto una (i, i+2, i+4, ..., i+2j) de la estructura Feistel que lleva a cabo el procesamiento criptográfico por bloque de clave común de la estructura Feistel.

"Definición"

En un proceso donde una mitad de las diferencias de entrada de la estructura Feistel en la ronda i consiste en ceros (en la Figura 7, ΔX_i = (00, 00, 00, 00, 00, 00, 00, 00)) y cada una de ellas y cada una de las diferencias de salida de la función F de la ronda i+2j se someten a la operación OR exclusiva en la sección OR exclusiva, un caso donde los resultados de la operación OR exclusiva se convierten en ceros (en la Figura 7, ΔX_{i+2j+1} = (00, 00, 00, 00, 00, 00, 00, 00)) se llama cancelación simultánea de diferencias.

En este momento, las cajas-S activas existentes en las funciones F de las rondas i, i+2, i+4, ..., i+2k se llaman cajas-S activas que provocan la cancelación simultánea de diferencias. Al definir el número de elementos diferentes de cero de un vector A como peso de Hamming hw (A), el número "a" de cajas-S activas que provocan la cancelación simultánea de diferencias puede expresarse 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 más arriba, el número de cajas-S activas que provocan la cancelación simultánea de diferencias es, ambos, dos, es decir, a = 2.

Según se describe más arriba, uno de los índices de robustez a ataques de criptoanálisis diferencial en el cifrado por bloque de clave común es el número mínimo de cajas-S activas en todas las funciones criptográficas, y se determina que cuanto mayor es el número mínimo de cajas-S activas, más alta es la resistencia a ataques de criptoanálisis diferencial.

Sin embargo, en la configuración donde se usa la misma matriz de conversión lineal para las funciones F de todas las etapas como en el algoritmo DES, existe la posibilidad de que solo dos cajas-S activas provoquen la cancelación simultánea de diferencias, como puede comprenderse a partir de la explicación con referencia a la Figura 4 y a la Figura 6. Existe el problema de que, debido a la presencia de dicha propiedad, el número mínimo de cajas-S activas no aumenta de manera suficiente y la robustez a ataques de criptoanálisis diferencial no se fortalece tanto.

[2. Procesamiento de análisis lineal en algoritmo criptográfico por bloque de clave común]

El procesamiento de análisis diferencial, según se describe más arriba, requiere que un ejecutor del análisis prepare datos de entrada (texto en lenguaje claro) que tengan una diferencia constante y analice sus datos de salida correspondientes (texto cifrado). Para el procesamiento de análisis lineal, no es necesario preparar datos de entrada (texto en lenguaje claro) que tengan una diferencia constante y el análisis se ejecuta según datos de entrada (texto en lenguaje claro) cuya cantidad es igual a o mayor que una cantidad predeterminada y sus correspondientes datos de salida (texto cifrado).

Según se describe más arriba, en el algoritmo criptográfico por bloque de clave común, las cajas-S como la sección de conversión no lineal se preparan y no hay relación lineal entre los datos de entrada (texto en lenguaje claro) y sus correspondientes datos de salida (texto cifrado). En el análisis lineal, el análisis se lleva a cabo mediante aproximación lineal de la entrada/salida de dicha caja-S, análisis de una relación lineal entre muchos datos de entradas (lenguaje en texto claro) y valores de bits constituyentes de los correspondientes datos de salida (texto cifrado) y reducción de claves que son candidatas asumidas. En el análisis lineal, no es necesario preparar datos de entrada con una diferencia específica, y el análisis se convierte en posible solo mediante preparación de un gran número de textos en lenguaje claro y sus correspondientes textos cifrados.

[3. Algoritmo criptográfico basado en la presente invención]

De aquí en adelante, se explicará un algoritmo criptográfico de la presente invención. El algoritmo criptográfico de la presente invención tiene una estructura que mejora la resistencia a ataques de criptoanálisis lineal, ataques de criptoanálisis diferencial descritos más arriba, y similares, es decir, con una estructura que mejora la dificultad en el análisis de clave y mejora la seguridad.

Una de las características del algoritmo criptográfico con respecto a la presente invención es que el algoritmo se construye configurando múltiples matrices MDS (distancia máxima separable) cuadradas diferentes antes que una estructura en la cual el procesamiento común (matriz de conversión) se aplica a la sección de conversión lineal de una función F de cada ronda como con el algoritmo DES convencional. De manera específica, el algoritmo se configura para llevar a cabo el procesamiento de conversión lineal mediante aplicación de matrices MDS cuadradas que son diferentes al menos en las rondas consecutivas numeradas con pares y en las rondas consecutivas numeradas con impares.

El algoritmo criptográfico con respecto a la presente invención implementa una estructura con la cual la cancelación simultánea de diferencias basada en un pequeño número de cajas-S activas no ocurre o es menos propenso a ocurrir mediante el uso de propiedades de las matrices MDS (distancia máxima separable) cuadradas, de modo que el número mínimo de cajas-S activas se amplía y el procesamiento criptográfico por bloque de clave común más robusto al ataque de criptoanálisis diferencial se lleva a cabo. De manera alternativa, la presente invención implementa una estructura con la cual la dificultad del análisis lineal que se ejecuta como un ataque de criptoanálisis de texto en lenguaje claro conocido.

El algoritmo criptográfico de la presente invención aplica una estructura criptográfica por bloque de clave común típica que se llama una estructura Feistel que tiene las funciones F del tipo SPN explicadas con referencia a las Figuras 1 y 2, es decir, aplica una estructura que convierte un texto en lenguaje claro en un texto cifrado o convierte un texto cifrado en un texto en lenguaje claro mediante simple repetición de la función F del tipo SPN que tiene la sección de conversión no lineal y la sección de conversión lineal en múltiples rondas.

Por ejemplo, la longitud de un texto en lenguaje claro se asume como 2 mn bits (aquí, m y n siendo, ambos, enteros). La estructura divide un texto en lenguaje claro de 2 mn bits en dos datos PL (Texto en lenguaje claro-Izquierda y Texto en lenguaje claro-Derecha), cada uno de mn bits, y ejecuta la función F en cada ronda mediante el uso de aquellos como valores de entrada. La función F es una función F con un tipo SPN que consiste en la sección de conversión no lineal compuesta de cajas-S y la sección de conversión lineal conectadas juntas.

En la configuración de la presente invención, como una matriz para el procesamiento de conversión lineal que se aplicará en la sección de conversión lineal en la función F, matrices seleccionadas de múltiples matrices MDS (distancia máxima separable) cuadradas diferentes se configuran como matrices que se aplicarán en las secciones de conversión lineal de las funciones F de las respectivas rondas. De manera específica, se aplican matrices MDS cuadradas que son diferentes al menos en las rondas consecutivas numeradas con pares y en las rondas consecutivas numeradas con impares.

Se explicará la matriz MDS cuadrada. La matriz cuadrada es una matriz que satisface las propiedades de (a) y (b) más abajo. (a) La matriz es una matriz cuadrada. (b) Determinantes de todas las submatrices incluidas en una matriz son diferentes de cero, a saber, det(submatriz) ≠ 0.

La matriz que satisface las condiciones de (a) y (b) de más arriba se llama la matriz MDS cuadrada. Las longitudes de bits de entrada/salida a la función F que se ejecuta en cada ronda del procesamiento criptográfico por bloque de clave común es mxn bit (m, n: entero). La Figura 8 muestra un ejemplo de la matriz MDS cuadrada en el caso donde la sección de conversión no lineal configurada en la función F se construye con m cajas-S, cada una de las cuales tiene entrada/salida de n bits, y la sección de conversión lineal ejecuta el procesamiento de conversión lineal según m-ésimas matrices cuadradas, cada una de las cuales tiene elementos en el campo de extensión GF(2^n) de 2 definido por un n-ésimo polinomio irreducible como sus elementos. Un ejemplo de la matriz MDS cuadrada que se muestra en la Figura 8 es un ejemplo de la matriz MDS cuadrada de n = 8 y m = 8.

Mediante la designación del número de elementos diferentes de cero en el vector A por el peso de Hamming hw(A), una m-ésima matriz MDS cuadrada por M, y un vector de entrada a la matriz MDS cuadrada M por x, una matriz MDS cuadrada que satisface (a) y (b) de más arriba satisface la siguiente desigualdad (Ecuación 1).

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

La expresión descrita más arriba (Ecuación 1) indica que el total del número de elementos diferentes de cero hw(x) de los datos de entrada x que se convertirán linealmente con la matriz MDS cuadrada (M) más el número de elementos diferentes de cero hw(M_x) de los datos de salida M_x que se ha convertido linealmente con la matriz MDS cuadrada (M) es mayor que el número de orden m de la matriz MDS cuadrada.

De manera incidental, el nombre de la matriz MDS cuadrada se provee porque una mitad derecha de una forma estándar de una matriz de generación del código de MDS (código de distancia máxima separable) cuadrada satisface las condiciones descritas más arriba.

Se conoce que, incluso en la configuración convencional en la cual una sola matriz se incorpora en todas las funciones F, el uso de una matriz MDS cuadrada como una matriz de conversión lineal permite que el número

mínimo de cajas-S activas se mantenga en un nivel comparativamente alto en comparación con un caso donde se usa una matriz diferente de la matriz MDS cuadrada.

La presente invención propone un método de uso de una matriz que satisface las condiciones de la matriz MDS cuadrada para la función F de cada ronda y además configurar diferentes matrices para respectivas rondas. De manera específica, se aplican matrices MDS cuadradas que son diferentes al menos en las rondas consecutivas numeradas con pares y en las rondas consecutivas numeradas con impares.

Múltiples ejemplos de configuraciones en cada una de las cuales la resistencia a ataques de criptoanálisis diferencial es más alta en el cifrado por bloque de clave común del tipo Feistel del número de etapa 2r (r siendo un entero) se explicarán más abajo.

En la siguiente explicación, MLT_j denota la matriz de conversión lineal que se aplicará en la sección de conversión lineal de la función F de la j-ésima etapa en la estructura criptográfica por bloque de clave común tipo Feistel de número de etapa 2r (número de ronda).

En la configuración de la presente invención, como una matriz para el procesamiento de conversión lineal que se aplicará en la sección de conversión lineal de la función F de cada etapa en la estructura criptográfica por bloque de clave común tipo Feistel de número de etapa 2r (número de onda), matrices seleccionadas de múltiples matrices MDS (distancia máxima separable) cuadradas diferentes se configuran como matrices que se aplicarán en las secciones de conversión lineal de las funciones F de las respectivas rondas. De manera específica, se aplican matrices MDS cuadradas que son diferentes al menos en las rondas consecutivas numeradas con pares y en las rondas consecutivas numeradas con impares.

De manera específica, en cumplimiento con la estructura criptográfica por bloque de clave común tipo Feistel de número de etapa (número de ronda) 2r, se generan q matrices MDS cuadradas L_1, L_2, ..., L_q ($q \leq r$). Entonces, como matrices para el procesamiento de conversión lineal que se aplicará en las secciones de conversión lineal en las funciones F de etapas numeradas con impares en la estructura criptográfica por bloque de clave común tipo Feistel de número de etapa (número de ronda) 2r, q matrices MDS cuadradas se configuran de manera repetida mediante designación de L_1, L_2, ..., L_q, L_1, L_2, ... a partir de su etapa superior de las funciones F. Además, para las funciones F de etapas numeradas con pares, q matrices MDS cuadradas se configuran, de manera repetida, mediante designación de L_1, L_2, …, L_q, L_1, L_2, ... a partir de su etapa inferior de las funciones F.

La Figura 9 muestra un ejemplo de configuración al cual se aplica la presente configuración. Como un ejemplo de configuración en el cual tres tipos de matrices MDS cuadradas diferentes se disponen en la estructura criptográfica por bloque de clave común tipo Feistel de q = 3, a saber, número de ronda 12 en el caso donde una estructura se define como la estructura criptográfica por bloque de clave común tipo Feistel de número de etapa (ronda número) 2r = 12, a saber r = 6, las matrices MDS cuadradas (L_1, L_2, L_3) que se establecerán en las secciones de conversión lineal de las funciones F en las respectivas rondas se muestran en la Figura 9.

La configuración de la Figura 9 es una estructura divide un texto en lenguaje claro de 2 mn bits en dos datos PL (Texto en lenguaje claro-Izquierda) y PR (Texto en lenguaje claro-Derecha), cada uno de mn bits, y ejecuta una función F en cada ronda mediante el uso de aquellos 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 que consiste en 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, donde un símbolo L_n que se muestra en cada función F denota una matriz MDS cuadrada 402. Es decir, L_1, L_2, y L_3 denotan tres tipos de matrices MDS cuadradas mutuamente diferentes, cada una de las cuales es una matriz MDS cuadrada que se aplicará al procesamiento de conversión lineal en la sección de conversión lineal de cada función F.

Una secuencia de procesamiento de configuración de la matriz de conversión lineal MLT_j se explicará con referencia a la Figura 10.

Etapa E21

Se selecciona un número q igual a o menor que una mitad r del número de ronda 2r, a saber, q que satisface $q \leq r$. Aquí, q es un entero de dos o más.

Etapa E22

Se generan q m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q en $GF(2^n)$. Detalles de las q m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q en $GF(2^n)$ se explicarán en un párrafo posterior.

Después de que las q m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q en $GF(2^n)$ se generan en la etapa E22, se ejecuta el procesamiento de configuración de matriz MDS cuadrada de más abajo.

Etapa E23

La matriz de conversión lineal MLT_{2i-1} de número de etapa 2i-1 ($1 \leq i \leq r$) se establece en $L_{(i-1 \bmod q)+1}$.

Etapa E24

La matriz de conversión lineal MLT_{2j} de número de etapa 2i ($1 \leq i \leq r$) se establece en $MLT_{2r-2i+1}$.

Por ejemplo, en el caso de una configuración a modo de ejemplo que se muestra en la Figura 9, es decir, en el caso donde el aparato de procesamiento criptográfico tiene 12 etapas (r = 6) y q = 3, la configuración será: $MLT_1 = L_1$, $MLT_2 = L_3$, $MLT_3 = L_2$, $MLT_4 = L_2$, $MLT_5 = L_3$, $MLT_6 = L_1$, $MLT_7 = L_1$, $MLT_8 = L_3$, $MLT_9 = L_2$, $MLT_{10} = L_2$, $MLT_{11} = L_3$, $MLT_{12} = L_1$.

Por consiguiente, el aparato de procesamiento criptográfico de la presente invención utiliza la siguiente estructura. Según la estructura criptográfica por bloque de clave común tipo Feistel de número de etapa (número de ronda) 2r, se generan q matrices MDS cuadradas, en donde $q \leq r$. Para las funciones F de las etapas numeradas con impares, q matrices MDS cuadradas se configuran, de manera repetida, mediante designación de $L_1, L_2, \ldots, L_q, L_1, L_2, \ldots$ de forma secuencial a partir de la función F de la etapa superior, y para las funciones F de las etapas numeradas con pares, q matrices MDS cuadradas se configuran, de manera repetida, mediante designación de $L_1, L_2, \ldots, L_q, L_1, L_2, \ldots$ de forma secuencial a partir de la función F de la etapa inferior.

A continuación, se explicarán detalles de las q m-ésimas matrices MDS cuadradas $L_1, L_2, \ldots, L_q$ en $GF(2^n)$ en la etapa E22 en el flujo de procesamiento de la Figura 10 y su establecimiento en las funciones F. La explicación se proveerá a lo largo de los siguientes artículos.

(3-a) Ejemplo de generación de matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis diferencial y su configuración según las funciones F

(3-b) Ejemplo de generación de matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis lineal y su configuración según las funciones F

(3-c) Ejemplo de generación de matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis diferencial y a ataques de criptoanálisis lineal y su configuración según las funciones F.

(3-a) Ejemplo de generación de matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis diferencial y su configuración según las funciones F. Primero, como un ejemplo de generación de matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis diferencial y su configuración según las funciones F, se explicarán tres ejemplos de procesamiento a1, a2 y a3.

(Ejemplo de procesamiento a1)

Se explicará un primer ejemplo de generación de matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis diferencial y su configuración según las funciones F. Primero, la explicación se proveerá para el procesamiento de generación de una matriz MDS cuadrada con referencia a un diagrama de flujo que se muestra en la Figura 11.

Etapa E101

Designación de 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 m-ésimas matrices MDS cuadradas $L_1, L_2, \ldots, L_q$ se generan de forma aleatoria en $GF(2^n)$. El diagrama de flujo que se muestra en la Figura 11 muestra un ejemplo de procesamiento como con el número de matrices MDS q = 6, el orden de extensión n = 8, y el tamaño de matriz m = 8.

Etapa E102

Se verifica si qm vectores de columna arbitrarios tomados de qm vectores de columna incluidos en las q m-ésimas matrices MDS cuadradas $L_1, L_2, \ldots, L_q$ son linealmente independientes. Si el flujo ha pasado la verificación, el flujo procede a la etapa E103; si no, el flujo regresa a la etapa E101.

Etapa E103

Las q m-ésimas matrices MDS cuadradas $L_1, L_2, \ldots, L_q$ se producen como matrices MDS cuadradas que se aplicarán al cifrado por bloque de clave común tipo Feistel de número de ronda 2r.

A través del proceso de más arriba, se generan las q m-ésimas matrices MDS cuadradas $L_1, L_2, \ldots, L_q$. Aquí, q satisface $q \leq r$.

