(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 511 615**

(51) Int. CI.:

H04L 9/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **08.07.2005 E 05788664 (0)**

(97) Fecha y número de publicación de la concesión europea: **12.02.2014 EP 1769603**

(54) Título: **Procedimiento y dispositivo de ejecución de un cálculo criptográfico**

(30) Prioridad:

22.07.2004 FR 0408139

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.10.2014

(73) Titular/es:

MORPHO (100.0%)
11 Boulevard Galliéni
92130 Issy Les Moulineaux, FR

(72) Inventor/es:

PELLETIER, HERVÉ

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento y dispositivo de ejecución de un cálculo criptográfico

El presente invento se refiere al dominio de la criptografía y más particularmente a la protección de la confidencialidad de las claves utilizadas por algoritmos criptográficos.

Los algoritmos criptográficos tienen por objeto cifrar datos. Tales algoritmos comprenden generalmente un encadenamiento de varias operaciones, o cálculos, que se aplican sucesivamente sobre un dato a cifrar con el fin de obtener un dato cifrado. Estos algoritmos utilizan claves secretas.

Tales algoritmos criptográficos pueden sufrir "ataques" que pretenden violar la confidencialidad de claves utilizadas. Hoy en día se conocen numerosos tipos de ataques.

Así, ciertos ataques están fundados sobre fugas de información detectadas durante la ejecución del algoritmo de cifrado. Están generalmente basados en una correlación entre las fugas de informaciones detectadas durante el tratamiento por el algoritmo de cifrado del dato y de la clave o de las claves secretas utilizadas. Se conocen así ataques de DPA, acrónimo de "Análisis de Potencia Diferencial" ("Differential Power Analysis" en ingles). Estos últimos requieren en general un conocimiento de los datos de salida cifrados. Se conocen igualmente ataques de SPA, acrónimo de "Análisis Simple de Potencia" ("Simple Power Analysis" en ingles) basados en un análisis de un simple gráfico de consumo de potencia como se ha descrito en el documento "Analizar de manera inteligente la simplicidad y la potencia de análisis simple de potencia en Tarjetas Inteligentes", Rita Mayer-Sommer división de ingeniería eléctrica ETH Zürich, 2000.

Un algoritmo criptográfico comprende de manera general varias operaciones lineales y/o no lineales. Para un dato inicial a cifrar, se obtiene un dato intermedio en curso de cifrado después de cada una de las operaciones del algoritmo.

Así, un algoritmo de tipo DES, acrónimo de "Norma de Cifrado de Datos" ("Data Encryption Standard" en ingles) o aún el algoritmo AES, acrónimo de "Norma de Cifrado Avanzada" ("Advanced Encryption Standard" en ingles) comprende operaciones no lineales. Los ataques de DPA y SPA se revelan como particularmente pertinentes contra el algoritmo de AES durante la ejecución de las operaciones no lineales.

Se han propuesto ya varios procedimientos de protección de algoritmos criptográficos de este tipo, en particular por enmascaramiento de los datos en curso de cifrado manipulados en el algoritmo de AES. Las operaciones no lineales son generalmente implementadas en forma de tablas de sustitución. Así, una operación no lineal correspondiente a una tabla de sustitución tab[i], aplicada a un dato x puede escribirse en la forma siguiente:

$$y = tab[x].$$

A veces es complejo enmascarar un dato en el curso de una operación no lineal con una máscara de valor aleatorio.

El documento FR 2 831 739 A describe un procedimiento de protección de un cálculo de cifrado según el algoritmo DES contra ataques de DPA o SPA. Este documento propone añadir a la operación realizada con la clave secreta una o varias operaciones realizadas con claves ficticias. Las claves pueden ser diferentes o idénticas entre sí.

El documento DE 102 23 175 A describe un procedimiento similar proponiendo una sola clave ficticia.

El presente invento pretende proponer un método fácil de implementar para proteger eficazmente ejecuciones de cálculos de los algoritmos criptográficos basados en al menos una clave secreta contra ataques de DPA o aún de SPA.

Un primer aspecto del invento propone un procedimiento de ejecución de un cálculo criptográfico en un componente electrónico, según un algoritmo criptográfico determinado que incluye al menos una operación con clave secreta a realizar con una clave criptográfica secreta que comprende m bloques de clave criptográfica secreta de n bits sobre un bloque de datos, donde m y n son números enteros positivos. El procedimiento comprende, para un bloque de clave criptográfica secreta dado, las etapas siguientes consistentes en:

- determinar 2^n-1 claves secretas secundarias diferentes sobre n bits, siendo cada una diferente de dicho bloque de clave criptográfica secreta;
- realizar dicha operación con clave secreta con dicho bloque de clave criptográfica secreta y con dichas claves secretas secundarias sobre un bloque de datos y obtener respectivamente un bloque de datos en curso de

cifrado y 2^n-1 bloques de datos secundarios;

- realizar dicha operación no lineal sobre dicho bloque de datos en curso de cifrado y sobre dichos bloques de datos secundarios;

- proporcionar un bloque de datos cifrado a partir del bloque de datos en curso de cifrado.

Se señala que las clave secretas secundarias son claves ficticias.

Gracias a estas disposiciones, se generan, además de las fugas de información unidas a los cálculos criptográficos ejecutados sobre un bloque de datos en curso de cifrado, fugas de información unidas a los cálculos criptográficos ejecutados sobre un bloque de datos secundarios. Un análisis de tales fugas de información es por este hecho más complejo y requiere por tanto más tiempo que el análisis de fugas de información durante la ejecución de cálculos criptográficos sobre el bloque de datos en curso de cifrado únicamente. Se protege así la confidencialidad de las claves criptográficas secretas. La complejidad de un ataque de tal algoritmo aumenta con el número de veces en que se realiza la operación 102 con clave secreta con una clave secreta secundaria ficticia.

Tal procedimiento pretende hacer aparecer los sesgos de correlación para hacer los ataques de SPA o DPA más largos o sea imposibles.

Así, en un modo de realización del presente invento, a fin de garantizar una mejor confidencialidad del algoritmo, para un bloque de clave criptográfica secreta, se determinan todos los valores posibles de claves en n bits, es decir 2^n valores, o aún 2^n -1 claves secretas secundarias ficticias en n bits diferentes del bloque de clave criptográfica secreta. Luego, se realizan la operación con clave secreta con la clave criptográfica secreta e igualmente todas estas claves secretas secundarias determinadas. Se obtiene entonces un bloque de datos en curso de cifrado y 2^n -1 bloques de datos secundarios sobre los que se realiza la operación no lineal. En este caso, las claves criptográficas secretas no son detectables.