Las q m-ésimas matrices MDS cuadradas $L_1, L_2, \ldots, L_q$ generadas de esta manera se configuran como matrices que se aplicarán al procesamiento de conversión lineal en la sección de conversión lineal de la función F de cada etapa

en la estructura criptográfica por bloque de clave común tipo Feistel de número de etapa (número de ronda) 2r, según el procesamiento de [etapa E23] y [etapa E24] explicado previamente con referencia a la Figura 10. Es decir, para etapas numeradas con impares, q matrices MDS cuadradas se designan como L_1, L_2, ..., L_q, L_1, L_2, ... en secuencia y de forma repetida a partir de la función F de la etapa superior, y para etapas numeradas con pares, q matrices MDS cuadradas se designan como L_1, L_2, ..., L_q, L_1, L_2, ... en secuencia y de forma repetida a partir de la función F de la etapa inferior.

Por consiguiente, las matrices MDS cuadradas de las rondas numeradas con pares y las matrices MDS cuadradas de las rondas numeradas con impares se disponen en órdenes mutuamente inversos, respectivamente, por medio de lo cual se garantiza que el procesamiento de cifrado y el procesamiento de descifrado sean iguales excepto por el procesamiento de reemplazo de una secuencia de claves.

La presente 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 matrices de conversión lineal incluidos en al menos q funciones F consecutivas en rondas numeradas con impares en una función criptográfica son linealmente independientes. (c) m vectores de columna arbitrarios de matrices de conversión lineal incluidos en al menos q funciones F consecutivas en rondas numeradas con pares son linealmente independientes. Dado que los aspectos (a) a (c) se garantizan, se garantiza que, en la estructura criptográfica por bloque de clave común tipo Feistel que tiene múltiples rondas, no ocurra la cancelación simultánea de diferencias por contribución de m o menos cajas-S activas. Por lo tanto, el valor mínimo del número de cajas-S activas en toda la función criptográfica aumentará.

Por consiguiente, el presente ejemplo de procesamiento hace posible ampliar el número mínimo de cajas-S activas en toda la función criptográfica que es uno de los índices de robustez a los ataques de criptoanálisis diferencial en el cifrado por bloque de clave común. Como resultado, el número de cajas-S activas cuando el análisis diferencial (ataque de criptoanálisis diferencial) se intenta aumentará y se mejorará la dificultad en el análisis. Por lo tanto, se lleva a cabo un procesamiento criptográfico de alta seguridad cuya clave es difícil de analizar.

(Ejemplo de procesamiento a2)

Se explicará un segundo ejemplo de generación de matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis diferencial y su configuración según las funciones F. El procesamiento de generación de las matrices MDS cuadradas se explicará con referencia al diagrama de flujo de la Figura 12.

Etapa E201

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 m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q se generan de forma aleatoria en GF(2^n). El diagrama de flujo que se muestra en la Figura 12 muestra un ejemplo de procesamiento como con el número de matrices MDS q = 6, el orden de extensión n = 8, y el tamaño de matriz m = 8.

Etapa E202

Se verifica si una matriz compuesta de m columnas seleccionadas de forma arbitraria de qm columnas incluidas en las q m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q es una MDS cuadrada. Si el flujo ha pasado la verificación, el flujo procede a la etapa E203; si no, el flujo regresa a la etapa E201. Aquí, la matriz MDS cuadrada significa una matriz que satisface las siguientes propiedades, según se describe más arriba. (a) Es una matriz cuadrada. (b) Determinantes de todas las submatrices incluidas en la matriz son diferentes de cero, a saber, det(submatriz) $\neq$ 0.

Etapa E203

Las q m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q se producen como matrices MDS cuadradas que se aplicarán al cifrado por bloque de clave común tipo Feistel de número de ronda 2r.

A través del proceso de más arriba, se generan las q m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q. Aquí, q satisface $q \leq r$.

En el procesamiento de generación de matriz MDS cuadrada en el ejemplo de procesamiento a1 descrito más arriba, como se explica en la secuencia de procesamiento de la Figura 11, se ha determinado la independencia lineal de una matriz compuesta de m columnas arbitrarias tomadas de qm columnas incluidas en las q m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q en la etapa E102. En el procesamiento de generación de matriz MDS cuadrada en el presente ejemplo de procesamiento a2, se verifica si una matriz compuesta de m columnas arbitrarias tomadas de qm columnas incluidas en las q m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q es una matriz MDS cuadrada. Es decir, se ejecutará una verificación más rigurosa.

De manera similar al ejemplo de procesamiento a1 explicado previamente, las qm-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q generadas por el procesamiento de generación de matriz MDS cuadrada que seguía a una secuencia de procesamiento que se muestra en la presente Figura 12 se configuran como matrices que se aplicarán al procesamiento de conversión lineal de las secciones de conversión lineal de las funciones F de las respectivas

etapas en la estructura criptográfica por bloque de clave común tipo Feistel de número de etapa (número de ronda) 2r, según el procesamiento de [etapa E23] y [etapa E24] explicado previamente con referencia a la Figura 10. Es decir, para etapas numeradas con impares, q matrices MDS cuadradas se designan de forma repetida como L_1, L_2, ..., L_q, L_1, L_2, ... en secuencia a partir de la función F de la etapa superior, y para etapas numeradas con pares, q matrices MDS cuadradas se designan de forma repetida como L_1, L_2, ..., L_q, L_1, L_2, ... en secuencia a partir de la función F de la etapa inferior.

Por consiguiente, las matrices MDS cuadradas de las rondas numeradas con pares y las matrices MDS cuadradas de las rondas numeradas con impares se disponen en órdenes mutuamente inversos, respectivamente, por medio de lo cual se garantiza que el procesamiento de cifrado y el procesamiento de descifrado sean iguales excepto por el procesamiento de reemplazo de una secuencia de claves.

La presente 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 matrices de conversión lineal incluidos en al menos q funciones F consecutivas en rondas numeradas con impares constituyen una matriz MDS cuadrada.

(c) m vectores de columna arbitrarios de matrices de conversión lineal incluidos en al menos q funciones F consecutivas en rondas numeradas con pares constituyen una matriz MDS cuadrada.

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

(d) El número de elementos diferentes de cero en los valores de diferencia obtenidos por contribución de "a" ($a \leq m$) cajas-S activas se convierte en 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 toda la función criptográfica aumenta.

Por consiguiente, mediante el presente ejemplo de procesamiento, es posible ampliar el número mínimo de cajas-S activas en toda la función criptográfica que es uno de los índices de robustez a ataques de criptoanálisis diferencial en el cifrado por bloque de clave común y, como resultado, el número de cajas-S activas en el caso donde se intenta el análisis diferencial (ataque de criptoanálisis diferencial) aumentará y se mejorará la dificultad en el análisis. Por lo tanto, se lleva a cabo un procesamiento criptográfico de alta seguridad cuya clave es difícil de analizar.

(Ejemplo de procesamiento a3)

Se explicará el tercer ejemplo de generación de matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis diferencial y su configuración según las funciones F. El procesamiento de generación de las matrices MDS cuadradas se explicará con referencia al diagrama de flujo de la Figura 13.

Etapa E301

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 qm-ésima matriz MDS cuadrada se genera en GF(2^n). El diagrama de flujo que se muestra en la Figura 1 muestra un ejemplo de procesamiento como con el número de matrices MDS q = 6, el orden de extensión n = 8, y el tamaño de matriz m = 8.

Etapa E302

m filas se seleccionan y extraen de forma arbitraria de la única qm-ésima matriz MDS cuadrada M y se conforma una matriz M' de m-filas y qm-columnas.

Etapa E303

Los qm vectores de columna incluidos en la matriz M' de m-filas y qm-columna se dividen de forma arbitraria en q grupos, cada uno de los cuales consiste en m vectores de columna sin presencia de un vector de columna en dos o más grupos. m-ésimas matrices cuadradas L_1, L_2, ..., L_q se producen a partir de los vectores de columna incluidos en los respectivos grupos como matrices MDS cuadradas que se aplicarán al cifrado por bloque de clave común tipo Feistel de número de ronda 2r.

A través del proceso de más arriba, se generan las q m-ésimas matrices MDS cuadradas L_1, L_2, …, L_q. Aquí, q satisface $q \leq r$.

La técnica de generación de matriz MDS cuadrada 3 en el ejemplo de procesamiento a3 se explicará de manera más concreta con referencia a la Figura 14.

Etapa E301

Una qm-ésima matriz MDS cuadrada M se genera en GF(2^n). Como se muestra en la Figura 14, se genera una matriz MDS cuadrada M de qmxqm. Es preciso observar que el orden de la matriz M generada en la presente etapa E301 puede ser mayor que qm (orden).

Etapa E302

Como se muestra en la Figura 14, se conforman m columnas seleccionadas y extraídas de forma arbitraria de la qm-ésima matriz MDS cuadrada M y una matriz M' de m filas y qm columnas. Es preciso observar que, aunque el ejemplo en la figura se muestra como un ejemplo en el cual m filas consecutivas se seleccionan y extraen, una matriz M' de m filas y qm columnas puede conformarse mediante la selección y extracción de m filas arbitrarias que tengan un espacio entre ellas que constituirá la m-ésima matriz MDS cuadrada M.

Etapa E303

Los qm vectores de columna incluidos en la matriz M' de m filas y qm columnas se dividen en x grupos, cada uno de los cuales tiene m vectores de columna sin presencia de un vector de columna en dos o más grupos, y m-ésimas matrices cuadradas L_1, L_2, ..., L_x se generan a partir de los vectores de columna incluidos en los respectivos grupos.

De manera similar a los ejemplos de procesamiento a1 y a2 explicados previamente, las q m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q generadas por el procesamiento de generación de matriz MDS cuadrada que seguía una secuencia de procesamiento explicada con referencia a las Figuras 13 y 14 se configuran como matrices que se aplicarán al procesamiento de conversión lineal de las secciones de conversión lineal de las funciones F de las respectivas etapas en la estructura criptográfica por bloque de clave común tipo Feistel de número de etapa (número de ronda) 2r, según el procesamiento de [etapa E23] y [etapa E24] explicado previamente con referencia a la Figura 10. Es decir, para etapas numeradas con impares, q matrices MDS cuadradas se designan de forma repetida como L_1, L_2, ..., L_q, L_1, L_2, ... en secuencia a partir de la función F de la etapa superior, y para etapas numeradas con pares, q matrices MDS cuadradas se designan de forma repetida como L_1, L_2, ..., L_q, L_1, L_2, ... de manera secuencial a partir de la función F de la etapa inferior.

Por consiguiente, las matrices MDS cuadradas de las rondas numeradas con pares y las matrices MDS cuadradas de las rondas numeradas con impares se disponen en órdenes mutuamente inversos, respectivamente, por medio de lo cual se garantiza que el procesamiento de cifrado y el procesamiento de descifrado sean iguales excepto por el procesamiento de reemplazo de una secuencia de claves.

La presente 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 la matriz de conversión lineal incluidos en al menos q funciones F consecutivas en las rondas numeradas con impares 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 numeradas con pares son linealmente independientes. Dado que estos aspectos (a) a (c) se garantizan, se garantiza que la cancelación simultánea de diferencias por contribución de m o menos cajas-S activas no ocurra en las 2q-1 rondas consecutivas en la estructura criptográfica por bloque de clave común tipo Feistel con número de ronda de múltiples etapas. Además, se garantiza lo siguiente. (d) De la propiedad de la matriz MDS cuadrada, el número de elementos diferentes de cero en los valores de diferencia obtenidos por contribución de "a" ($a \leq m$) cajas-S activas se convierte en m+1-a o más. Por lo tanto, el valor mínimo del número de cajas-S activas en toda la función criptográfica aumenta.

Un caso donde el ejemplo de procesamiento a3 especialmente produce un efecto es un caso donde m y r se convierten en grandes, un coste de tiempo requerido en un sistema de procesamiento de determinación de matriz de los ejemplos de procesamiento a1 y a2 descritos más arriba se convierte en enorme y, por lo tanto, es difícil determinar una matriz en un tiempo realista. Incluso en dicho caso, si se utiliza la técnica de generación de matriz MDS cuadrada del presente ejemplo de procesamiento a3, el procesamiento de generación de matriz en un tiempo comparativamente corto será posible.

Ello es porque en el ejemplo de procesamiento a3 es posible aplicar un sistema que puede procesar grandes m y r suficientemente en un tiempo realista, por ejemplo, un método de generación para generar una matriz con el código Reed-Solomon.

También en el presente ejemplo de procesamiento a3, según se describe más arriba, es posible ampliar el número mínimo de cajas-S activas en toda la función criptográfica que es uno de los índices de robustez a los ataques de criptoanálisis diferencial en el cifrado por bloque de clave común. Como resultado, cuando se intenta el análisis diferencial (ataque de criptoanálisis diferencial), el número de cajas-S activas aumenta, lo cual mejorará la dificultad en el análisis. Por lo tanto, se lleva a cabo un procesamiento criptográfico de alta seguridad cuya clave es difícil de analizar.

[(3-b) Ejemplo de generación de matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis lineal y su configuración según las funciones F]

A continuación, se explicarán dos ejemplos de procesamiento b1, b2 como ejemplos de generación de las matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis lineal y su configuración según las funciones F.

(Ejemplo de procesamiento b1)

Se explicará un primer ejemplo de generación de las matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis lineal y su configuración según las funciones F. El procesamiento de generación de las matrices MDS cuadradas se explicará con referencia al diagrama de flujo que se muestra en la Figura 15.

Etapa E401

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 m-ésimas matrices MDS cuadradas M_1, M_2, ..., M_q se generan de forma aleatoria en GF(2^n). El diagrama de flujo que se muestra en la Figura 14 muestra un ejemplo de procesamiento como con el número de matrices MDS cuadradas q = 6, el orden de extensión n = 8, y el tamaño de matriz m = 8.

Etapa E402

Se verifica si m vectores de fila arbitrarios tomados de 2m vectores de fila incluidos en dos matrices inversas adyacentes después de calcular las matrices inversas M_1^{-1}, M_2^{-1}, ..., M_q^{-1}, de q m-ésimas matrices MDS cuadradas M_1, M_2, ..., de M_q son linealmente independientes. t^R en la Figura 15 denota un vector transpuesto de un vector de fila. Si el flujo ha pasado la verificación, el flujo procede a la etapa E403; si no, el flujo regresa a la etapa E401. Aquí, las matrices $M1^{-1}$, Mq^{-1} se considerarán matrices adyacentes.

Etapa E403

Las q m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q se producen como matrices MDS cuadradas que se aplicarán al cifrado por bloque de clave común tipo Feistel de número de ronda 2r.

A través del proceso de más arriba, se generan las q m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q. Aquí, q satisface $q \leq r$.

Las q m-ésimas matrices MDS cuadradas generadas de esta manera L_1, L_2, ..., L_q se configuran como matrices que se aplicarán al procesamiento de conversión lineal de las secciones de conversión lineal de las funciones F de las respectivas etapas en la estructura criptográfica por bloque de clave común tipo Feistel de número de etapa (número de ronda) 2r, según el procesamiento de [etapa E23] y [etapa E24] explicado previamente con referencia a la Figura 10. Es decir, para las etapas numeradas con impares, q matrices MDS cuadradas se designan, de manera repetida, como L_1, L_2, ... , L_q, L_1, L_2, ... en secuencia a partir de la función F de la etapa superior, y para etapas numeradas con pares, q matrices MDS cuadradas se designan de forma repetida como L_1, L_2, .. , L_q, L_1, L_2, ... de manera secuencial a partir de la función F de la etapa inferior.

Las matrices MDS cuadradas de las rondas numeradas con pares y las matrices MDS cuadradas de las rondas numeradas con impares se disponen en órdenes mutuamente inversos, respectivamente, por medio de lo cual se garantiza que el procesamiento de cifrado y el procesamiento de descifrado sean iguales excepto por el reemplazo de una secuencia de claves.

La presente 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 de manera consecutiva en rondas numeradas con impares en una función criptográfica y en una matriz inversa incluidos de forma consecutiva en rondas numeradas con pares son linealmente independientes. Estas propiedades permiten aumentar la dificultad en el análisis por aproximación lineal en ataques de criptoanálisis lineal, y se lleva a cabo un procesamiento criptográfico de alta seguridad con dificultad aumentada en el análisis, es decir, cuya clave es difícil de analizar.

(Ejemplo de procesamiento b2)

Se explicará un segundo ejemplo de generación de las matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis lineal y su configuración según las funciones F. La explicación se proveerá para el procesamiento de generación de la matriz MDS cuadrada con referencia al diagrama de flujo que se muestra en la Figura 16.

Etapa E501

Designación de 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 m-ésimas matrices MDS cuadradas M_1, M_2, ..., M_q se generan de forma aleatoria en GF(2^n). El diagrama de flujo que se muestra en la Figura 16 muestra un ejemplo de procesamiento como con el número de matrices MDS cuadradas q = 6, el orden de extensión n = 8, y el tamaño de matriz m = 8.

Etapa E502

Se verifica si m vectores de fila arbitrarios tomados de 2m vectores de fila incluidos en dos matrices inversas adyacentes después de calcular las matrices inversas M_1^{-1}, M_2^{-1}, ..., M_q^{-1}, de las q m-ésimas matrices MDS cuadradas M_1, M_2, ..., de M_q constituyen una matriz MDS cuadrada. ${}^tR$ en la Figura 16 denota un vector transpuesto de un vector de fila. Si el flujo ha pasado la verificación, el flujo procede a la etapa E503; si no, el flujo regresa a la etapa E401. Aquí, las matrices $M1^{-1}$, Mq^{-1} se considerarán matrices adyacentes. La matriz MDS cuadrada es una matriz que satisface las siguientes propiedades. (a) Es una matriz cuadrada. (b) Determinantes de todas las submatrices incluidas en la matriz son diferentes de cero, a saber, det(submatriz) ≠ 0.

Etapa E503

Las q m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q se producen como matrices MDS cuadradas que se aplicarán al cifrado por bloque de clave común tipo Feistel de número de ronda 2r.

A través del proceso de más arriba, se generan las q m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q. Aquí, q satisface $q \leq r$.

En el procesamiento de generación de matriz MDS cuadrada en el ejemplo de procesamiento b1 descrito más arriba, como se explica en la secuencia de procesamiento de la Figura 15, lo que se determina es la independencia lineal cuando se toman m vectores de columna arbitrarios de qm vectores de columna incluidos en las matrices inversas M_1^{-1}, M_2^{-1}, ..., M_q^{-1} de las q m-ésimas matrices MDS cuadradas M_1, M_2, ..., M_q en la etapa E402. En el procesamiento de generación de matriz MDS cuadrada en el presente ejemplo de procesamiento b2, se verifica si m vectores de columna arbitrarios tomados de m vectores de columna incluidos en matrices inversas M_1^{-1}, M_2^{-1}, ..., M_q^{-1} de las q m-ésimas matrices MDS cuadradas M_1, M_2, ..., M_q constituyen una matriz MDS cuadrada. Es decir, se ejecutará una verificación más rigurosa.

De manera similar al ejemplo de procesamiento b1 descrito previamente, las q m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q generadas por el procesamiento de generación de matriz MDS cuadrada que cumple con una secuencia de procesamiento que se muestra en la presente Figura 16 se configuran como matrices que se aplicarán al procesamiento de conversión lineal de las secciones de conversión lineal de las funciones F de las respectivas etapas en la estructura criptográfica por bloque de clave común tipo Feistel de número de etapa (número de ronda) 2r, según el procesamiento [etapa E23] y [etapa E24] explicado previamente con referencia a la Figura 10. Es decir, para etapas numeradas con impares, q matrices MDS cuadradas se designan como L_1, L_2, ..., L_q, L_1, L_2, ... en secuencia y de forma repetida a partir de la función F de la etapa superior, y para etapas numeradas con pares, q matrices MDS cuadradas se designan como L_1, L_2, ..., L_q, L_1, L_2, ... en secuencia y de forma repetida a partir de la función F de la etapa inferior.

Por consiguiente, las matrices MDS cuadradas de las rondas numeradas con pares y las matrices MDS cuadradas de las rondas numeradas con impares se disponen en órdenes mutuamente inversos, respectivamente, por medio de lo cual se garantiza que el procesamiento de cifrado y el procesamiento de descifrado sean iguales excepto por el procesamiento de reemplazo de una secuencia de claves.

La presente 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 matrices inversas de la matriz de conversión lineal incluidos de manera consecutiva en rondas numeradas con impares en la función criptográfica y de la matriz de conversión lineal incluidos de manera consecutiva en rondas numeradas con pares constituyen una matriz MDS cuadrada. Estas propiedades permiten aumentar la dificultad en el análisis por aproximación lineal en ataques de criptoanálisis lineal, y se lleva a cabo un procesamiento 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 llevan a cabo una resistencia mejorada a ataques de criptoanálisis diferencial y a ataques de criptoanálisis lineal y su configuración según las funciones F]

A continuación, se explicará un ejemplo de generación de matrices MDS cuadradas que llevan a cabo una resistencia mejorada a ataques de criptoanálisis diferencial y a ataques de criptoanálisis lineal y su configuración según las funciones F.

El algoritmo criptográfico con la resistencia a ataques de criptoanálisis diferencial se lleva a cabo mediante la aplicación del procesamiento explicado con referencia a las Figuras 10 a 13 previamente, es decir, mediante configuración de matrices MDS cuadradas que se aplicarán a la conversión lineal en las secciones de procesamiento lineal de las funciones F mediante aplicación de cualquiera de los ejemplos de procesamiento a1 (Figura 11) a a3 (Figura 13) descritos más arriba. Además, el algoritmo criptográfico con la resistencia a ataques de criptoanálisis lineal se lleva a cabo mediante aplicación del procesamiento explicado con referencia a la Figura 10 y a las Figuras 14 y 15 previamente, es decir, mediante establecimiento de matrices MDS cuadradas que se aplicarán

a la conversión lineal en las secciones de procesamiento lineal de las funciones F mediante aplicación de cualquiera de los ejemplos de procesamiento b1 (Figura 14) y b2 (Figura 15) descritos más arriba.

El algoritmo que usa matrices MDS cuadradas que llevan a cabo la resistencia mejorada a ataques de criptoanálisis diferencial y ataques de criptoanálisis lineal se implementa mediante configuración de matrices MDS cuadradas generadas llevando a cabo tanto uno del procesamiento de los ejemplos de procesamiento a1 (Figura 11) a a3 (Figura 12) como uno del procesamiento de los ejemplos de procesamiento b1 (Figura 14) y b2 (Figura 15) como matrices que se aplicarán al procesamiento de conversión lineal de las secciones de conversión lineal de las funciones F de las respectivas etapas en la estructura criptográfica por bloque de clave común tipo Feistel de número de etapa (número de ronda) 2r.

Es decir, q matrices MDS cuadradas se generan por cualquiera de las siguientes combinaciones: un ejemplo de procesamiento a1 y un ejemplo de procesamiento b1; un ejemplo de procesamiento a1 y un ejemplo de procesamiento b2; un ejemplo de procesamiento a2 y un ejemplo de procesamiento b1; un ejemplo de procesamiento a2 y un ejemplo de procesamiento b2; un ejemplo de procesamiento a3 y un ejemplo de procesamiento b1; un ejemplo de procesamiento a3 y un ejemplo de procesamiento b2; y se configuran como matrices que se aplicarán al procesamiento de conversión lineal de las secciones de conversión lineal de las funciones F de las respectivas etapas en la estructura criptográfica por bloque de clave común tipo Feistel de número de ronda 2r. Es decir, para etapas numeradas con impares, q matrices MDS cuadradas se designan de forma repetida como L_1, L_2, ..., L_q, L_1, L_2, ... en secuencia a partir de la función F de la etapa superior, y para etapas numeradas con pares, q matrices MDS cuadradas se designan de forma repetida como L_1, L_2, ..., L_q, L_1, L_2, ... en secuencia a partir de la función F de la etapa inferior. Mediante la presente configuración, el procesamiento criptográfico que lleva a cabo la resistencia mejorada a ataques de criptoanálisis diferencial y a ataques de criptoanálisis lineal se convierte en posible.

Un ejemplo de procesamiento de generación de matrices MDS cuadradas para implementar el procesamiento criptográfico que lleva a cabo la resistencia mejorada a ataques de criptoanálisis diferencial y a ataques de criptoanálisis lineal se explicará con referencia a la Figura 17. El presente procesamiento es una combinación del ejemplo de procesamiento a2 y ejemplo de procesamiento b2 descritos más arriba.

Etapa E601

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 m-ésimas matrices cuadradas se generan de forma aleatoria en $GF(2^n)$. El diagrama de flujo que se muestra en la Figura 17 muestra un ejemplo de procesamiento como con el número de matrices MDS cuadradas q = 6, el orden de extensión n = 8, y el tamaño de matriz m = 8.

Etapa E602

Cuando m columnas se toman de qm columnas incluidas en las q m-ésimas matrices MDS cuadradas, M_1, M_2, ..., M_q, se verifica si ellas constituyen una matriz MDS cuadrada. Si el flujo ha pasado la verificación, el flujo procede a la etapa E603; si no, el flujo regresa a la etapa E601. 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 diferente de cero, a saber, det(submatriz) ≠ 0.

Etapa E603

Matrices inversas M_1^{-1}, M_2^{-1}, ..., M_q^{-1} de las q m-ésimas matrices MDS cuadradas M_1, M_2, ..., M_q se calculan, y se verifica si m vectores de fila arbitrarios tomados de 2m vectores de fila incluidos en dos matrices inversas adyacentes constituyen una matriz MDS cuadrada. tR en la Figura 17 denota un vector transpuesto de un vector de fila. Si el flujo ha pasado la verificación, el flujo procede a la etapa E604; si no, el flujo regresa a la etapa E601. Aquí, las matrices M_1^{-1}, Mq-1 se considerarán matrices adyacentes.

Etapa E604

Las q m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q se producen como matrices MDS cuadradas que se aplicarán al cifrado por bloque de clave común tipo Feistel de número de ronda 2r.

A través del proceso de más arriba, se generan las q m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q. Aquí, q satisface $q \leq r$.

Las q m-ésimas matrices MDS cuadradas L_1, L_2, ..., L_q generadas por el procesamiento de generación de matriz MDS cuadrada que seguía una secuencia de procesamiento que se muestra en la presente Figura 17 se configuran como matrices que se aplicarán al procesamiento de conversión lineal de las secciones de conversión lineal de las secciones de funciones F de las respectivas etapas en la estructura criptográfica por bloque de clave común tipo Feistel de número de etapa (número de ronda) 2r, según el procesamiento de [etapa E23] y [etapa E24] explicado previamente con referencia a la Figura 10. Es decir, para las etapas numeradas con impares, q matrices MDS cuadradas se designan, de manera repetida, como L_1, L_2, ... , L_q, L_1, L_2, ... de forma secuencial a partir de la función

F de la etapa superior, y para etapas numeradas con pares, q matrices MDS cuadradas se designan, de manera repetida, como L_1, L_2,..., L_q, L_1, L_2,... de forma secuencial a partir de la función F de la etapa inferior.

Por consiguiente, las matrices MDS cuadradas de las rondas numeradas con pares y las matrices MDS cuadradas de las rondas numeradas con impares se disponen en órdenes mutuamente inversos, respectivamente, por medio de lo cual se garantiza que el procesamiento de cifrado y el procesamiento de descifrado sean iguales excepto por el procesamiento de reemplazo de una secuencia de claves.

La presente 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 incluidos en al menos q funciones F consecutivas en rondas numeradas con impares en la función criptográfica constituyen una matriz MDS cuadrada. (c) m vectores de columna arbitrarios de la matriz de conversión lineal incluidos en al menos q funciones F consecutivas en rondas numeradas con pares constituyen una matriz MDS cuadrada. Dado que dichos aspectos (a) a (c) se garantizan, en la estructura criptográfica por bloque de clave común tipo Feistel con número de ronda de las múltiples etapas, se garantiza que la cancelación simultánea de diferencias por contribución de m o menos cajas-S activas no ocurra en las 2q-1 rondas consecutivas. Además, (d) de la propiedad de la matriz MDS cuadrada, se garantiza que el número de elementos diferentes de cero en los valores de diferencia obtenidos por contribución de "a" ($a \leq m$) cajas-S activas se convierte en m+1-a o más. Por lo tanto, el valor mínimo del número de cajas-S activas en toda la función criptográfica aumenta. Además, se garantiza lo siguiente. (e) m vectores de columna arbitrarios de matrices inversas de las matrices de conversión lineal incluidos de manera consecutiva en las rondas numeradas con impares y de las matrices de conversión lineal incluidos de manera consecutiva en las rondas numeradas con pares en la función criptográfica constituyen una matriz MDS cuadrada. Estas propiedades permiten aumentar la dificultad en el análisis por aproximación lineal en ataques de criptoanálisis lineal, y se lleva a cabo un procesamiento criptográfico de alta seguridad con dificultad aumentada en el análisis, es decir, cuya clave es difícil de analizar.

Por consiguiente, mediante el presente ejemplo de procesamiento, la dificultad en el análisis en ataques de criptoanálisis diferencial y ataques de criptoanálisis lineal aumenta, y se lleva a cabo el procesamiento criptográfico de alta seguridad cuya clave es difícil de analizar. El ejemplo que se muestra en la Figura 17 ha sido, como se describe más arriba, un ejemplo de generación de las matrices MDS cuadradas por la combinación del ejemplo de procesamiento a2 y ejemplo de procesamiento b2 explicados previamente. Sin embargo, puede adoptarse otra generación. Es decir, q matrices MDS cuadradas se generan mediante combinación de uno de los siguientes pares: el ejemplo de procesamiento a1 y el ejemplo de procesamiento b1, el ejemplo de procesamiento a1 y el ejemplo de procesamiento b2, el ejemplo de procesamiento a2 y el ejemplo de procesamiento b1, el ejemplo de procesamiento a3 y el ejemplo de procesamiento b1, y el ejemplo de procesamiento a3 y el ejemplo de procesamiento b2. Para etapas numeradas con impares, q matrices MDS cuadradas se designan de forma repetida como L_1, L_2, ..., L_q, L_1, L_2, ... en secuencia a partir de la función F de la etapa superior, y para etapas numeradas con pares, q matrices MDS cuadradas se designan, de forma repetida, como L_1, L_2, ..., L_q, L_1, L_2,... en secuencia a partir de la función F de la etapa inferior, como una matriz que se aplicará en las secciones de conversión lineal de las funciones F de las respectivas etapas en la estructura criptográfica por bloque de clave común tipo Feistel de número de etapa (número de ronda) 2r; por medio de lo cual se puede llevar a cabo el procesamiento criptográfico de alta seguridad que ha mejorado la dificultad en el análisis tanto en ataques de criptoanálisis diferencial como en ataques de criptoanálisis lineal y cuya clave es difícil de analizar.

Aunque la explicación hasta este punto ha supuesto 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 de mn bits a mn bits, el efecto similar a ataques de criptoanálisis diferencial y ataques de criptoanálisis lineal puede obtenerse, de manera efectiva, incluso en el caso donde se utiliza una matriz mnxmn definida en GF(2). En realidad, la matriz arbitraria en $GF(2^n)$ puede llevarse a una correspondencia uno a uno con una matriz en GF(2) que muestre la misma conversión. Por lo tanto, puede decirse que la matriz en GF(2) muestra una representación más general. La matriz en GF(2) tiene mn columnas y mn filas, las cuales son n-veces aquellas en el caso de $GF(2^n)$. Por este motivo, la primera columna de la matriz en $GF(2^n)$ corresponde a la primera a n-ésima columnas de la matriz en GF(2), y la primera fila de la matriz en $GF(2^n)$ corresponde a la primera a n-ésima filas de aquella. Es decir, la i-ésima fila corresponde a [(i-1)+1]-ésima a [(i-1)+n]-ésima filas, y la i-ésima columna corresponde a [(i-1)+1]-ésima a [(i-1)+n]-ésima columnas. Por lo tanto, con el fin de llevar a cabo una operación de extracción de una columna o fila en $GF(2^n)$, si se usa una matriz definida en GF(2), es necesario llevar a cabo una operación de extracción de n filas o n columnas que correspondan a la columna o fila en GF(2) de manera acorde. 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 de más arriba permite que las matrices se extiendan fácilmente a matrices definidas en GF(2).

Finalmente, la Figura 18 muestra una configuración a modo de ejemplo de un módulo CI 600 como un aparato de procesamiento criptográfico para llevar a cabo el procesamiento criptográfico. El procesamiento descrito más arriba es ejecutable en varios aparatos de procesamiento de información, por ejemplo, un PC, una tarjeta IC, un lector/escritor, etc., y el módulo CI 600 que se muestra en la Figura 18 puede usarse como un constituyente para dichos varios aparatos.

Una CPU (unidad central de procesamiento, CPU, por sus siglas en inglés) 601 que se muestra en la Figura 18 es un procesador para ejecutar varios programas como, por ejemplo, iniciar el procesamiento criptográfico, finalizarlo, controlar la transmisión/recepción de datos, controlar la transferencia de datos entre secciones de configuración, y

ejecutar varios programas. La memoria 602 consiste en ROM (memoria de solo lectura, ROM, por sus siglas en inglés) para almacenar un programa que la CPU 601 ejecuta o datos fijos como parámetros de operación, RAM (memoria de acceso aleatorio, RAM, por sus siglas en inglés) utilizada como un área de almacenamiento del programa ejecutado en el procesamiento de la CPU 601, parámetros que siempre varían en el procesamiento del programa, y un área de trabajo, etc. La memoria 602 puede también utilizarse como un área de almacenamiento de datos clave necesarios para el procesamiento criptográfico, etc. Es preferible que un área de almacenamiento de datos, etc., se construya como memoria con una estructura con sello de seguridad.

Una sección de procesamiento criptográfico 603 lleva a cabo el cifrado, descifrado, etc., que sigue, por ejemplo, el algoritmo de procesamiento criptográfico por bloque de clave común tipo Feistel descrito más arriba. Aunque se muestra el ejemplo en el cual el medio de procesamiento criptográfico se lleva a cabo como un módulo individual, este puede configurarse de modo que, por ejemplo, un programa criptográfico se almacena en ROM y la CPU 601 lee y ejecuta el programa almacenado en la ROM sin proveer dicho módulo criptográfico independiente.

Un generador de número aleatorio 604 ejecuta el procesamiento de generación de números aleatorios que son necesarios en la generación de una clave que se requiere para el procesamiento criptográfico y similares.

Una sección de transmisión/recepción 605 es una sección de comunicación de datos para llevar a cabo la comunicación de datos de forma externa, que ejecuta la comunicación de datos con, por ejemplo, un lector-escritor, etc., y un módulo CI, y que produce un texto cifrado generado en el módulo CI o ingresa allí datos, etc., del lector escritor externo, etc.

En lo anterior, la presente invención se ha descrito en detalle con referencia a realizaciones específicas. Sin embargo, es evidente que las personas con experiencia en la técnica pueden lograr la modificación y sustitución de la realización sin desviarse del alcance de la presente invención. Es decir, la presente invención fue divulgada a modo de ilustración y no debería interpretarse restrictivamente. El alcance de la invención se define por las reivindicaciones anexas.

Es preciso observar que una serie de procesamientos explicada en la descripción puede implementarse por hardware, por software, o por una combinación de ambos. Cuando se lleva a cabo el procesamiento por software, un programa que registra una secuencia de procesamiento puede ejecutarse mediante su instalación en la memoria construida en hardware exclusivo en un ordenador, o puede ejecutarse mediante su instalación en un ordenador de propósito general que pueda llevar a cabo varios procesamientos.