En un modo de realización del invento, el procedimiento comprende, para un bloque de clave criptográfica secreta, las etapas que consisten en:

- determinar y disponer aleatoriamente las claves secretas secundarias en una tabla inicial que comprende dicho bloque de clave criptográfica secreta;

- almacenar en memoria la dirección correspondiente a dicho bloque de clave criptográfica secreta en la tabla inicial;

- aplicar la operación con clave secreta al bloque de datos con las claves de la tabla inicial y obtener una primera tabla transformada de 2^n primeros elementos, correspondiendo cada primer elemento al resultado de la operación con clave secreta aplicada al bloque de datos con la clave situada en la tabla inicial en la misma dirección que dicho primer elemento;

- aplicar dicha operación no lineal a los elementos de dicha primera tabla transformada y obtener una segunda tabla transformada de 2^n segundos elementos, correspondiendo cada segundo elemento al resultado de la operación no lineal aplicada al primer elemento situado en la misma dirección en la primera tabla transformada que dicho segundo elemento;

- recuperar, en la segunda tabla transformada, el elemento correspondiente al bloque de datos en curso de cifrado situado en la dirección de dicho bloque de clave criptográfica secreta.

La tabla inicial comprende ventajosamente todos los valores de clave posibles.

Gracias a estas disposiciones, se manipula de manera que tengan la misma probabilidad todas las claves posibles cuando se ejecuta la operación con clave secreta y la operación no lineal. Tal procedimiento garantiza una protección muy grande de la confidencialidad del algoritmo en cuanto a los ataques de DPA y SPA.

Se puede recuperar el elemento correspondiente al bloque de datos en curso de cifrado en la segunda tabla transformada mediante una función SPA resistente tomando como parámetro la dirección del bloque de clave criptográfica secreta dada. Se entiende por "función resistente contra los ataques de tipo SPA" una función para la que no es posible determinar una clave secreta en una sola traza de fuga. Considerando que la señal de fuga W, correspondiente a una corriente, o aún a un campo electromagnético, durante una manipulación de un octeto α para un cálculo del algoritmo, es de la forma siguiente:

$$W(\alpha)=H(\alpha)+b;$$

donde H(α) es el modelo de fuga y b el ruido extrínseco e intrínseco.

Se considera que una función ejecutada sobre el octeto α es una función resistente contra los ataques de SPA cuando se tiene la ecuación siguiente:

$$|W_{\alpha} - W_{\alpha'}| \leq b,$$

donde α' es otro octeto.

Cuando el algoritmo criptográfico comprende un número determinado de vueltas, cada una de las cuales incluye al menos una operación de clave criptográfica secreta que precede a una operación no lineal realizada mediante una tabla de sustitución, se pueden realizar las etapas del procedimiento enunciadas anteriormente para al menos la primera vuelta y al menos la última vuelta del algoritmo criptográfico.

En efecto, las primeras y últimas vueltas del algoritmo AES son las más frágiles frente a los ataques de tipo de SPA y DPA. Así, aplicando el procedimiento según un modo de realización del presente invento a la primera vuelta y a la última vuelta, se protege la confidencialidad del algoritmo limitando al mismo tiempo el número de cálculos a añadir para la protección de este algoritmo.

La etapa de disposición aleatoria de las claves en la tabla puede ser hecha a cada comienzo del algoritmo criptográfico.

Por otra parte, se puede realizar simultáneamente la operación con clave secreta con un bloque de clave criptográfica secreta y con la clave secreta secundaria y/o se puede realizar simultáneamente la operación no lineal sobre el bloque de datos y los bloques de datos secundarios a fin de proporcionar un buen rendimiento en cuanto a la ejecución de los cálculos del algoritmo.

En un modo de realización del presente invento, el algoritmo criptográfico es el AES.

En un modo de realización del presente invento, una al menos de las operaciones del algoritmo criptográfico es realizada sobre el bloque de datos en curso de cifrado enmascarado con un valor aleatorio. De preferencia, las operaciones del algoritmo distintas de las realizadas con las claves secretas secundarias y las realizadas sobre bloques de datos secundarios, son realizadas sobre un bloque de datos en curso de cifrado que está enmascarado.

Otro aspecto del invento propone un componente electrónico adaptado para ejecutar un cálculo criptográfico según un algoritmo criptográfico determinado que incluye al menos una operación con clave secreta a realizar con una clave criptográfica secreta que comprende m bloques de clave secreta de n bits sobre un bloque de datos y una operación no lineal, comprendiendo medios dispuestos para poner en práctica un procedimiento como se ha enunciado anteriormente.

Otros aspectos, propósitos y ventajas del invento aparecerán con la lectura de la descripción de uno de sus modos de realización.

El invento será igualmente mejor comprendido con ayuda de los dibujos, en los que:

La fig. 1 ilustra un procedimiento de cálculo criptográfico según un modo de realización del presente invento;

La fig. 2 ilustra las principales etapas de un algoritmo de tipo AES;

La fig. 3 ilustra una operación con clave secreta según un modo de realización del invento;

La fig. 4 ilustra la ejecución de una operación no lineal según un modo de realización del presente invento;

La fig. 5 ilustra una gestión del paso en la primera vuelta de un algoritmo de tipo AES que comprende cálculos criptográficos ejecutados según un modo de realización del presente invento;

La fig. 6 ilustra una gestión del paso entre dos vueltas consecutivas de un algoritmo de tipo AES que comprende cálculos criptográficos ejecutados según un modo de realización del presente invento.

Generalmente, un algoritmo criptográfico comprende varias operaciones que son aplicadas sucesivamente a un bloque de datos, siendo aplicada cada una al bloque de datos transformado por la operación precedente. A la salida del algoritmo, un bloque de datos en curso de cifrado es un bloque de datos cifrado.

La fig. 1 ilustra un procedimiento de ejecución de un cálculo criptográfico según un algoritmo criptográfico, según un modo de realización del presente invento. Tal algoritmo incluye al menos una operación con clave secreta 102 a

realizar con una clave criptográfica secreta 103 sobre un bloque de datos 101 para obtener un bloque de datos en curso de cifrado 104. El algoritmo incluye igualmente una operación no lineal 107 a realizar sobre el bloque de datos en curso de cifrado 104 para obtener otro bloque de datos en curso de cifrado 104. El bloque de datos 101 puede ser el resultado de una operación precedente en el caso en que una o varias operaciones preceden a la operación con clave secreta 102. En el caso en que la operación con clave secreta 102 es la primera operación del algoritmo, puede corresponder al bloque de datos a cifrar 100, recibido a la entrada del algoritmo.