Por ejemplo, un programa puede registrarse con antelación en un disco duro o ROM (memoria de solo lectura) como un medio de registro. De manera alternativa, el programa puede almacenarse de forma temporal o permanente en medios de registro extraíbles como, por ejemplo, un disco flexible, CD-ROM (memoria de solo lectura de disco compacto, CD-ROM, por sus siglas en inglés), un disco MO (magneto-óptico), un DVD (disco versátil digital), un disco magnético y memoria de semiconductor. Dicho medio de registro extraíble puede proveerse como el así llamado paquete de software.

Además de instalar el programa en el ordenador desde un medio de registro extraíble según se describe más arriba, puede adoptarse el siguiente esquema. El programa se transfiere de manera inalámbrica al ordenador desde un sitio de descarga, o se transfiere por cable al ordenador a través de una red como, por ejemplo, una LAN (red de área local, LAN, por sus siglas en inglés) e Internet, mientras el ordenador recibe el programa que se está transfiriendo de tal modo y lo instala en un medio de registro como, por ejemplo, un disco duro interno.

Es preciso observar que varios tipos de procesamientos escritos en la descripción pueden ejecutarse en paralelo o individualmente según la capacidad de procesamiento del aparato que está llevando a cabo el procesamiento o si fuera necesario que se está ejecutando en secuencia temporal según la descripción. Es preciso observar que, en la presente descripción, el sistema es uno que tiene una estructura de combinación lógica de múltiples dispositivos, pero que no se encuentra limitado a sistemas que tienen, cada uno, sus propios dispositivos en el mismo recinto.

Como se describe más arriba, según la configuración de la presente invención, en el procesamiento criptográfico por bloque de clave común tipo Feistel de ejecución de la función F del tipo SPN que tiene la sección de conversión no lineal y la sección de conversión lineal de forma repetida para múltiples rondas, se configura para llevar a cabo lo siguiente. Mientras se lleva a cabo el procesamiento de conversión lineal de la función F correspondiente a cada una de las múltiples rondas como procesamiento de conversión lineal que aplica las matrices MDS (distancia máxima separable) cuadradas, se aplican las matrices MDS cuadradas L_a, L_b que son diferentes al menos en las rondas consecutivas numeradas con impares y en las rondas consecutivas numeradas con pares, respectivamente, y el procesamiento de conversión lineal con matrices MDS cuadradas se lleva a cabo, en donde se aplican matrices MDS cuadradas L_a, L_b diferentes al menos en las rondas consecutivas numeradas con pares y en las rondas consecutivas numeradas con impares, y una matriz compuesta de m vectores de columna seleccionados de forma arbitraria de los vectores de columna que constituyen las matrices inversas L_a^{-1}, L_b^{-1} de las matrices MDS cuadradas es linealmente independiente o constituye una matriz MDS cuadrada. Por consiguiente, la resistencia a ataques de criptoanálisis lineal en el cifrado por bloque de clave común se mejora y la dificultad para analizar una clave de cifrado, etc., aumenta, de modo que se lleva a cabo un procesamiento criptográfico de alta seguridad. Por lo tanto, la

presente invención puede aplicarse a un aparato de procesamiento criptográfico que se requiere para mejorar la dificultad en el análisis para encontrar una clave y tener alta seguridad.

Además, según la configuración de la presente invención, en el procesamiento criptográfico por bloque de clave común tipo Feistel que ejecuta la función F del tipo SPN que tiene la sección de conversión no lineal y la sección de conversión lineal de manera repetida en múltiples rondas se configura para llevar a cabo el procesamiento de conversión lineal de la función F correspondiente a cada una de las múltiples rondas como procesamiento de conversión lineal que aplica matrices MDS (distancia máxima separable) cuadradas, y al mismo tiempo aplica matrices MDS cuadradas que son diferentes al menos en las rondas consecutivas numeradas con pares y en las rondas consecutivas numeradas con impares, en donde dichas matrices MDS cuadradas exhiben independencia lineal o constituyen matrices MDS cuadradas. Por lo tanto, se garantiza que no ocurra la cancelación simultánea de diferencias por contribución de cajas-S activas y es posible ampliar un número mínimo de cajas-S activas en toda la función criptográfica que es uno de los índices de robustez a los ataques de criptoanálisis diferencial en el cifrado por bloque de clave común. Mediante la presente configuración, se mejora la resistencia tanto a ataques de criptoanálisis lineal como a ataques de criptoanálisis diferencial y, por consiguiente, se implementa un procesamiento criptográfico de mayor seguridad. Por lo tanto, la presente invención puede aplicarse al aparato de procesamiento criptográfico que se requiere para aumentar la dificultad al analizar una clave y tener alta seguridad.

REIVINDICACIONES

1. Un aparato de procesamiento de información, que comprende:

una unidad de memoria tangible (602) que almacena datos claves necesarios para el procesamiento criptográfico tipo Feistel;

un procesador (601) configurado para ejecutar varios programas y para controlar el inicio y la finalización del procesamiento criptográfico tipo Feistel; y

un aparato de procesamiento de cifrado (603) configurado para llevar a cabo el procesamiento criptográfico tipo Feistel, el aparato de procesamiento de cifrado incluyendo

una primera sección de procesamiento de cifrado que opera en una ronda n del procesamiento criptográfico tipo Feistel y que incluye una primera sección de transformación no lineal (121) configurada para transformar información de entrada en primera información transformada no lineal, y una primera sección de transformación lineal (122) configurada para transformar la primera información transformada no lineal en primera información transformada lineal;

una segunda sección de procesamiento de cifrado que opera en una ronda n+2 del procesamiento criptográfico tipo Feistel y que incluye una segunda sección de transformación no lineal configurada para transformar la información de entrada en segunda información transformada no lineal, y una segunda sección de transformación lineal configurada para transformar la segunda información transformada no lineal en segunda información transformada lineal; y

una sección OR exclusiva (142, 143, 144) configurada para llevar a cabo una operación OR exclusiva según la segunda información transformada lineal y la primera información transformada lineal,

caracterizado por que

cuando la primera información transformada no lineal se expresa como un primer vector de secuencia, la primera información transformada lineal se expresa como un segundo vector de secuencia, la segunda información transformada no lineal se expresa como tercer vector de secuencia, y la segunda información transformada lineal se expresa como un cuarto vector de secuencia, entonces (1) un primer vector de fila elegido de una primera matriz inversa de una primera matriz MDS cuadrada que transforma el primer vector de secuencia en el segundo vector de secuencia, y (2) un segundo vector de fila elegido de una segunda matriz inversa de una segunda matriz MDS cuadrada que transforma el tercer vector de secuencia en el cuarto vector de secuencia y que es diferente de la primera matriz MDS cuadrada, son linealmente independientes.

2. El aparato de procesamiento de información de la reivindicación 1, en donde la unidad de memoria (602) comprende:

una memoria de solo lectura que almacena parámetros de operación y los varios programas que el procesador ejecuta; y

una memoria de acceso aleatorio que almacena parámetros que varían durante la ejecución de los varios programas.

3. El aparato de procesamiento de información de la reivindicación 1, que además comprende:

un generador de número aleatorio (604) configurado para generar el número aleatorio necesario para generar los datos claves.

4. El aparato de procesamiento de información de la reivindicación 1, que además comprende:

una unidad de transmisión/recepción (605) configurada para ejecutar la comunicación de datos con un dispositivo externo.

5. El aparato de procesamiento de información de la reivindicación 1, en donde el aparato de procesamiento de información es un ordenador (600).

6. El aparato de procesamiento de información de la reivindicación 1, en donde el aparato de procesamiento de información es una tarjeta IC.

7. El aparato de procesamiento de información de la reivindicación 1, en donde el aparato de procesamiento de información es un aparato lector/escritor.

8. El aparato de procesamiento de información según la reivindicación 1, en donde el aparato de procesamiento de cifrado además comprende:

una sección de adquisición de clave configurada para adquirir la clave común que se utiliza en un aparato de descifrado.

9. El aparato de procesamiento de información según la reivindicación 1, en donde el aparato de procesamiento de cifrado además comprende:

una sección de clave expandida configurada para producir claves expandidas, y en donde una de las claves expandidas se ingresa a la primera sección de procesamiento de cifrado, y la otra de las claves expandidas se ingresa a la segunda sección de procesamiento de cifrado.

10. Un aparato de procesamiento de descifrado, que comprende:

una unidad de memoria tangible (602) que almacena datos claves necesarios para el procesamiento de descifrado tipo Feistel;

un procesador (601) configurado para ejecutar varios programas y para controlar el inicio y la finalización del procesamiento de descifrado tipo Feistel; y

un aparato de procesamiento de descifrado (603) configurado para llevar a cabo el procesamiento de descifrado tipo Feistel, el aparato de procesamiento de descifrado incluyendo

una primera sección de procesamiento de descifrado que opera en una ronda n del procesamiento de descifrado tipo Feistel y que incluye una primera unidad de transformación no lineal (121) configurada para transformar de información de entrada a primera información transformada no lineal, y una primera unidad de transformación lineal (122) configurada para transformar de dicha información transformada no lineal a primera información transformada lineal;

una segunda sección de procesamiento de descifrado que opera en una ronda n+2 del procesamiento de descifrado tipo Feistel y que incluye una segunda unidad de transformación no lineal configurada para transforma de información de entrada a segunda información transformada no lineal, y una segunda unidad de transformación lineal configurada para transformar de dicha información transformada no lineal a segunda información transformada lineal; y

una sección OR exclusiva (142, 143, 144) configurada para llevar a cabo una operación OR exclusiva según dicha segunda información transformada lineal y dicha primera información transformada lineal,

caracterizado por que

cuando dicha primera información transformada no lineal se expresa como un primer vector de secuencia, dicha primera información transformada lineal se expresa como un segundo vector de secuencia, dicha segunda información transformada no lineal se expresa como un tercer vector de secuencia, y dicha segunda información transformada lineal se expresa como un cuarto vector de secuencia, un primer vector de fila elegido de una matriz inversa de una primera matriz MDS cuadrada, que indica transformación de dicho primer vector de secuencia a dicho segundo vector de secuencia, y un segundo vector de fila elegido de una matriz inversa de una segunda matriz MDS cuadrada, que indica una transformación de dicho tercer vector de secuencia a dicho cuarto vector de secuencia y que es diferente de dicha primera matriz MDS cuadrada, son linealmente independientes.

11. El aparato de procesamiento de descifrado según la reivindicación 10, que además comprende:

una sección de adquisición de clave configurada para adquirir la clave común que se utiliza en un aparato de cifrado.

12. El aparato de procesamiento de descifrado según la reivindicación 10, que además comprende:

una sección de clave expandida configurada para producir claves expandidas, y en donde una de las claves expandidas se ingresa a la primera sección de procesamiento de descifrado, y la otra de las claves expandidas se ingresa a la segunda sección de procesamiento de descifrado.

FIG. 1

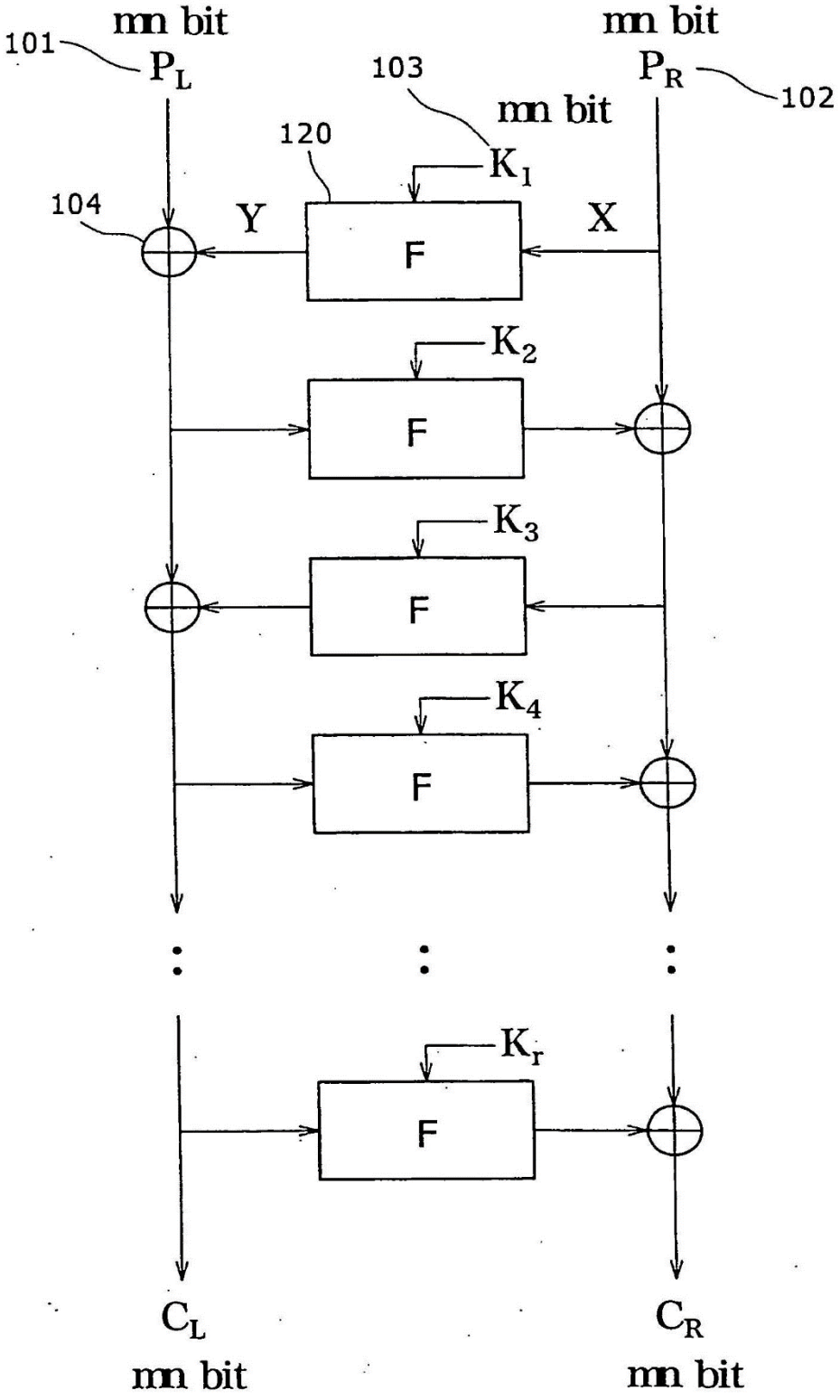

mn bit
101
P_L
mn bit
P_R
102
103
mn bit
120
K_1
104
Y
X
F
K_2
F
K_3
F
K_4
F
K_r
F
C_L
mn bit
C_R
mn bit

FIG. 2A

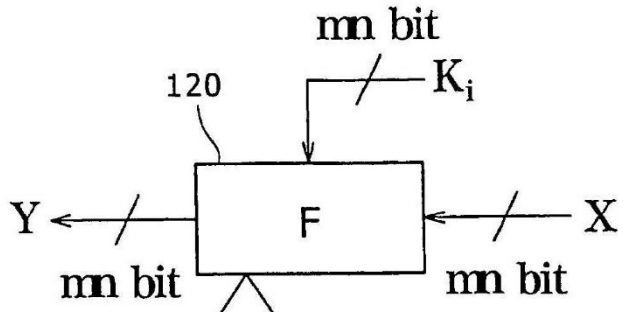

mn bit
K_i
120
Y
F
X
mn bit
mn bit

FIG. 2B

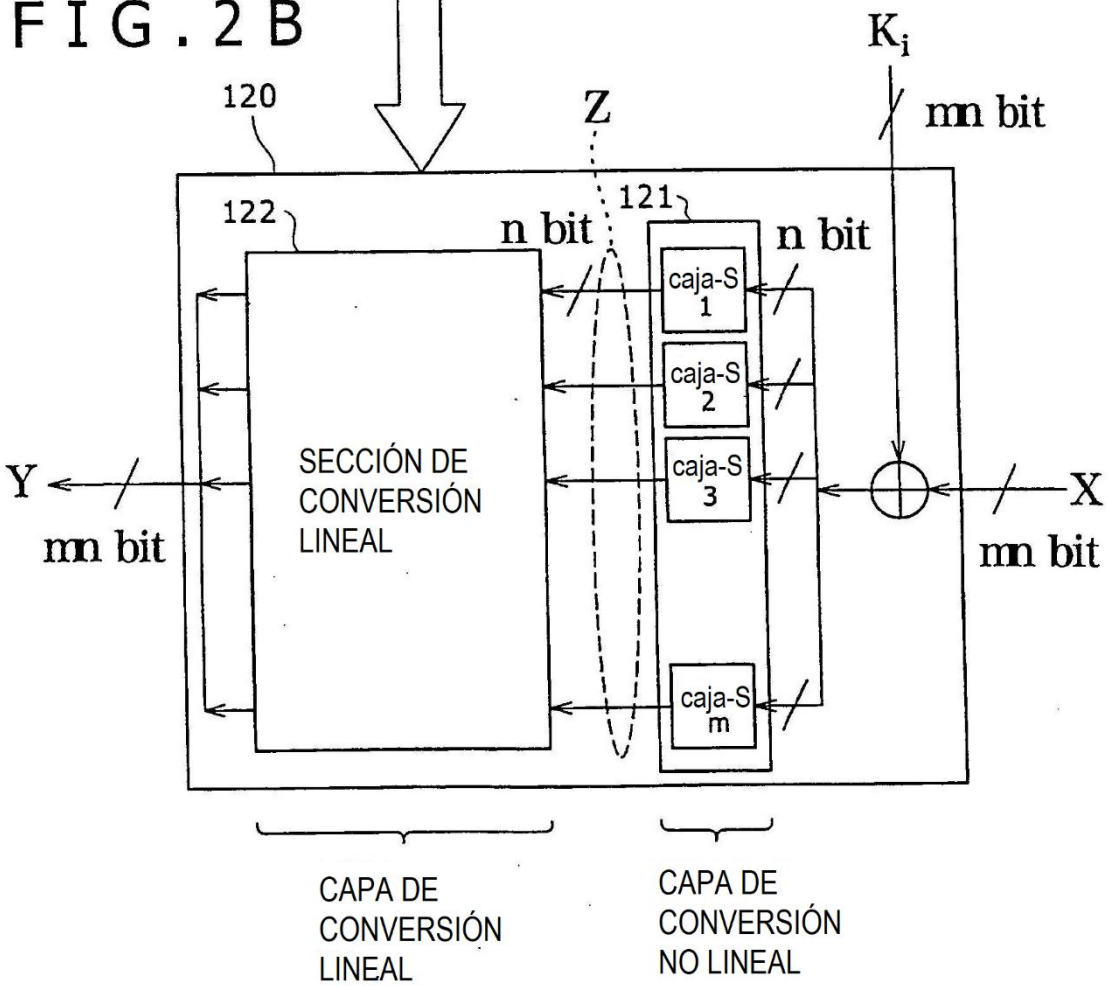

K_i
120
Z
mn bit
122
121
n bit
n bit
caja-S 1
caja-S 2
caja-S 3
caja-S m
Y
SECCIÓN DE CONVERSIÓN LINEAL
X
mn bit
mn bit
CAPA DE CONVERSIÓN LINEAL
CAPA DE CONVERSIÓN NO LINEAL

FIG. 3

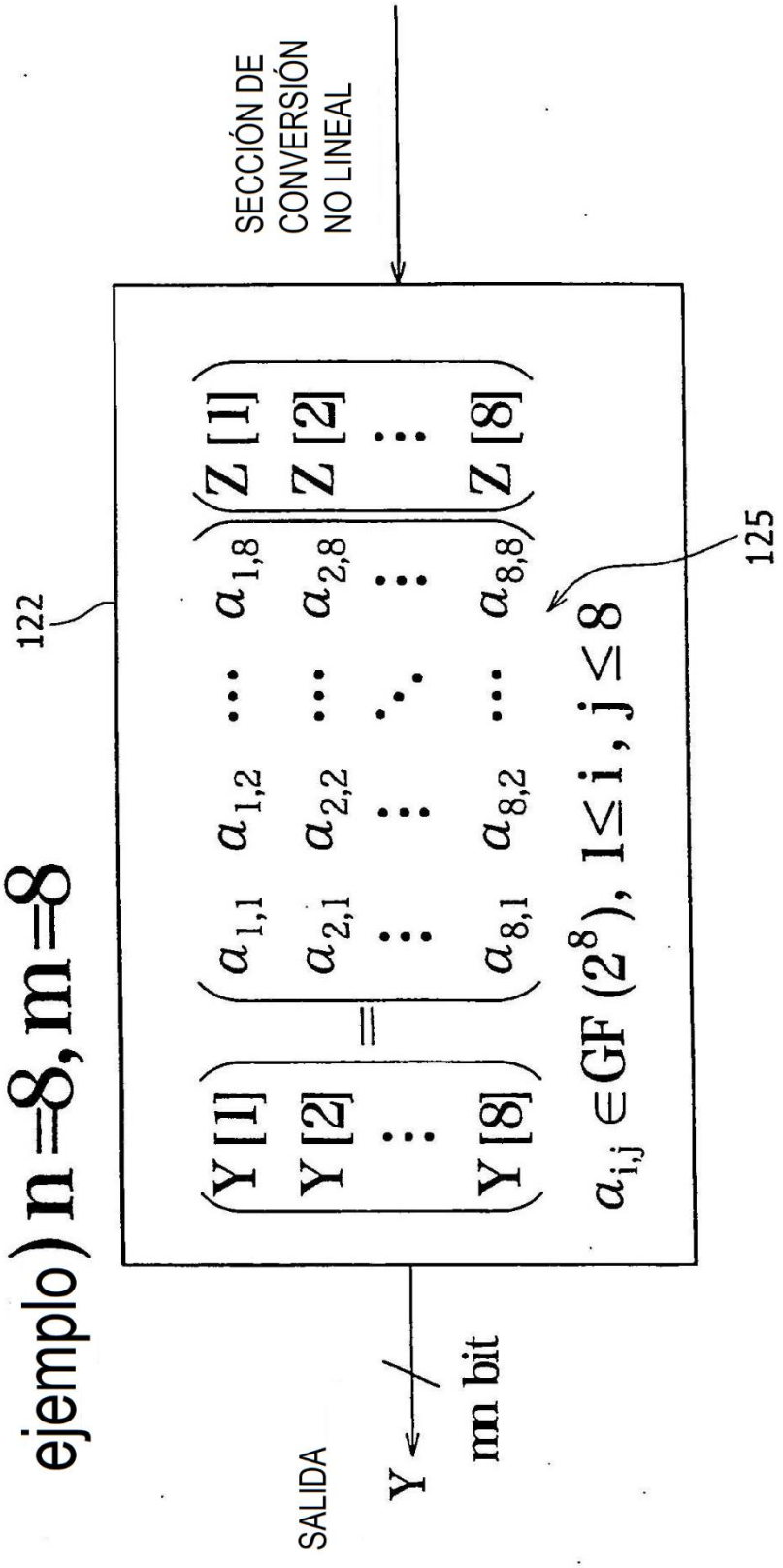

ejemplo) n=8, m=8
122
SECCIÓN DE CONVERSIÓN NO LINEAL
$\begin{pmatrix} Y[1] \\ Y[2] \\ \vdots \\ Y[8] \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,8} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,8} \\ \vdots & \vdots & \ddots & \vdots \\ a_{8,1} & a_{8,2} & \cdots & a_{8,8} \end{pmatrix}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

FIG. 4

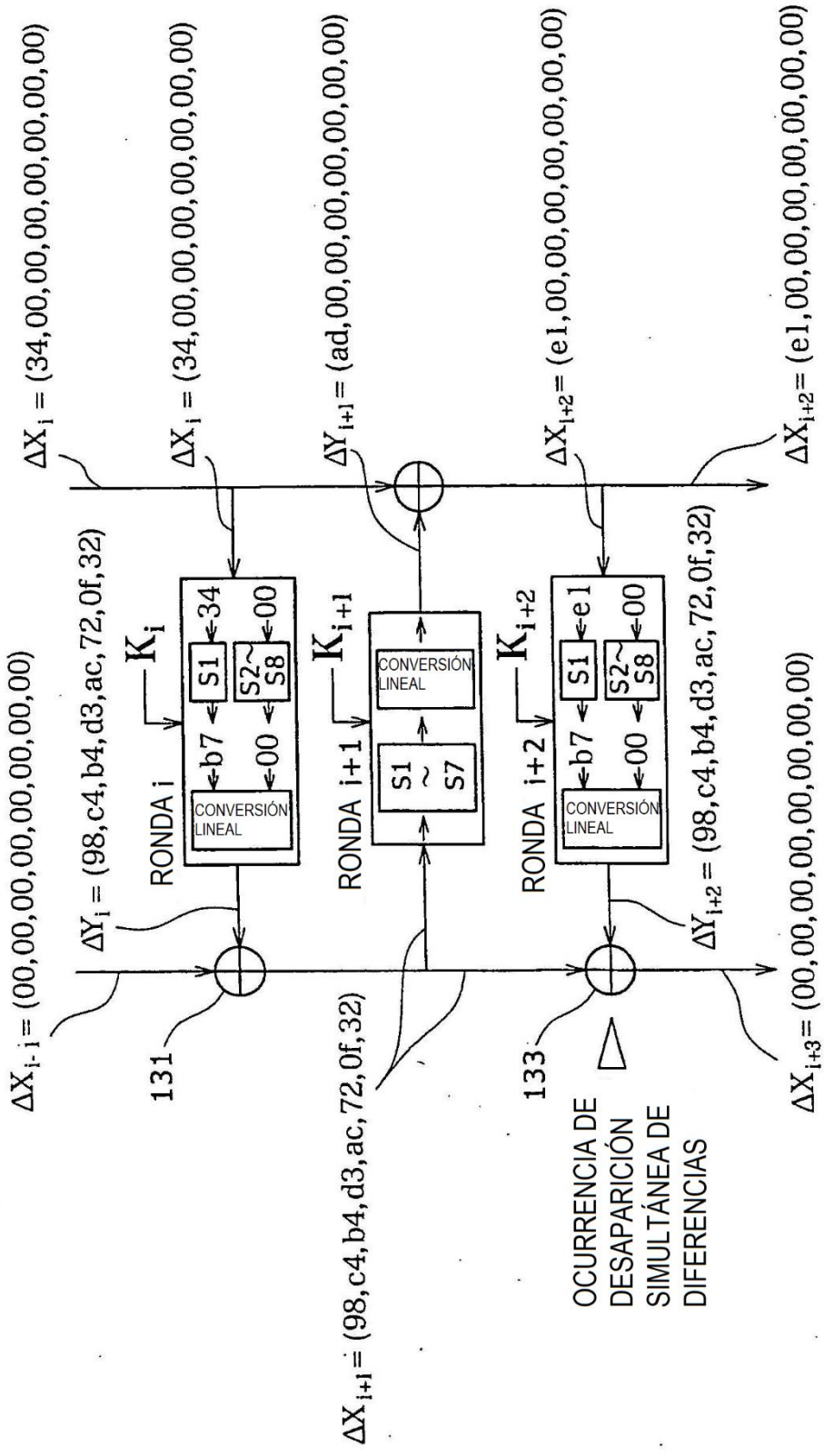

ΔX_i = (34,00,00,00,00,00,00,00)
ΔX_i = (34,00,00,00,00,00,00,00)
ΔY_i+1 = (ad,00,00,00,00,00,00,00)
ΔX_i+2 = (e1,00,00,00,00,00,00,00)
ΔX_i+2 = (e1,00,00,00,00,00,00,00)
ΔX_i-1 = (00,00,00,00,00,00,00,00)
ΔY_i = (98,c4,b4,d3,ac,72,0f,32)
RONDA i
K_i
S1
34
S2~S8
00
b7
00
CONVERSIÓN LINEAL
RONDA i+1
K_i+1
CONVERSIÓN LINEAL
S1 ~ S7
RONDA i+2
K_i+2
e1
S1
S2~S8
00
b7
00
CONVERSIÓN LINEAL
ΔY_i+2 = (98,c4,b4,d3,ac,72,0f,32)
131
133
ΔX_i+1 = (98,c4,b4,d3,ac,72,0f,32)
ΔX_i+3 = (00,00,00,00,00,00,00,00)
OCURRENCIA DE DESAPARICIÓN SIMULTÁNEA DE DIFERENCIAS

FIG. 5

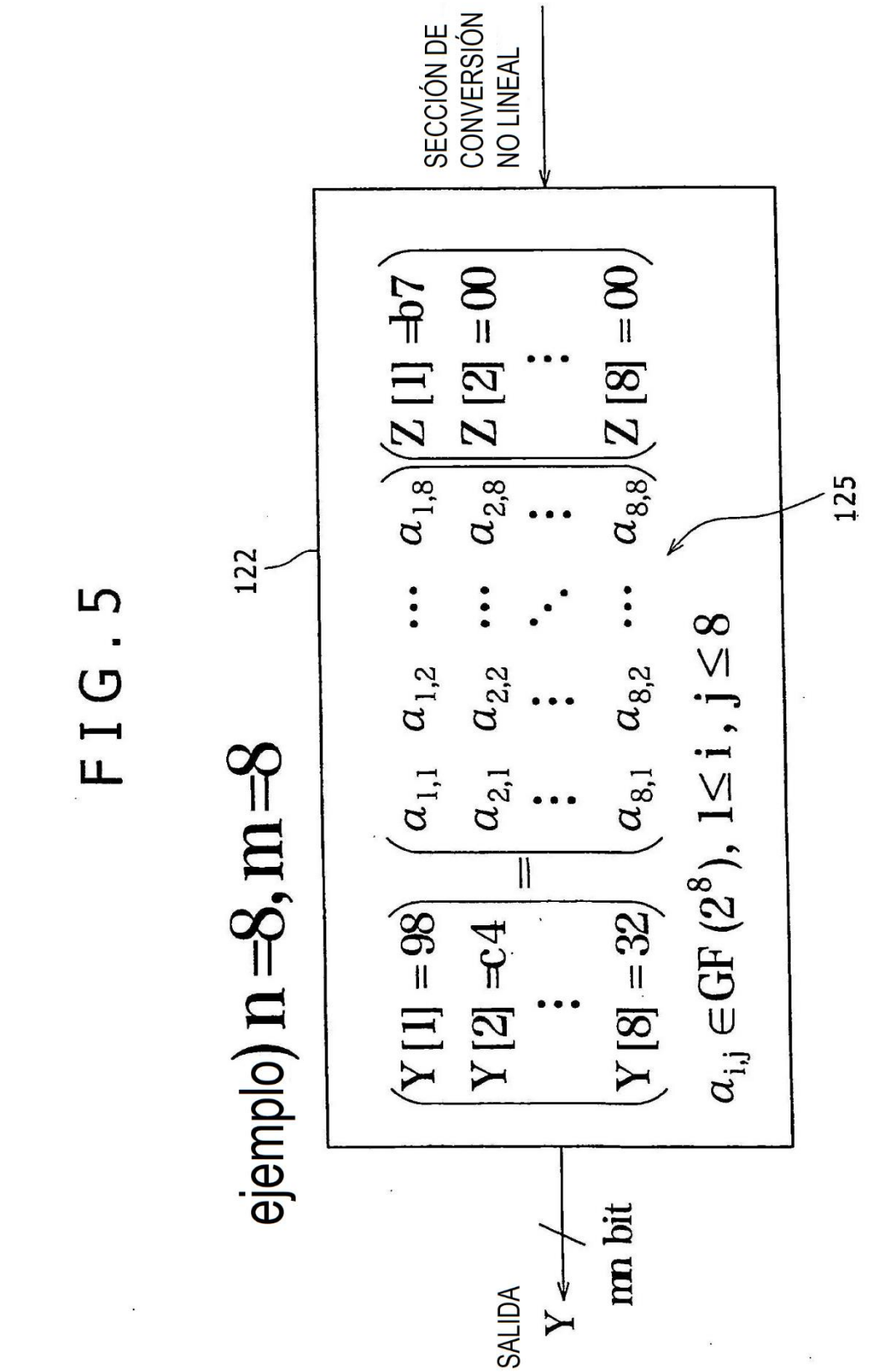

ejemplo) n=8, m=8
122
SECCIÓN DE CONVERSIÓN NO LINEAL
125
SALIDA
Y
m bit

FIG. 6

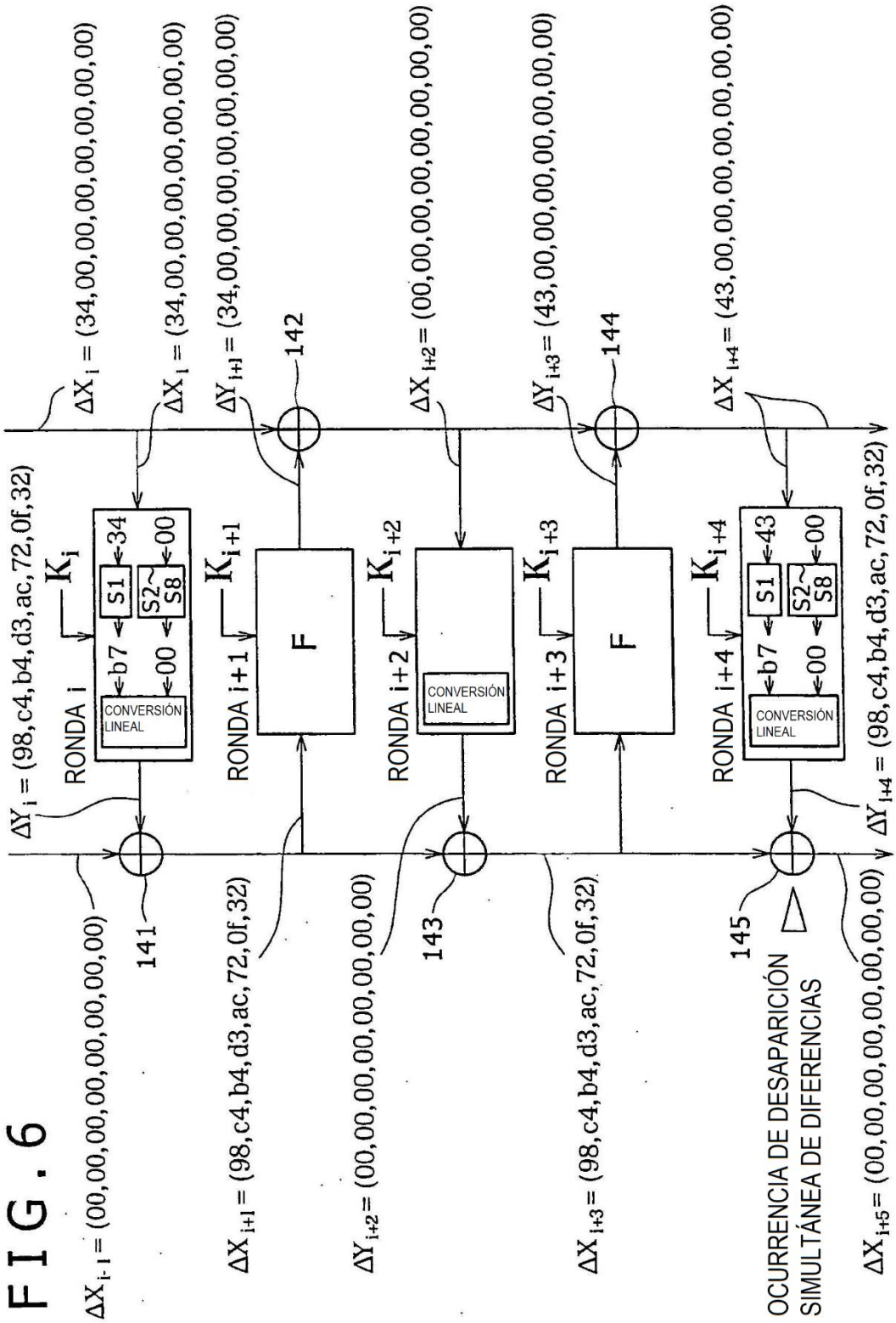

ΔX i-1 = (00,00,00,00,00,00,00,00)
ΔY i = (98,c4,b4,d3,ac,72,0f,32)
ΔX i = (34,00,00,00,00,00,00,00)
RONDA i
Ki
S1
34
S2~S8
00
b7
00
CONVERSIÓN LINEAL
141
ΔX i+1 = (98,c4,b4,d3,ac,72,0f,32)
ΔY i+1 = (34,00,00,00,00,00,00,00)
142
RONDA i+1
Ki+1
F
ΔY i+2 = (00,00,00,00,00,00,00,00)
ΔX i+2 = (00,00,00,00,00,00,00,00)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