A título de ejemplo, en el caso en que la operación con clave secreta es realizada por una clave criptográfica secreta de 128 bits que comprende 16 bloques de clave criptográfica secreta de un octeto cada una, la operación con clave secreta 102 es realizada 16 veces sobre un bloque de datos de un octeto, una vez con cada uno de los bloques de clave criptográfica secreta. Después de haber determinado un valor de clave secreta secundaria 105 diferente del valor del bloque de clave criptográfica secreta 103 correspondiente, se realiza la operación 102 con la clave secreta secundaria 105 determinada sobre el bloque de datos 101 para obtener un bloque de datos secundario 106. Luego, se aplica sobre este bloque de datos secundario, la operación no lineal 107 para obtener otro bloque de datos secundario 106.

A la salida del algoritmo criptográfico se obtiene un bloque de datos cifrado 108.

El invento cubre todas las implementaciones posibles, es decir los casos en que se realiza la operación con una clave secreta secundaria antes, simultáneamente o después de la operación con los bloques de clave criptográfica secreta.

Dado que las operaciones no lineales son las más frágiles frente a los ataques de tipo DPA o SPA, son protegidas como prioridad. Así cuando el algoritmo criptográfico comprende operaciones lineales después de la operación no lineal 107, es preferible realizar estas operaciones únicamente sobre el bloque de datos en curso de cifrado 104 a fin de limitar el número de cálculos a ejecutar.

El presente invento se ha descrito a continuación en su aplicación no limitativa a un algoritmo de tipo AES más particularmente a un algoritmo AES que manipula claves de 16 octetos.

La fig. 2 ilustra un procedimiento de criptografía según un algoritmo de tipo AES. Tal algoritmo toma como entrada un bloque de datos inicial a cifrar 201 para proporcionar a la salida un bloque de datos cifrado correspondiente 208.

El algoritmo comprende varias vueltas (o "round" en inglés). En general está basado sobre una clave secreta principal K. Una clave principal puede tener un tamaño de 128 bits, de 192 bits o aún de 256 bits. Tal clave es derivada clásicamente en una pluralidad de claves, denominadas K_l. Las claves derivadas tienen un tamaño de 16 octetos para un algoritmo que manipula claves de 128 bits, un tamaño de 24 octetos para un algoritmo que manipula claves de 192 bits y un tamaño de 32 octetos para un algoritmo que manipula claves de 256 bits.

Se considera a título de ejemplo que la clave secreta principal K tiene un tamaño de 128 bits y es derivada en 10 claves de 16 octetos, siendo cada una de estas claves utilizadas en una vuelta específica.

El mensaje inicial a cifrar tiene un tamaño de 128 bits. Se le trata generalmente por bloques de datos iniciales de un octeto 201. A un bloque de datos de un octeto para una vuelta determinada del algoritmo le corresponde un octeto de una clave.

Se representa clásicamente el mensaje a cifrar en forma de una matriz de estado 4×4 de 16 bloques de datos iniciales de 8 bits. Los bloques de datos de 8 bits pueden ser tratados unos después de los otros o aún simultáneamente. El invento cubre todas estas implementaciones.

Este mensaje a cifrar es en primer lugar transformado por una operación 202 de clave criptográfica secreta, clásicamente referenciada 'AddRoundKey'. Esta operación 202 añade al bloque de datos inicial 201 por un o exclusivo la clave exclusiva principal K 203.

La clave secreta principal K 203 es utilizada durante la primera aplicación de la operación 202 para obtener un bloque de datos en curso de cifrado. Luego el bloque de datos entra en una primera vuelta 204. Para una clave de 128 bits, tal algoritmo comprende clásicamente 9 vueltas 204 que comprenden cada una las mismas operaciones sucesivas siguientes:

- una operación 205, clásicamente denominada 'ByteSub'; esta última es una función no lineal generalmente implementada en forma de una tabla de sustitución;
- una operación 206, clásicamente denominada ' ShiftRow'; esta última es una función que opera desfases o

desplazamientos de líneas sobre la matriz de estado;

- una operación 207, clásicamente denominada 'MixColumn', esta última es una función de interferencia de columnas sobre la matriz de Estado; y

- la operación 202 'AddRoundKey' con la clave K_r correspondiente a la vuelta T_r.

Luego, sobre el bloque de datos en curso de cifrado así obtenido a la salida de las 9 vueltas, se aplica de nuevo la operación 205 'ByteSub', la operación 206 'ShiftRow', y finalmente la operación 202 'AddRoundKey' con la clave K_{10}.

Para cada una de las vueltas T_r, para r igual a 1 a 9, una clave secreta K_r derivada de la clave secreta principal es utilizada para la ejecución de la operación 202 'AddRoundKey'.

Se denomina $K_{l,r}$ al valor del íesimo octeto de la clave en la vuelta T_r del AES, donde i está comprendido entre 1 y L_r, donde r está comprendido entre 1 y N_r con N_r=10 y L_r=16 en el caso en que el algoritmo AES manipula claves de 128 bits, N_r=12 y L_r=24 en el caso en que el algoritmo AES manipula claves de 192 bits y N_r=16 y L_r=32 en el caso en que el algoritmo AES manipula claves de 256 bits.

Se denomina M al mensaje de entrada a cifrar por el algoritmo y Mi, para i igual a 1 a 16, los bloques de datos iniciales de un octeto correspondientes. Así, a cada bloque de datos de un octeto a tratar por el algoritmo, se aplica cada uno de los bloques de clave criptográfica secreta de un objeto de la clave criptográfica secreta.

Se realiza la operación de clave secreta 202 'AddRoundKey' con un bloque de clave criptográfica secreta para obtener un bloque de datos en curso de cifrado e igualmente con las claves secretas secundarias diferentes del bloque de clave criptográfica secreta y diferentes entre sí para obtener un bloque de datos secundario. Cuanto más importante es el número de claves secretas secundarias, más compleja y larga es la confidencialidad de la clave criptográfica secreta a violar.

A este efecto, en un modo de realización preferido, se construye de manera aleatoria una tabla inicial que comprende todos los valores posibles de un octeto. Así, cada tabla comprende en particular el bloque de clave criptográfica secreta a aplicar al bloque de datos por la operación 'AddRoundKey' 202.

Tal tabla de claves comprende 256 elementos, que toman los valores de 1 a 256. Estos valores son ordenados en un orden aleatorio.

En un modo de realización preferente, esta tabla es creada en cada lanzamiento del algoritmo de AES.

La fig. 3 ilustra una operación de clave secreta 102 según un modo de realización del invento. Tal operación puede corresponder a la operación 'AddRoundKey' 202 modificada según un modo de realización del invento.

La operación 102 es una operación a realizar con un bloque de clave criptográfica secreta K 304 escrita sobre n bits. Una tabla 301 comprende elementos correspondientes a todos los valores posibles o sea 2^n elementos, ordenados aleatoriamente. A título de ejemplo, n es igual a 8. Un elemento 304 corresponde a un bloque de clave criptográfica secreta de la operación con clave secreta 102. Se busca bloque de clave criptográfica secreta en la tabla 301 de preferencia mediante una función resistente contra los ataques de SPA. Este tipo de función de búsqueda es bien conocido por el experto en la técnica y no ha sido detallado en este documento. De preferencia, se almacena entonces en memoria la dirección del bloque de clave criptográfica secreta.

Se aplica la operación 102 de clave secreta al bloque de datos 101 con todos los elementos de la tabla 301 que comprenden los valores de claves, ya sea simultáneamente, o bien secuencialmente. Se obtiene entonces una tabla 303 transformada que comprende 2^n elementos, o sea 256 elementos. Cada uno de estos elementos corresponde al resultado de la operación 102 aplicada al bloque de datos 101 con una clave secreta situada en la tabla 301 en la misma dirección que este elemento. Esta tabla 303 comprende en particular un elemento 305 correspondiente al bloque de datos en curso de cifrado, siendo este bloque el resultado de la operación con clave secreta 102 aplicada con el bloque de clave criptográfica secreta 304.

Al ser aplicada la operación de manera que todos los valores de clave posibles tengan la misma probabilidad, esta etapa es protegida contra cualquier ataque relativo a un análisis de las fugas de información durante la ejecución del cálculo.

Luego, en un algoritmo de tipo AES, la operación con clave secreta va seguida de la operación no lineal 107 'ByteSub'. Tal operación puede ser fuente de informaciones preciosas durante ataques de SPA o de DPA. De hecho es muy importante proteger su ejecución. Así, en un modo de realización preferido del invento, se aplica tal

operación sobre todos los elementos de la tabla 303.

La fig. 4 ilustra la ejecución de una operación no lineal según un modo de realización del presente invento. Así, la operación no lineal 107 es aplicada o bien simultáneamente, o bien secuencialmente, a todos los elementos de la tabla 303 para proporcionar una tabla 402 que comprende 2^n elementos, o sea 256 elementos. Cada elemento corresponde al resultado de la operación no lineal aplicada sobre el elemento de la tabla 303 situado en la misma dirección.

Así, se está en disposición de recuperar el bloque de datos en curso de cifrado 403 una vez que se ha almacenado en memoria la dirección del bloque de clave criptográfica secreta en la tabla 301 que comprende las claves.

Se recupera entonces el bloque de datos en curso de cifrado 403 en la tabla 402, sobre la base de la dirección del bloque de clave criptográfica secreta previamente almacenada en memoria, de preferencia, por medio de una función resistente contra los ataques de SPA.

Se pueden entonces realizar las operaciones 'ShiftRow' 206, 'MixColumns' 207 únicamente sobre el bloque de datos en curso de cifrado y no ya sobre los bloques de datos secundarios, salidos de operaciones con claves secretas secundarias y no de los bloques de clave criptográfica secreta. Estas últimas operaciones son entonces de preferencia realizadas aplicando máscaras de valores aleatorios al bloque de datos en curso de cifrado manipulado.

En un algoritmo de tipo AES, todas o parte de las operaciones 202 'AddRoundKey' pueden ser realizadas según un modo de realización del invento.

En ciertos casos, se puede desear ejecutar una parte solamente de las operaciones 'AddRoundKey' 202 y 'ByteSub' 205 del algoritmo según un modo de realización del presente invento. En este caso se ejecutarán según el invento, de preferencia las operaciones 'AddRoundKey' 202 y 'ByteSub' 205 al comienzo del algoritmo, es decir al menos la primera vuelta del algoritmo, o al final del algoritmo, es decir en al menos la última vuelta del algoritmo.

A fin de mejorar la protección contra los ataques precedentemente descritos, es ventajoso enmascarar los bloques de datos en curso de cifrado manipulados. El enmascaramiento puede ser realizado fácilmente añadiendo un valor aleatorio por un o exclusivo.

La fig. 5 ilustra las etapas para cifrar un mensaje de 16 octetos según un algoritmo de tipo AES que comprende cálculos criptográficos ejecutados según un modo de realización del presente invento, y más particularmente el paso a la primera vuelta. En esta figura, la tabla que contiene todos los valores de claves es denominada RAND[l]. Esta tabla comprende los valores de 1 a 256 aleatoriamente ordenados. El mensaje M a cifrar está compuesto de 16 bloques de datos de un octeto cada uno, M_i para i igual de 1 a 16.

Así, al comienzo del algoritmo, se trata en primer lugar el primer octeto M_1 501 del mensaje M a cifrar.

En la etapa 502, se realiza la operación 'AddRoundKey' según un modo de realización del invento. Así, en una primera etapa 504, se busca en primer lugar el bloque de clave criptográfica secreta $K_{i,1}$ en la tabla RAND[l] mediante una función resistente contra los ataques SPA para obtener su posición en esta tabla y se genera un valor de octeto aleatorio A_i, utilizado para enmascarar el bloque de datos manipulado. Luego, se ejecuta un bucle para j igual a 1 hasta j igual a 256, mediante las etapas 505, 506, 508, a fin de aplicar la operación 'AddRoundKey' con todas las claves de la tabla RAND[l] seguida de la ejecución de la operación 'ByteSub'. Cuando todos los elementos de la tabla RAND[l] han sido tratados, en la etapa 511 se recupera, mediante una función resistente a los ataques de SPA, el bloque de datos en curso de cifrado correspondiente al resultado de las operaciones sobre el bloque de datos M_1 con el bloque de clave criptográfica secreta correspondiente.