FIG. 7

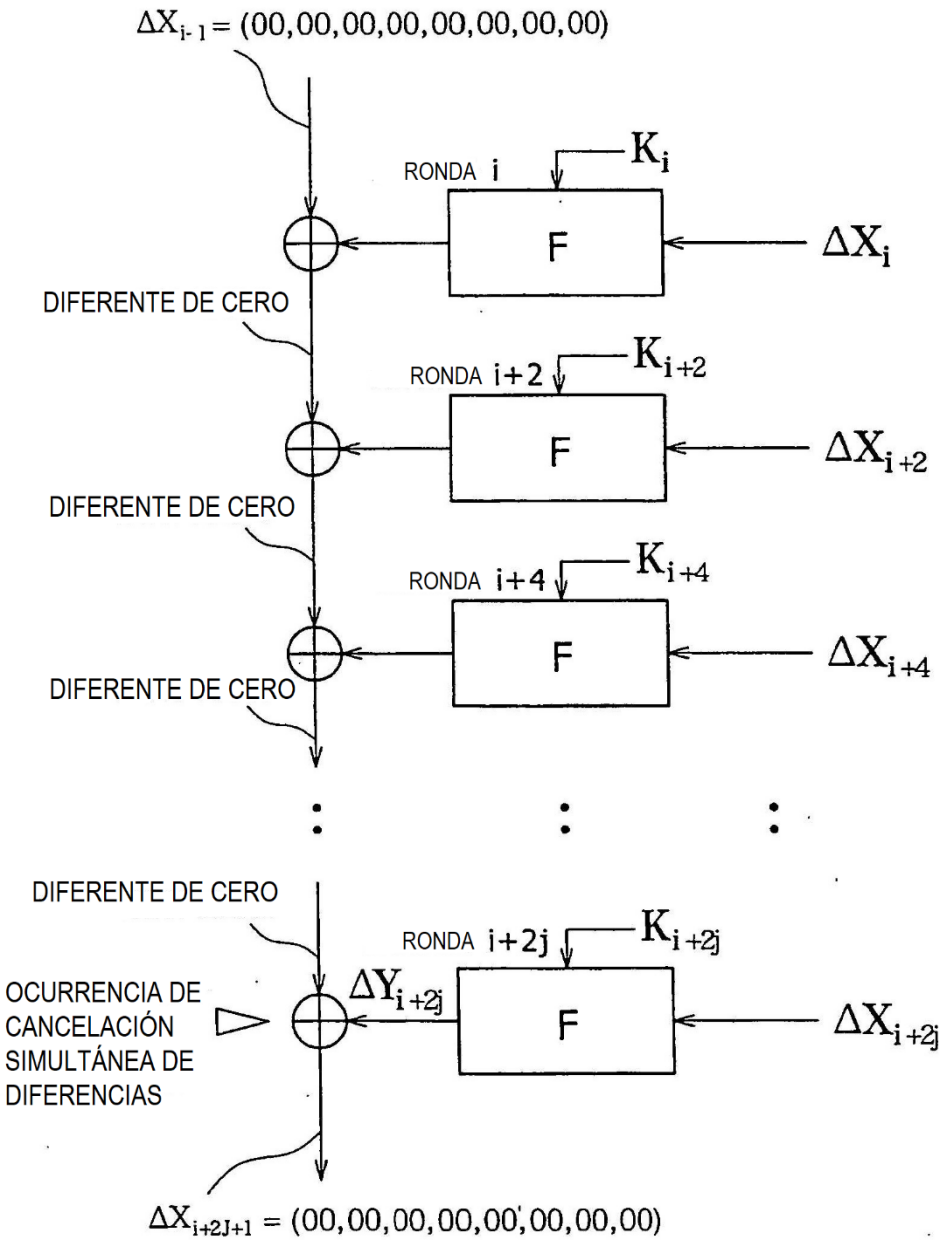

ΔX_{i-1} = (00,00,00,00,00,00,00,00)
RONDA i
K_i
F
ΔX_i
DIFERENTE DE CERO
RONDA i+2
K_{i+2}
F
ΔX_{i+2}
DIFERENTE DE CERO
RONDA i+4
K_{i+4}
F
ΔX_{i+4}
DIFERENTE DE CERO
DIFERENTE DE CERO
RONDA i+2j
K_{i+2j}
OCURRENCIA DE CANCELACIÓN SIMULTÁNEA DE DIFERENCIAS
ΔY_{i+2j}
F
ΔX_{i+2j}
ΔX_{i+2J+1} = (00,00,00,00,00,00,00,00)

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

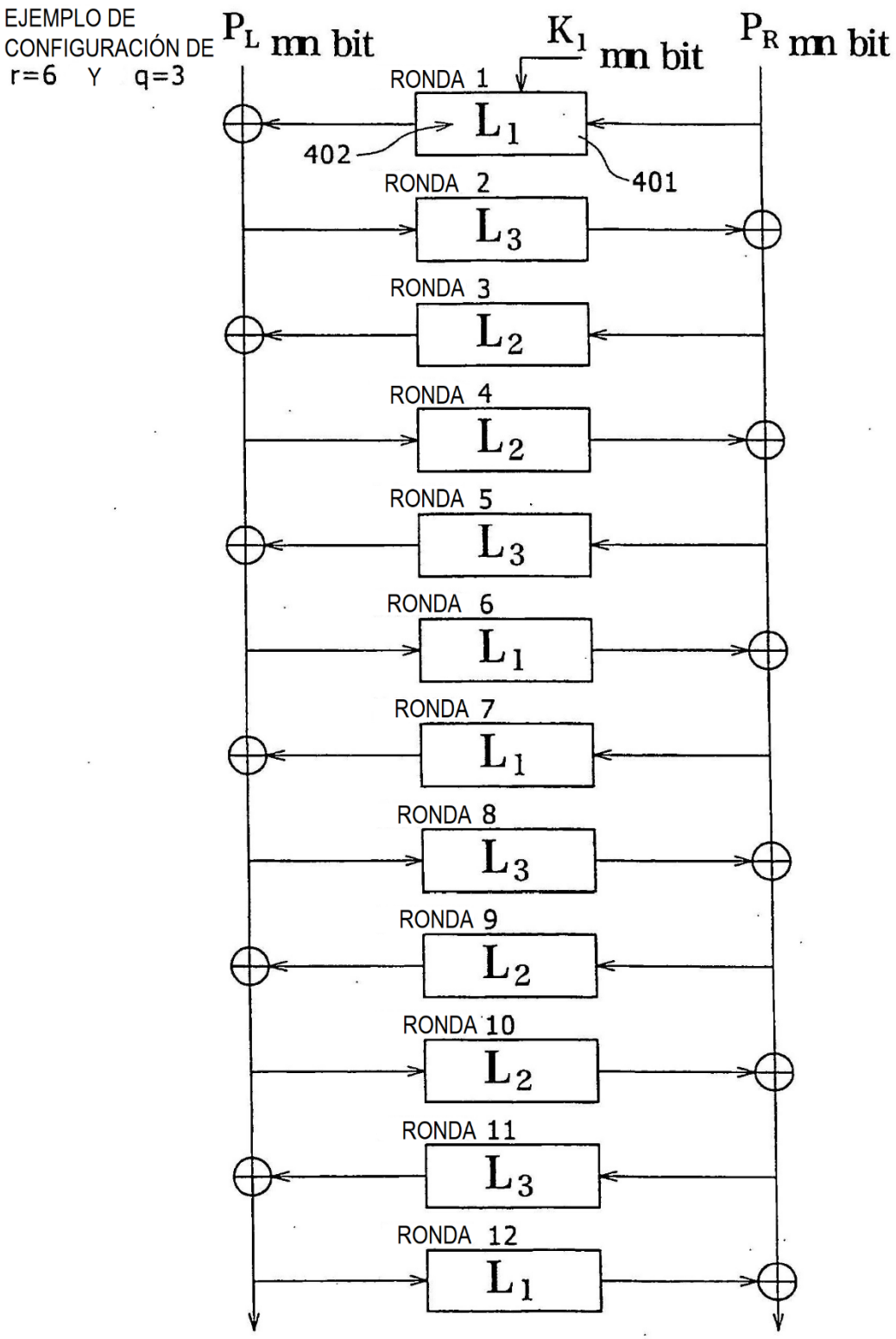

EJEMPLO DE CONFIGURACIÓN DE r=6 Y q=3
P_L mn bit
K_1 mn bit
P_R mn bit
RONDA 1
L_1
402
401
RONDA 2
L_3
RONDA 3
L_2
RONDA 4
L_2
RONDA 5
L_3
RONDA 6
L_1
RONDA 7
L_1
RONDA 8
L_3
RONDA 9
L_2
RONDA 10
L_2
RONDA 11
L_3
RONDA 12
L_1

FIG. 10

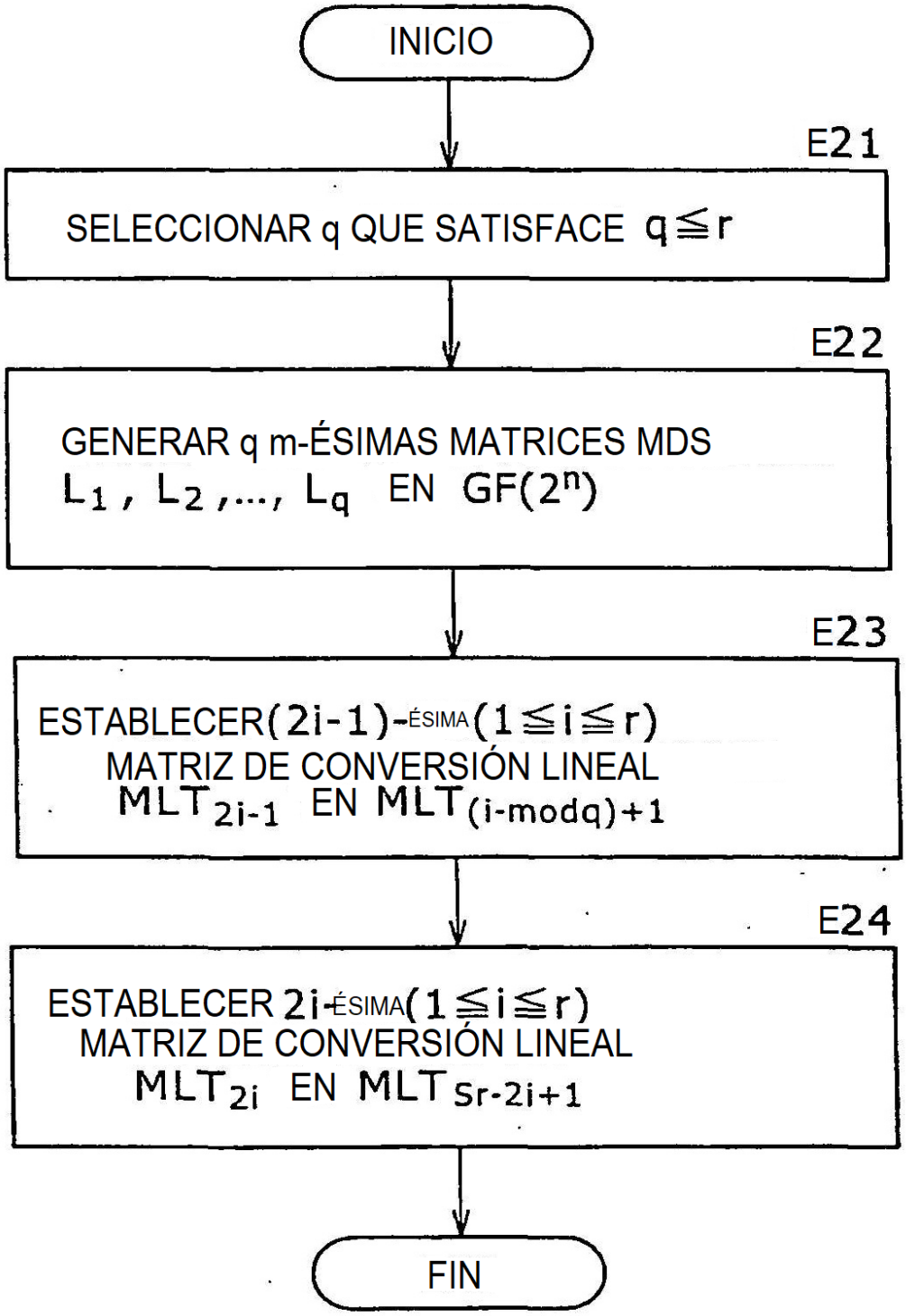

INICIO
E21
SELECCIONAR q QUE SATISFACE $q \leqq r$
E22
GENERAR q m-ÉSIMAS MATRICES MDS
$L_1, L_2, \ldots, L_q$ EN $GF(2^n)$
E23
ESTABLECER (2i-1)-ÉSIMA $(1 \leqq i \leqq r)$
MATRIZ DE CONVERSIÓN LINEAL
MLT_{2i-1} EN $MLT_{(i-modq)+1}$
E24
ESTABLECER 2i-ÉSIMA $(1 \leqq i \leqq r)$
MATRIZ DE CONVERSIÓN LINEAL
MLT_{2i} EN $MLT_{Sr-2i+1}$
FIN

FIG. 11

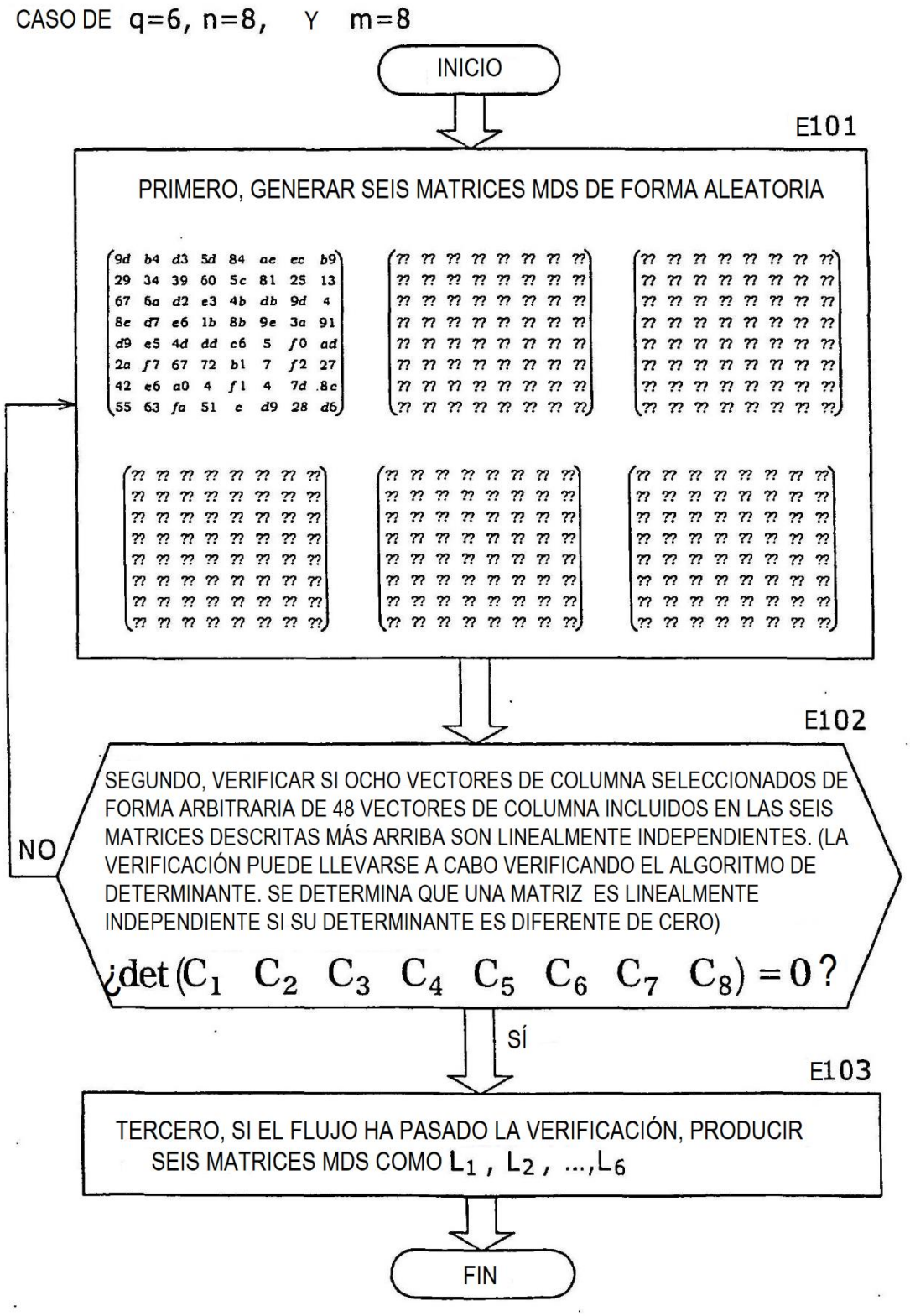

CASO DE q=6, n=8, Y m=8
INICIO
E101
PRIMERO, GENERAR SEIS MATRICES MDS DE FORMA ALEATORIA
9d b4 d3 5d 84 ae ec b9
29 34 39 60 5c 81 25 13
67 6a d2 e3 4b db 9d 4
8e d7 e6 1b 8b 9e 3a 91
d9 e5 4d dd c6 5 f0 ad
2a f7 67 72 b1 7 f2 27
42 e6 a0 4 f1 4 7d 8c
55 63 fa 51 c d9 28 d6
E102
SEGUNDO, VERIFICAR SI OCHO VECTORES DE COLUMNA SELECCIONADOS DE FORMA ARBITRARIA DE 48 VECTORES DE COLUMNA INCLUIDOS EN LAS SEIS MATRICES DESCRITAS MÁS ARRIBA SON LINEALMENTE INDEPENDIENTES. (LA VERIFICACIÓN PUEDE LLEVARSE A CABO VERIFICANDO EL ALGORITMO DE DETERMINANTE. SE DETERMINA QUE UNA MATRIZ ES LINEALMENTE INDEPENDIENTE SI SU DETERMINANTE ES DIFERENTE DE CERO)
NO
¿det (C1 C2 C3 C4 C5 C6 C7 C8) = 0?
SÍ
E103
TERCERO, SI EL FLUJO HA PASADO LA VERIFICACIÓN, PRODUCIR SEIS MATRICES MDS COMO L1 , L2 , ...,L6
FIN