A continuación, se incrementa i en la etapa 512. Se reiteran así todas las operaciones precedentemente descritas sobre todos los octetos M_l del mensaje a cifrar. Luego, se aplican sobre los bloques de datos en curso de cifrado así obtenidos las operaciones 'SiftRows' y 'MixColumn', siendo estas operaciones preferiblemente realizadas de manera enmascarada.

La fig. 6 ilustra las etapas para cifrar un mensaje de 16 octetos según un algoritmo de tipo AES que comprende cálculos criptográficos ejecutados según un modo de realización del presente invento y más particularmente el paso entre dos vueltas consecutivas del algoritmo.

La etapa 602 representa la operación 'AddRoundKey' ejecutada al final de una vuelta del algoritmo. Las etapas 602 y 603 son similares a las etapas de la fig. 5 precedentemente descritas. Se señala que en la etapa 606, se enmascara el cálculo añadiendo por un o exclusivo una máscara B, que es un valor aleatorio.

Así, durante un ataque sobre la operación no lineal, se recoge de manera que tengan la misma probabilidad el conjunto de las fugas de información unidas a la operación no lineal de sustitución ya que esta última es realizada sobre todos los bloques de datos secundarios y el bloque de datos en curso de cifrado. De esta manera, durante un ataque DPA realizado durante la ejecución de cálculos del algoritmo según un modo de realización del invento, se pueden detectar 256 bits, 1 bit para cada octeto de clave. En consecuencia todas las hipótesis de clave son validadas por un ataque de este tipo. La confidencialidad de las claves secretas es así preservada.

A fin de preservar un buen rendimiento de ejecución del algoritmo criptográfico, se puede realizar ventajosamente de manera simultánea y por tanto paralelamente una parte de los cálculos ejecutados según el invento.

REIVINDICACIONES

1. Procedimiento de ejecución de un cálculo criptográfico en un componente electrónico, según un algoritmo criptográfico determinado que incluye al menos una operación con clave secreta (102) a realizar sobre un bloque de datos (101) con una clave criptográfica secreta (103) que comprende m bloques de clave criptográfica secreta de n bits, y una operación no lineal (107), comprendiendo dicho procedimiento, para un bloque de clave criptográfica secreta dado, las etapas siguientes consistentes en:

- determinar 2^n-1 claves secretas secundarias diferentes (105) sobre n bits, siendo cada una diferente de dicho bloque de clave criptográfica secreta;

- realizar dicha operación con clave secreta (102) con dicho bloque de clave criptográfica secreta (103) y con dichas claves secretas secundarias sobre un bloque de datos (101) y obtener respectivamente un bloque de datos en curso de cifrado (104) y 2^n-1 bloques de datos secundarios (106);

- realizar dicha operación no lineal (107) sobre dicho bloque de datos en curso de cifrado (104) y sobre dichos bloques de datos secundarios (106);

- proporcionar un bloque de datos cifrado (108) a partir del bloque de datos en curso de cifrado.

2. Procedimiento según la reivindicación 1, que comprende, para un bloque de clave criptográfica secreta, las etapas que consisten en:

/a/ determinar y disponer aleatoriamente las claves secretas secundarias en una tabla inicial que comprende dicho bloque de clave criptográfica secreta;

/b/ almacenar en memoria la dirección correspondiente a dicho bloque de clave criptográficas secreta en la tabla inicial;

/c/ aplicar la operación con clave secreta al bloque de datos (101) con las claves de la tabla inicial (301) y obtener una primera tabla transformada (303) de 2^n primeros elementos, correspondiendo cada primer elemento al resultado de la operación con clave secreta (102) aplicada al bloque datos (101) con la clave situada en la tabla inicial en la misma dirección que dicho primer elemento;

/d/ aplicar dicha operación no lineal (107) a los elementos de dicha primera tabla transformada (303) y obtener una segunda tabla transformada (402) de 2^n segundos elementos, correspondiendo cada segundo elemento al resultado de la operación no lineal (107) aplicada al primer elemento situado en la misma dirección en la primera tabla transformada (303) que dicho segundo elemento;

/e/ recuperar, en la segunda tabla transformada (402), el elemento correspondiente al bloque de datos en curso de cifrado (403) situado en la dirección de dicho bloque de clave criptográfica secreta.

3. Procedimiento según la reivindicación 2, según el cual se recupera el elemento correspondiente al bloque de datos en curso de cifrado (403), en la segunda tabla transformada, mediante una función resistente contra un ataque de tipo SPA acrónimo de 'Simple Power Analysis' tomando como parámetro la dirección de la clave criptográfica secreta.

4. Procedimiento según la reivindicación 2 ó 3, según el cual el algoritmo criptográfico comprende un número determinado de vueltas, cada una de las cuales incluye al menos una operación de clave criptográfica secreta que precede a una operación no lineal;

y según el cual se realizan las etapas /a/ a /e/ para al menos la primera vuelta y al menos la última vuelta del algoritmo criptográfico.

5. Procedimiento según una cualquiera de las reivindicaciones 2 a 4, según el cual se realiza la etapa de disposición aleatoria al comienzo del algoritmo criptográfico.

6. Procedimiento según una cualquiera de las reivindicaciones precedentes, según el cual se realiza simultáneamente la operación con clave secreta (102) con uno de los bloques de clave criptográfica secreta y con las claves secretas secundarias y/o se realiza simultáneamente la operación no lineal sobre el bloque de datos y los bloques de datos secundarios.

7. Procedimiento según una cualquiera de las reivindicaciones precedentes, según el cual el algoritmo criptográfico es el AES.

8. Procedimiento según una cualquiera de las reivindicaciones precedentes, según el cual una al menos de las operaciones del algoritmo criptográfico es realizada sobre el bloque de datos en curso de cifrado enmascarado con un valor aleatorio.

9. Componente electrónico adaptado para ejecutar un cálculo criptográfico según un algoritmo criptográfico determinado que incluye al menos una operación con clave secreta (102) a realizar con una clave criptográfica secreta (103) que comprende m bloques de clave secreta de n bits sobre un bloque de datos (101) y una operación no lineal (107), comprendiendo medios dispuestos para poner en práctica un procedimiento según una cualquiera de las reivindicaciones precedentes.