FIG. 12

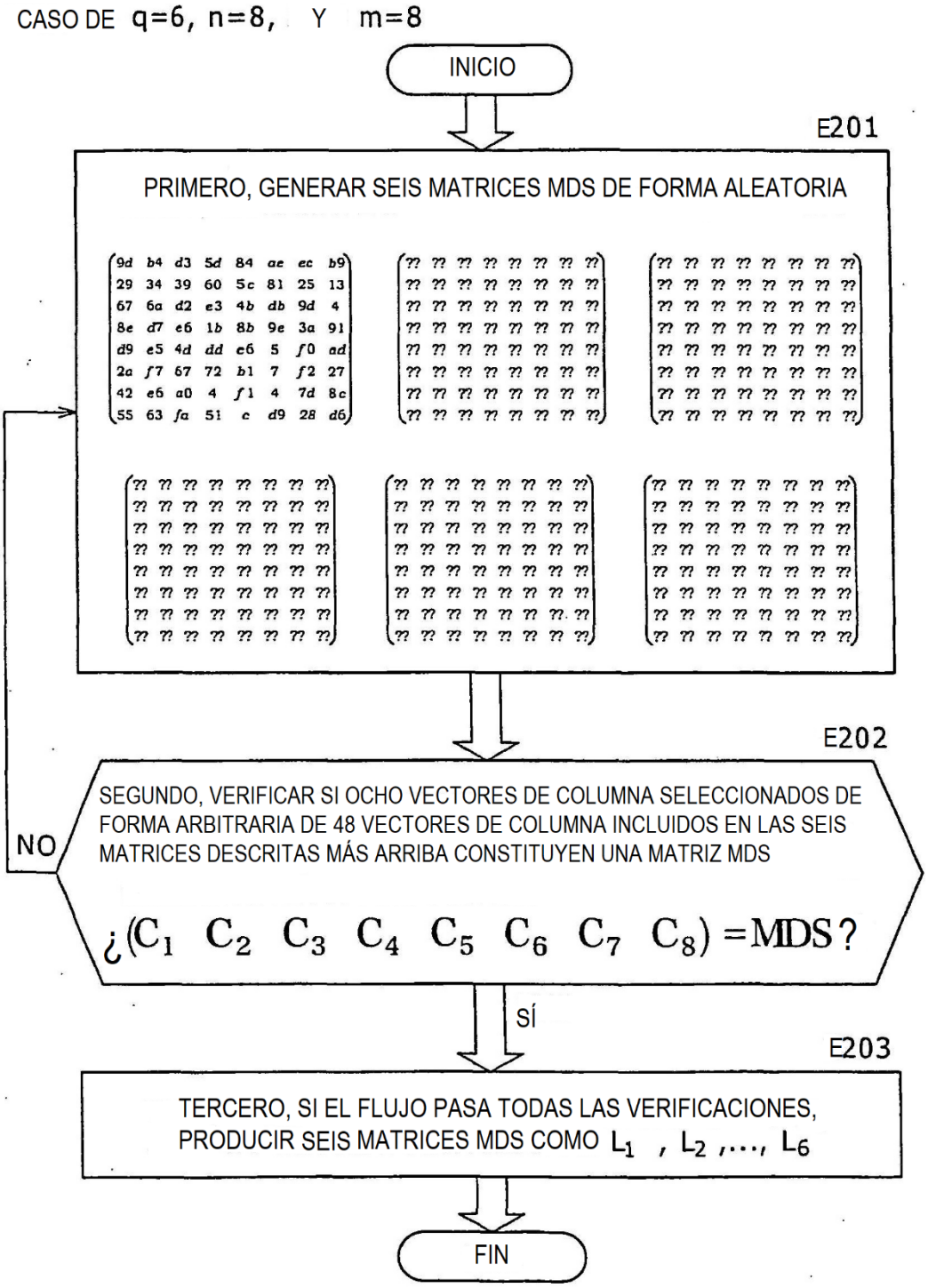

CASO DE q=6, n=8, Y m=8
INICIO
E201
PRIMERO, GENERAR SEIS MATRICES MDS DE FORMA ALEATORIA
9d b4 d3 5d 84 ae ec b9
29 34 39 60 5c 81 25 13
67 6a d2 e3 4b db 9d 4
8e d7 e6 1b 8b 9e 3a 91
d9 e5 4d dd e6 5 f0 ad
2a f7 67 72 b1 7 f2 27
42 e6 a0 4 f1 4 7d 8c
55 63 fa 51 c d9 28 d6
E202
SEGUNDO, VERIFICAR SI OCHO VECTORES DE COLUMNA SELECCIONADOS DE FORMA ARBITRARIA DE 48 VECTORES DE COLUMNA INCLUIDOS EN LAS SEIS MATRICES DESCRITAS MÁS ARRIBA CONSTITUYEN UNA MATRIZ MDS
¿(C1 C2 C3 C4 C5 C6 C7 C8) =MDS?
NO
SÍ
E203
TERCERO, SI EL FLUJO PASA TODAS LAS VERIFICACIONES, PRODUCIR SEIS MATRICES MDS COMO L1 , L2 ,..., L6
FIN

FIG. 13

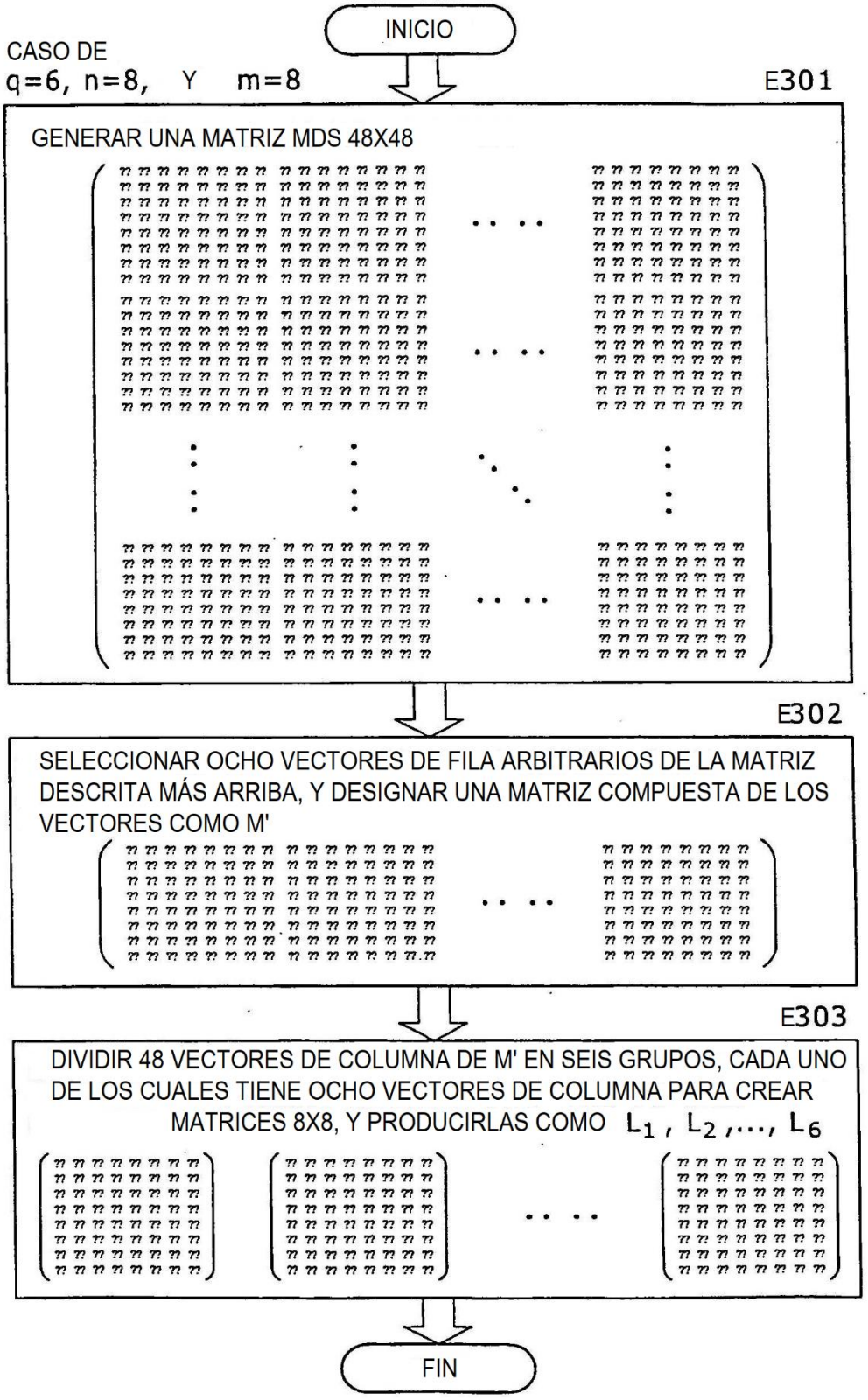

INICIO
CASO DE
q=6, n=8, Y m=8
E301
GENERAR UNA MATRIZ MDS 48X48
E302
SELECCIONAR OCHO VECTORES DE FILA ARBITRARIOS DE LA MATRIZ DESCRITA MÁS ARRIBA, Y DESIGNAR UNA MATRIZ COMPUESTA DE LOS VECTORES COMO M'
E303
DIVIDIR 48 VECTORES DE COLUMNA DE M' EN SEIS GRUPOS, CADA UNO DE LOS CUALES TIENE OCHO VECTORES DE COLUMNA PARA CREAR MATRICES 8X8, Y PRODUCIRLAS COMO L1 , L2 ,..., L6
FIN