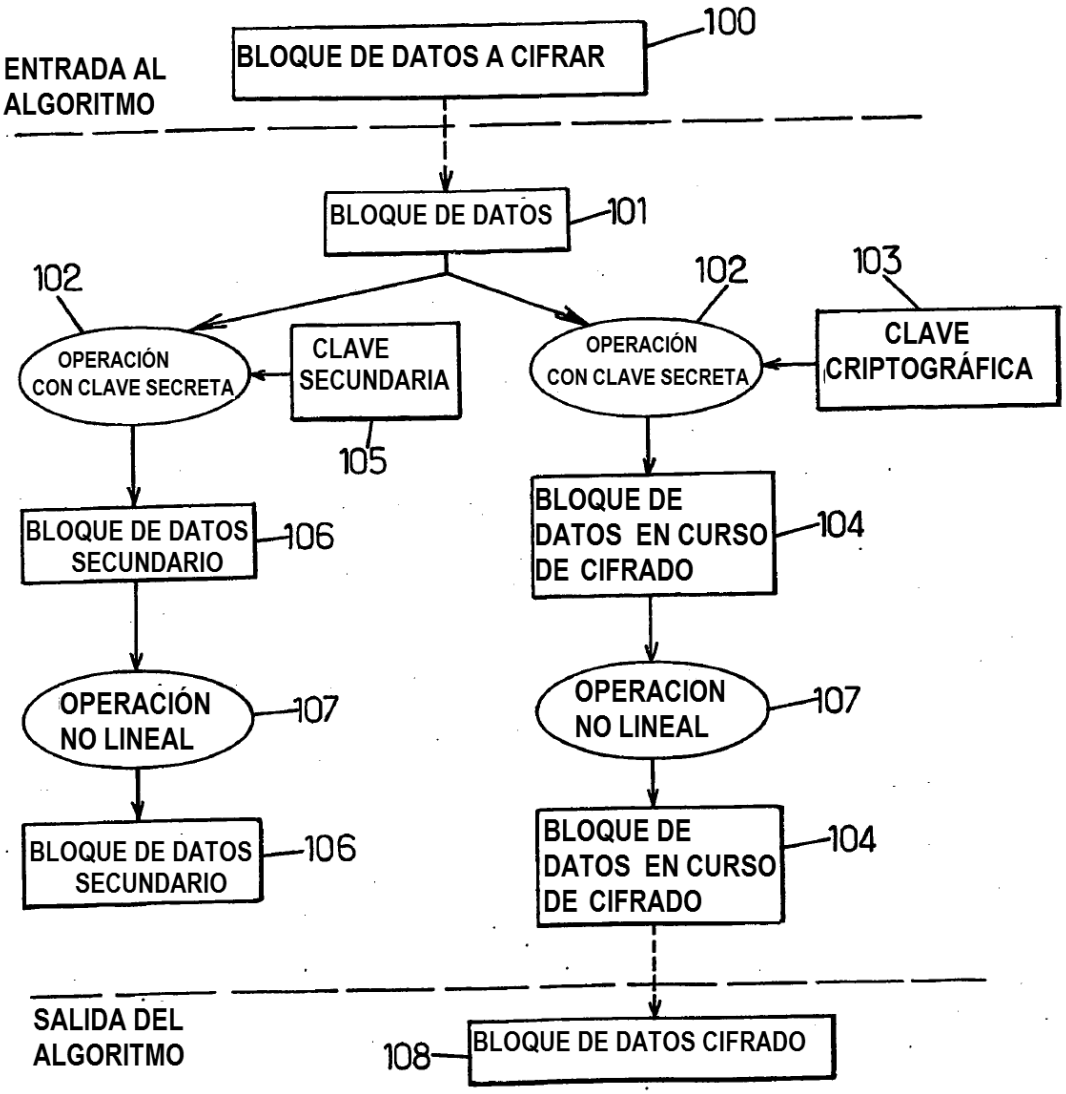

ENTRADA AL ALGORITMO
BLOQUE DE DATOS A CIFRAR
100
BLOQUE DE DATOS
101
102
OPERACIÓN CON CLAVE SECRETA
CLAVE SECUNDARIA
105
102
OPERACIÓN CON CLAVE SECRETA
103
CLAVE CRIPTOGRÁFICA
BLOQUE DE DATOS SECUNDARIO
106
BLOQUE DE DATOS EN CURSO DE CIFRADO
104
OPERACIÓN NO LINEAL
107
OPERACION NO LINEAL
107
BLOQUE DE DATOS SECUNDARIO
106
BLOQUE DE DATOS EN CURSO DE CIFRADO
104
SALIDA DEL ALGORITMO
108
BLOQUE DE DATOS CIFRADO

FIG.1.