FIG. 14

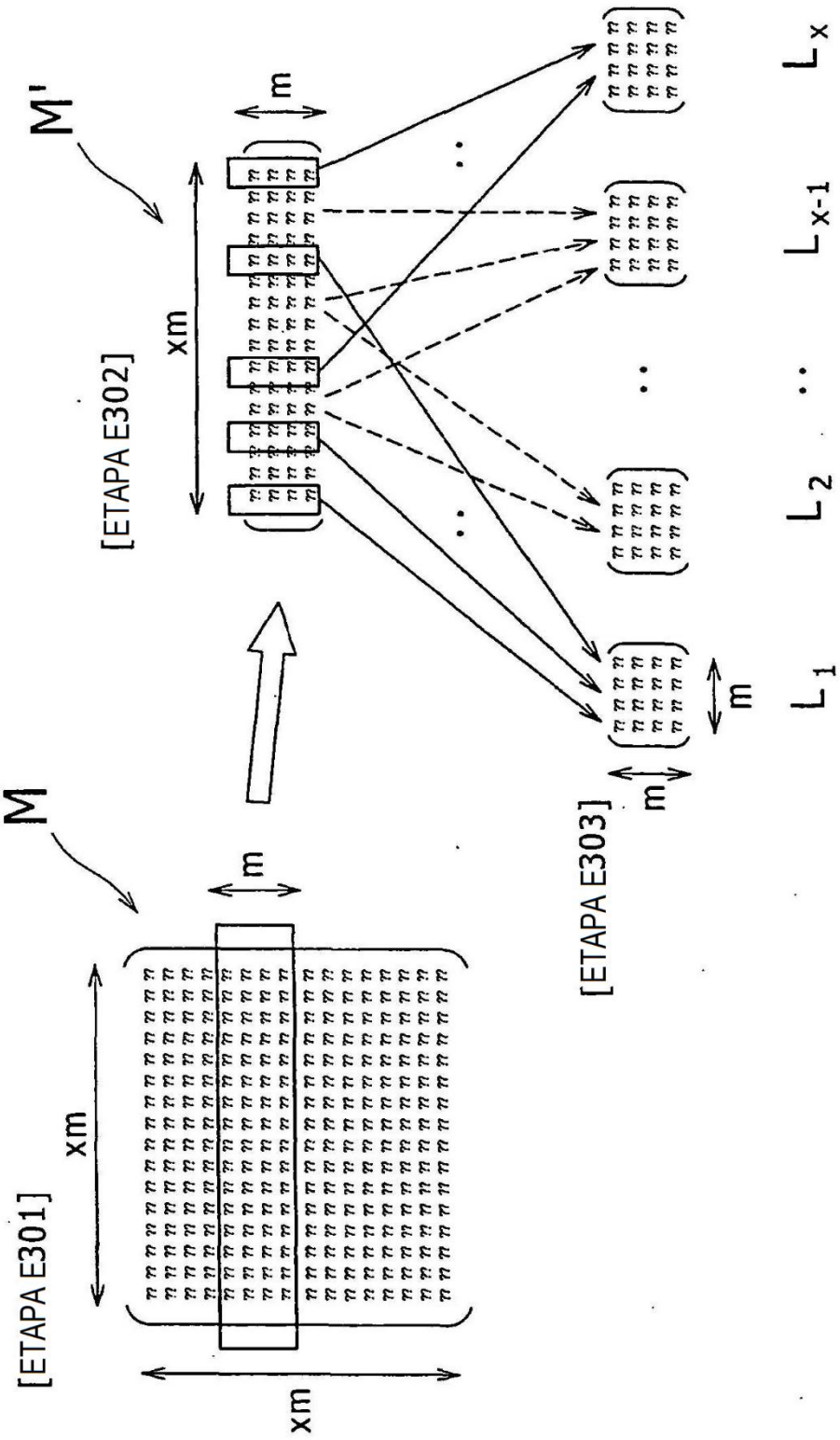


FIG. 15

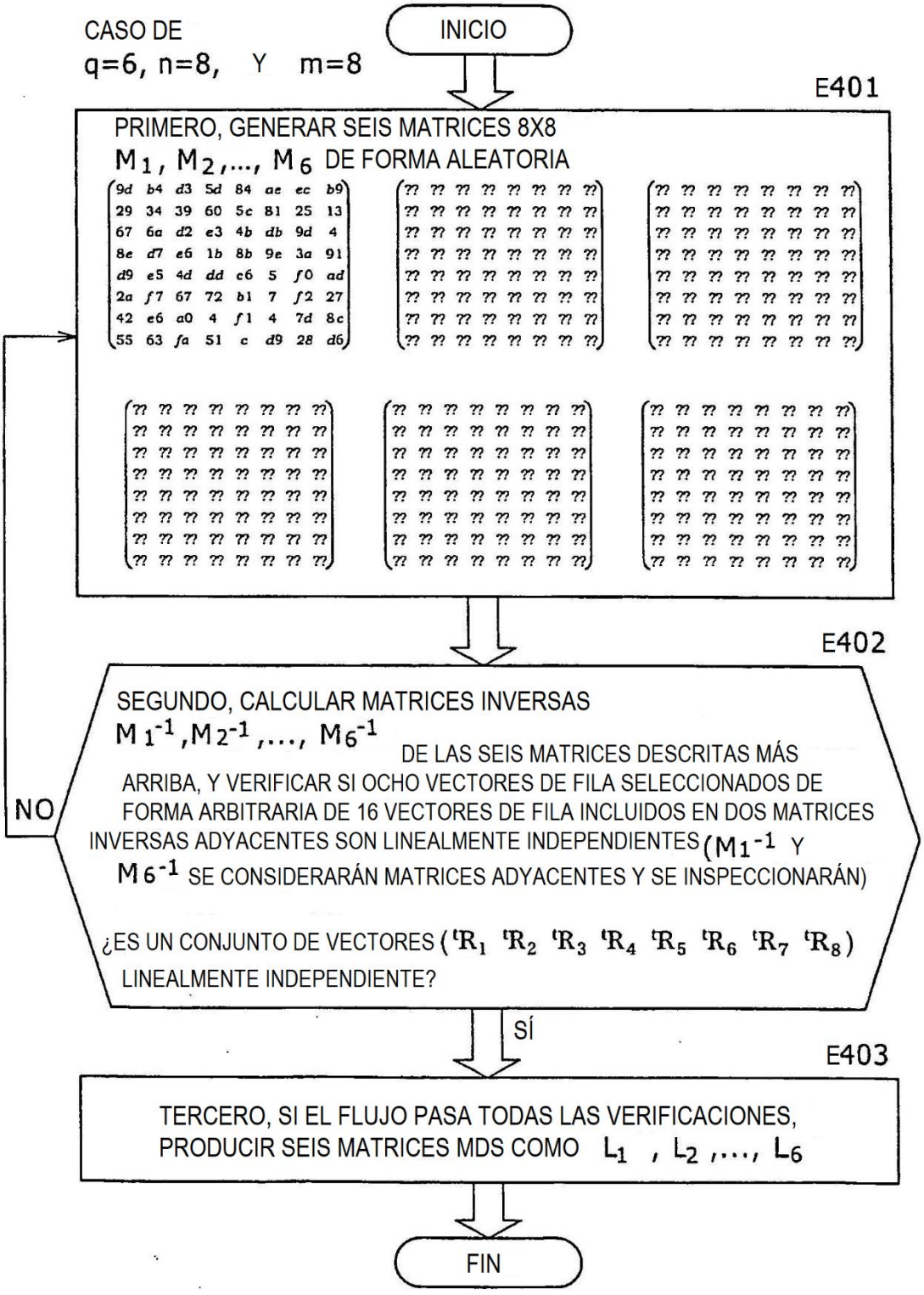

CASO DE
q=6, n=8, Y m=8
INICIO
E401
PRIMERO, GENERAR SEIS MATRICES 8X8
M1, M2,..., M6 DE FORMA ALEATORIA
9d b4 d3 5d 84 ae ec b9
29 34 39 60 5c 81 25 13
67 6a d2 e3 4b db 9d 4
8e d7 e6 1b 8b 9e 3a 91
d9 e5 4d dd c6 5 f0 ad
2a f7 67 72 b1 7 f2 27
42 e6 a0 4 f1 4 7d 8c
55 63 fa 51 c d9 28 d6
E402
SEGUNDO, CALCULAR MATRICES INVERSAS
M1-1, M2-1,..., M6-1
DE LAS SEIS MATRICES DESCRITAS MÁS ARRIBA, Y VERIFICAR SI OCHO VECTORES DE FILA SELECCIONADOS DE FORMA ARBITRARIA DE 16 VECTORES DE FILA INCLUIDOS EN DOS MATRICES INVERSAS ADYACENTES SON LINEALMENTE INDEPENDIENTES (M1-1 Y M6-1 SE CONSIDERARÁN MATRICES ADYACENTES Y SE INSPECCIONARÁN)
¿ES UN CONJUNTO DE VECTORES (tR1 tR2 tR3 tR4 tR5 tR6 tR7 tR8) LINEALMENTE INDEPENDIENTE?
NO
SÍ
E403
TERCERO, SI EL FLUJO PASA TODAS LAS VERIFICACIONES, PRODUCIR SEIS MATRICES MDS COMO L1 , L2 ,..., L6
FIN

FIG. 16

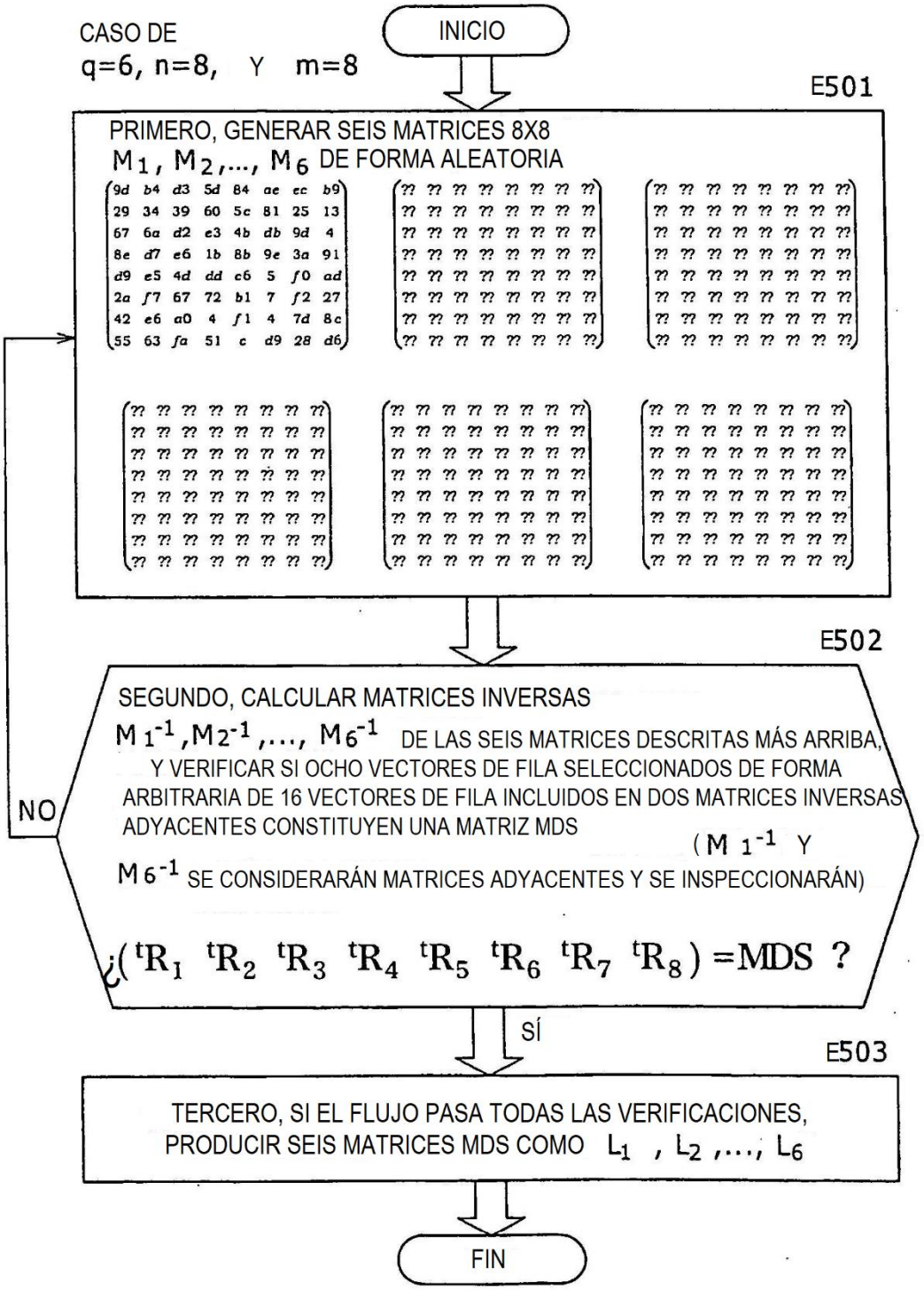

CASO DE
q=6, n=8, Y m=8
INICIO
E501
PRIMERO, GENERAR SEIS MATRICES 8X8
M1, M2,..., M6 DE FORMA ALEATORIA
9d b4 d3 5d 84 ae ec b9
29 34 39 60 5c 81 25 13
67 6a d2 e3 4b db 9d 4
8e d7 e6 1b 8b 9e 3a 91
d9 e5 4d dd c6 5 f0 ad
2a f7 67 72 b1 7 f2 27
42 e6 a0 4 f1 4 7d 8c
55 63 fa 51 c d9 28 d6
E502
SEGUNDO, CALCULAR MATRICES INVERSAS
M1-1, M2-1, ..., M6-1 DE LAS SEIS MATRICES DESCRITAS MÁS ARRIBA,
Y VERIFICAR SI OCHO VECTORES DE FILA SELECCIONADOS DE FORMA
ARBITRARIA DE 16 VECTORES DE FILA INCLUIDOS EN DOS MATRICES INVERSAS
ADYACENTES CONSTITUYEN UNA MATRIZ MDS
(M1-1 Y
M6-1 SE CONSIDERARÁN MATRICES ADYACENTES Y SE INSPECCIONARÁN)
¿(tR1 tR2 tR3 tR4 tR5 tR6 tR7 tR8) =MDS ?
NO
SÍ
E503
TERCERO, SI EL FLUJO PASA TODAS LAS VERIFICACIONES,
PRODUCIR SEIS MATRICES MDS COMO L1 , L2 ,..., L6
FIN

FIG. 17

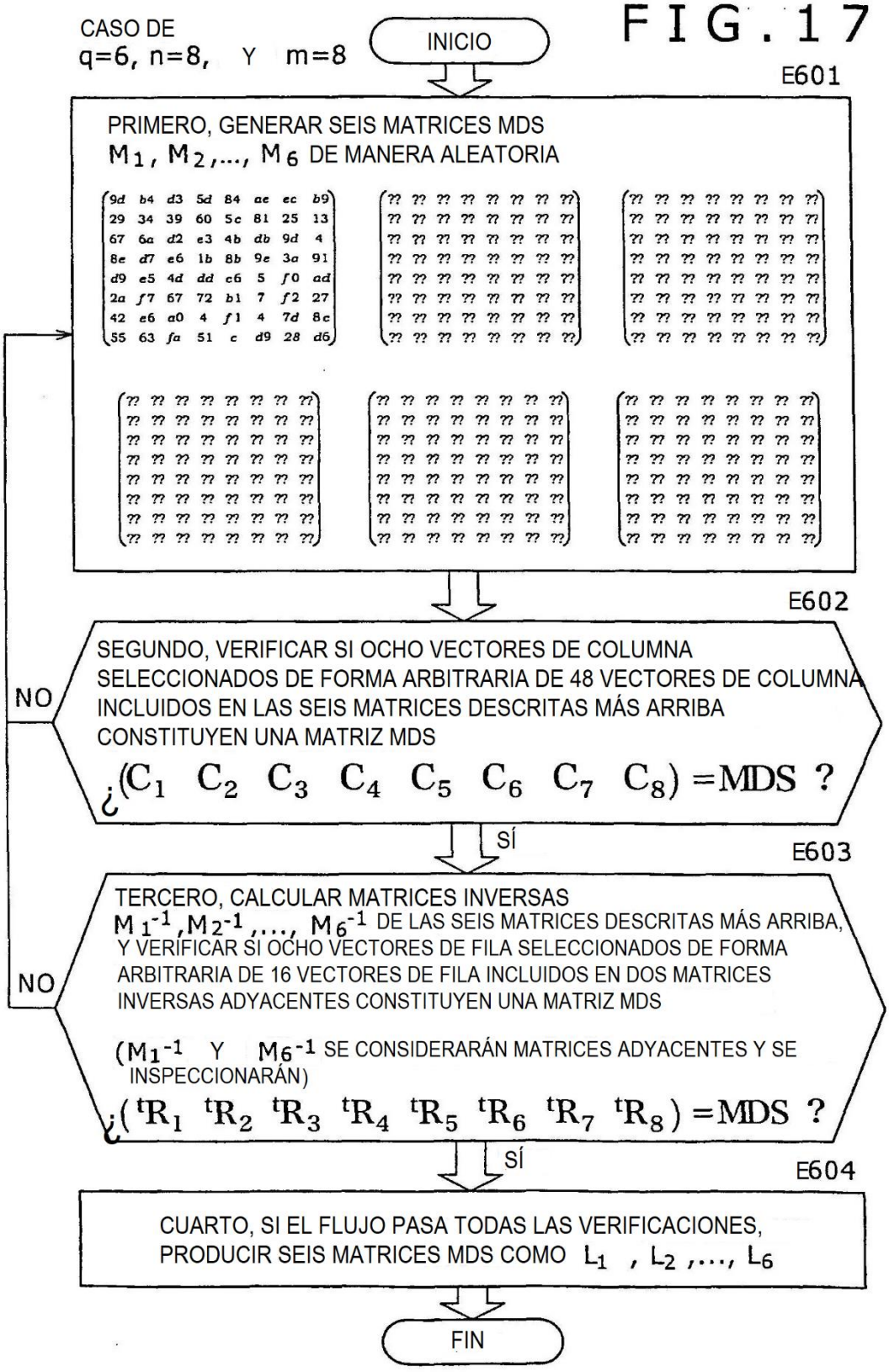
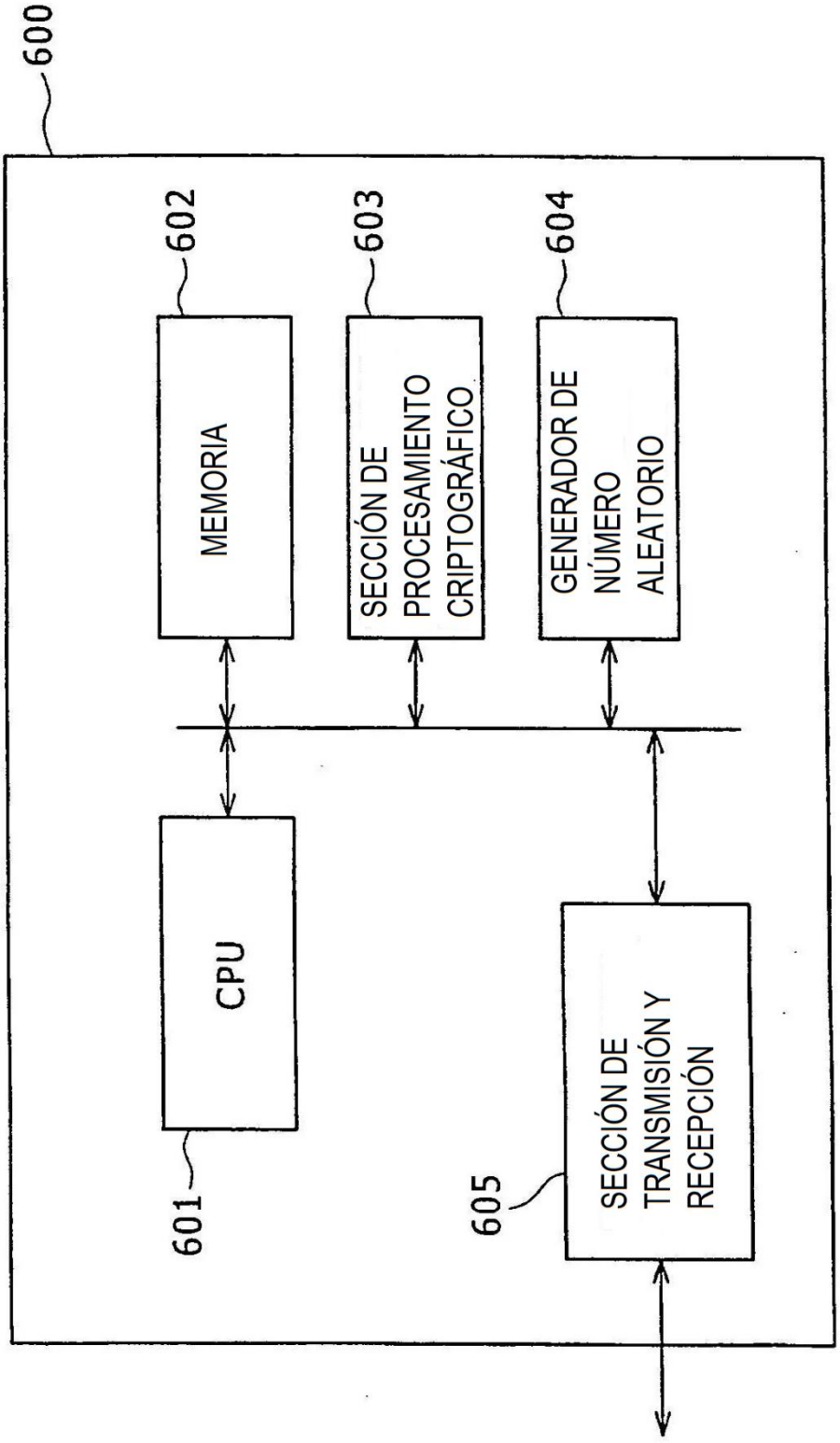

CASO DE
q=6, n=8, Y m=8
INICIO
E601
PRIMERO, GENERAR SEIS MATRICES MDS
M1, M2,..., M6 DE MANERA ALEATORIA
E602
SEGUNDO, VERIFICAR SI OCHO VECTORES DE COLUMNA SELECCIONADOS DE FORMA ARBITRARIA DE 48 VECTORES DE COLUMNA INCLUIDOS EN LAS SEIS MATRICES DESCRITAS MÁS ARRIBA CONSTITUYEN UNA MATRIZ MDS
¿(C1 C2 C3 C4 C5 C6 C7 C8) =MDS ?
NO
SÍ
E603
TERCERO, CALCULAR MATRICES INVERSAS
M1-1, M2-1 ,..., M6-1 DE LAS SEIS MATRICES DESCRITAS MÁS ARRIBA, Y VERIFICAR SI OCHO VECTORES DE FILA SELECCIONADOS DE FORMA ARBITRARIA DE 16 VECTORES DE FILA INCLUIDOS EN DOS MATRICES INVERSAS ADYACENTES CONSTITUYEN UNA MATRIZ MDS
(M1-1 Y M6-1 SE CONSIDERARÁN MATRICES ADYACENTES Y SE INSPECCIONARÁN)
¿(tR1 tR2 tR3 tR4 tR5 tR6 tR7 tR8) =MDS ?
NO
SÍ
E604
CUARTO, SI EL FLUJO PASA TODAS LAS VERIFICACIONES, PRODUCIR SEIS MATRICES MDS COMO L1 , L2 ,..., L6
FIN

FIG.18


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