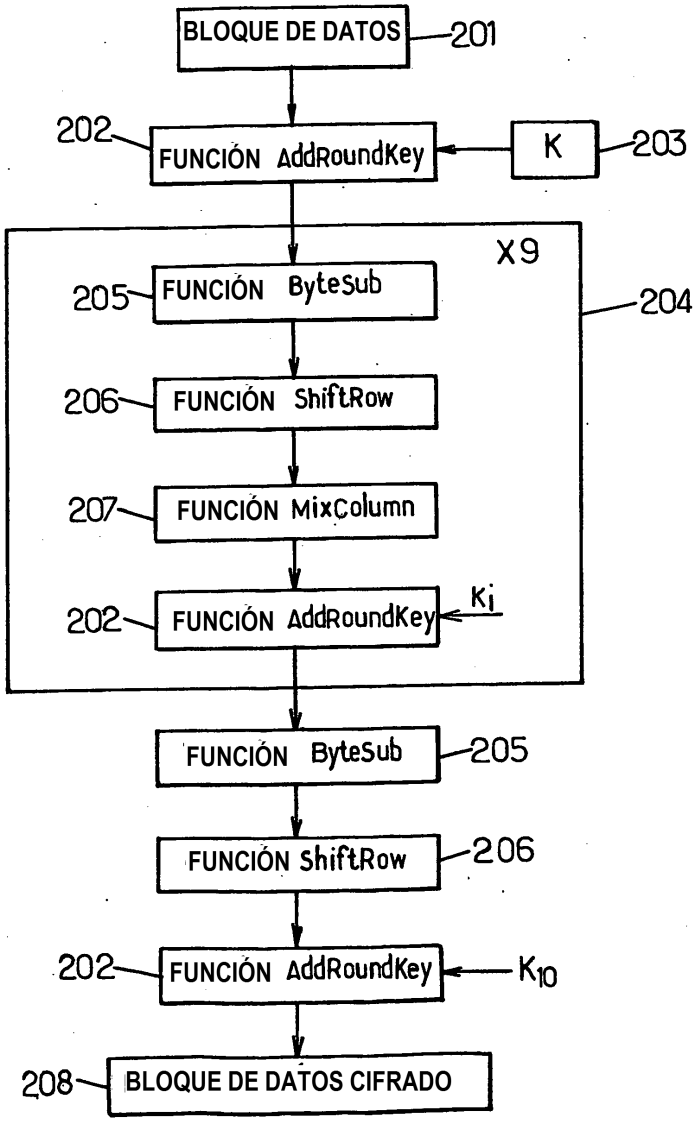

BLOQUE DE DATOS
201
202
FUNCIÓN AddRoundKey
K
203
X9
205
FUNCIÓN ByteSub
204
206
FUNCIÓN ShiftRow
207
FUNCIÓN MixColumn
202
FUNCIÓN AddRoundKey
Ki
FUNCIÓN ByteSub
205
FUNCIÓN ShiftRow
206
202
FUNCIÓN AddRoundKey
K10
208
BLOQUE DE DATOS CIFRADO

FIG.2.

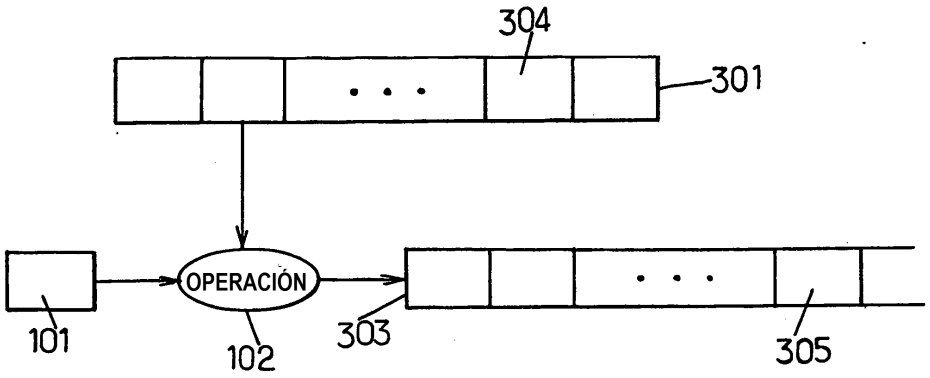

304
301
OPERACIÓN
101
102
303
305

FIG.3.

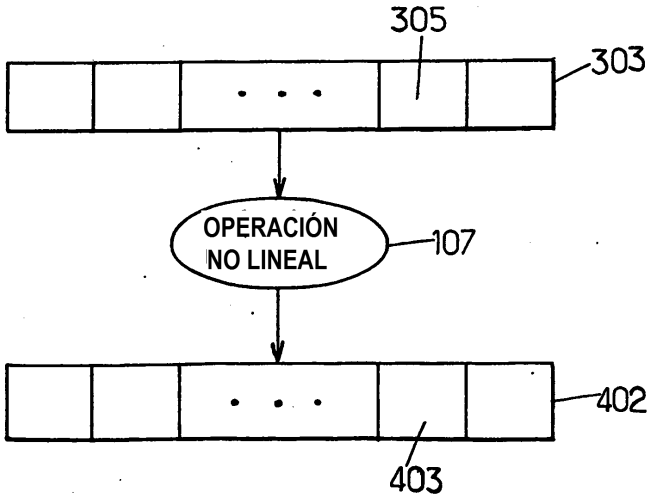

305
303
OPERACIÓN
NO LINEAL
107
402
403

FIG.4.

FIG.5.

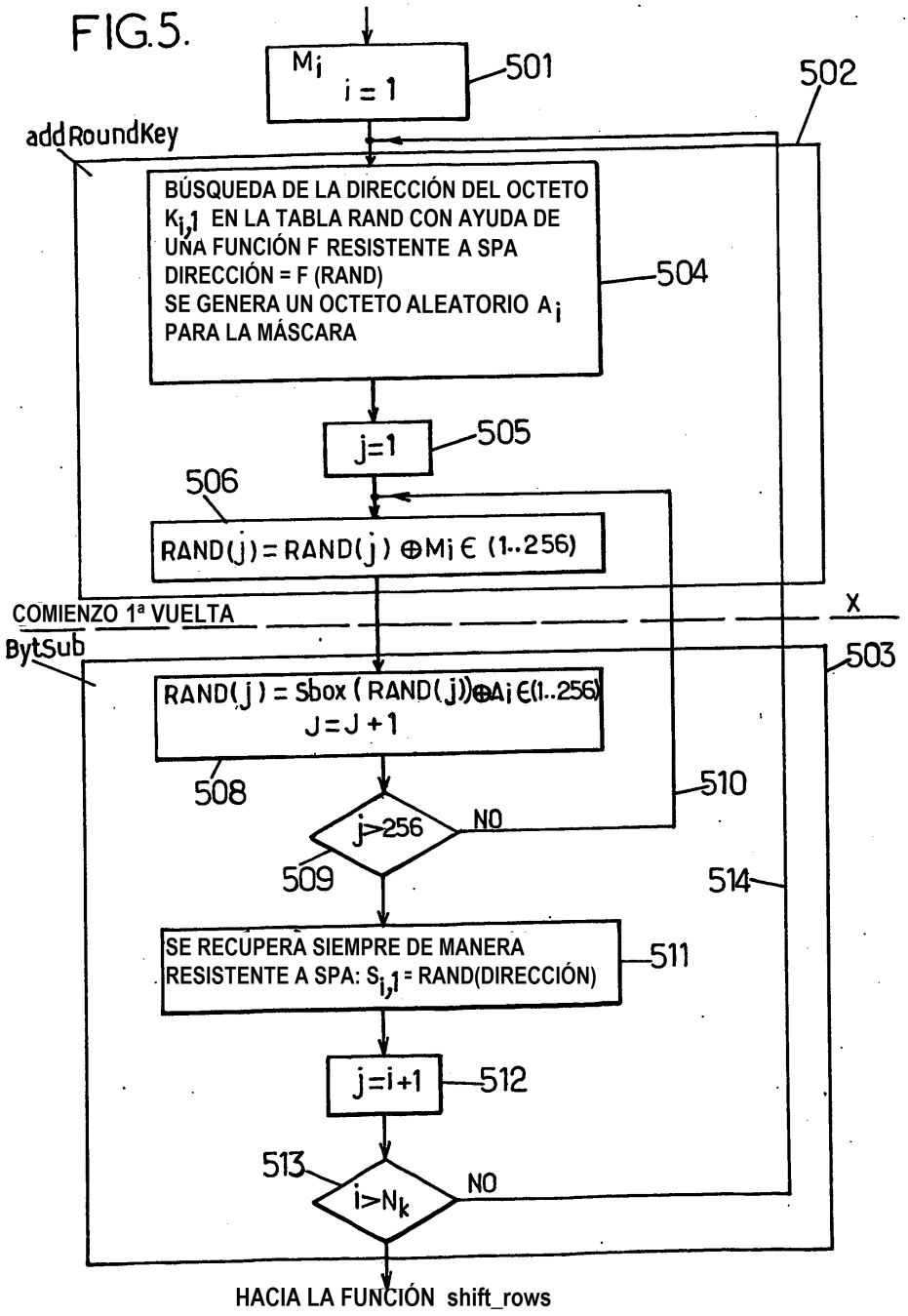
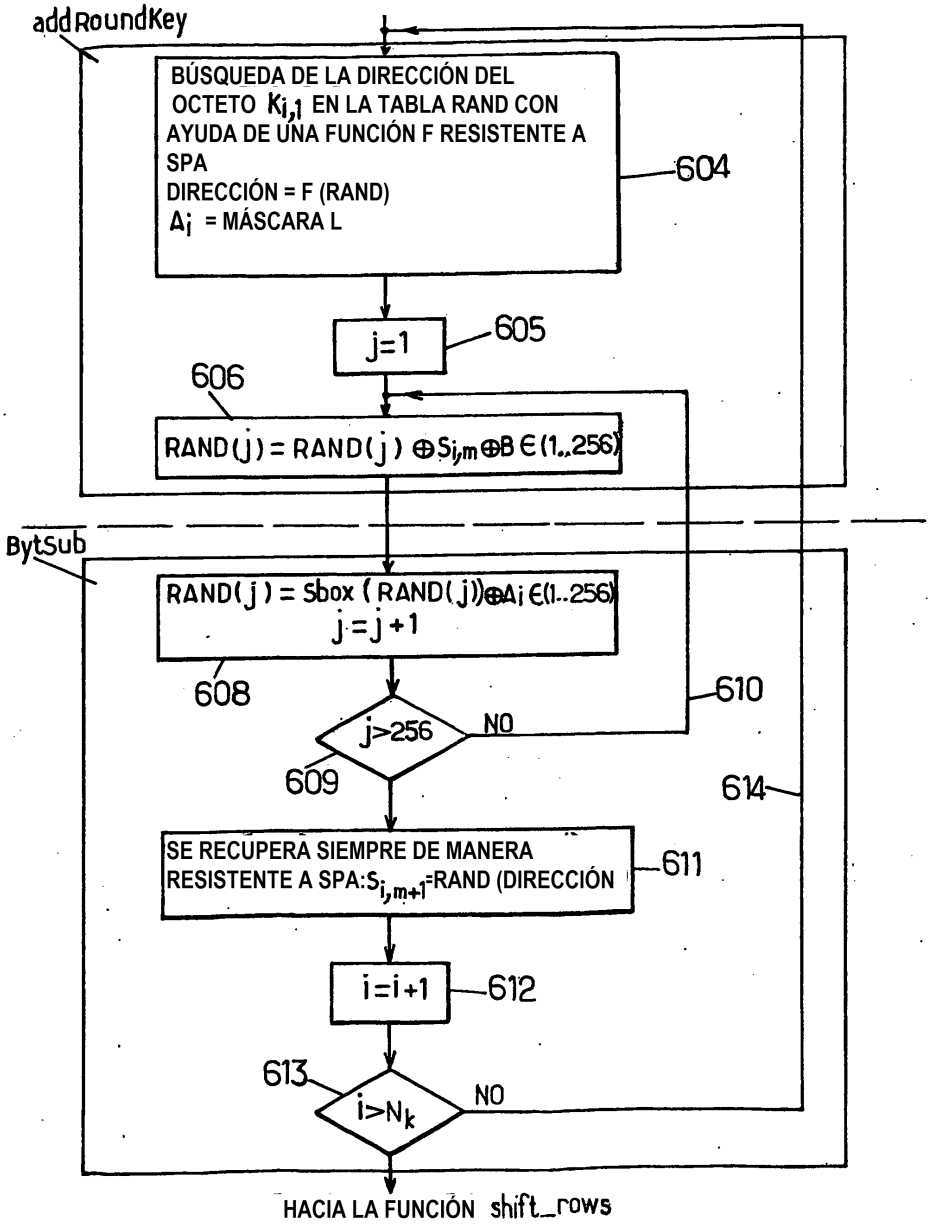

Mi
i = 1
501
502
addRoundKey
BÚSQUEDA DE LA DIRECCIÓN DEL OCTETO Ki,1 EN LA TABLA RAND CON AYUDA DE UNA FUNCIÓN F RESISTENTE A SPA
DIRECCIÓN = F (RAND)
SE GENERA UN OCTETO ALEATORIO Ai PARA LA MÁSCARA
504
j=1
505
506
RAND(j) = RAND(j) ⊕Mi ∈ (1..256)
COMIENZO 1ª VUELTA
X
ByteSub
503
RAND(j) = Sbox (RAND(j) ⊕Ai ∈(1..256)
J=J+1
508
510
j>256
NO
509
514
SE RECUPERA SIEMPRE DE MANERA RESISTENTE A SPA: Si,1 = RAND(DIRECCIÓN)
511
j=i+1
512
513
i>Nk
NO
HACIA LA FUNCIÓN shift_rows

FIG.6.


addRoundKey
BÚSQUEDA DE LA DIRECCIÓN DEL OCTETO $K_{i,1}$ EN LA TABLA RAND CON AYUDA DE UNA FUNCIÓN F RESISTENTE A SPA
DIRECCIÓN = F (RAND)
A_i = MÁSCARA L
604
j=1
605
606
RAND(j) = RAND(j) ⊕ $S_{i,m}$ ⊕B ∈(1..256)
BytSub
RAND(j) = Sbox (RAND(j)) ⊕A_i ∈(1..256)
j = j +1
608
j>256
NO
609
610
614
SE RECUPERA SIEMPRE DE MANERA RESISTENTE A SPA: $S_{i,m+1}$=RAND (DIRECCIÓN
611
i=i+1
612
613
$i>N_k$
NO
HACIA LA FUNCIÓN shift_rows