(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 269 625**

(51) Int. Cl.:
H04L 9/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **02290908 .9**
(86) Fecha de presentación : **11.04.2002**
(87) Número de publicación de la solicitud: **1263163**
(87) Fecha de publicación de la solicitud: **04.12.2002**

(54) Título: **Procedimiento fundado en un algoritmo de cifrado por bloque con repetición de rondas y dispositivo para su realización.**

(30) Prioridad: **31.05.2001 FR 01 07163**

(45) Fecha de publicación de la mención BOPI:
01.04.2007

(45) Fecha de la publicación del folleto de la patente:
01.04.2007

(73) Titular/es: **SAGEM Défense Sécurité**
Le Ponant de Paris, 27 rue Leblanc
75015 Paris, FR

(72) Inventor/es: **Chabanne, Hervé**

(74) Agente: **Durán Moya, Carlos**

DESCRIPCIÓN

Procedimiento fundado en un algoritmo de cifrado por bloque con repetición de rondas y dispositivo para su realización.

La presente invención se refiere a perfeccionamientos en los procedimientos -y dispositivos para su realización- fundados en un algoritmo de cifrado por bloque con repetición de ronda, apropiado para facilitar, a partir de un dato de entrada de longitud determinada, un criptograma o dato de salida que depende del dato de entrada y de una llave memorizada inaccesible en lectura desde el exterior.

Para fijar ideas, los perfeccionamientos que la invención está destinada a aportar se pueden referir a algoritmos con repetición de rondas involutivas -tales como el algoritmo DES (Data Encryption Standard) corrientemente utilizado en las tarjetas de criptografía para establecer un criptograma a partir de un dato de entrada de 8 octetos y de una clave maestra de 56 elementos binarios o bits útiles) o algoritmo KASUMI (denominado también MISTY)- o algoritmos de repetición de rondas no involutivas -tal como el algoritmo AES-.

Entre los diferentes tipos de ataque que se pueden conducir contra medios de algoritmos, el ataque DFA (Differential Fault Analysis) consiste en provocar errores durante la ejecución de un algoritmo criptográfico, y después comparar los resultados obtenidos

- por una parte, cuando los cálculos han sido ejecutados correctamente y
- por otra parte, cuando los cálculos han sido ejecutados con errores,

y finalmente deducir de esta comparación la clave utilizada.

Este ataque, cuando su utilización resulta posible, es relativamente eficaz, puesto que permite en algunas decenas de llamadas al algoritmo encontrar la clave utilizada. Frecuentemente se pone en práctica contra algoritmos DES implementados en tarjetas de microcircuito (tarjetas de criptografía ("cartes à puce")).

El documento EP 1 052 801 A2 divulga un procedimiento de puesta en práctica de algoritmos criptográficos según el cual, para aumentar la seguridad en caso de violación, se ponen en práctica, con el algoritmo, funciones que, en el desarrollo del algoritmo, comportan la ejecución de operaciones suplementarias, por medio de las cuales el desarrollo temporal del algoritmo se modifica cada vez de manera aleatoria o de manera controlada seudo-aleatoria, pero el resultado de la codificación no queda influido, de manera que, para las operaciones suplementarias, se trata de operaciones sin resultado o de manera que los resultados que proceden de la realización de operaciones matemáticas suplementarias no son tratados ulteriormente, anulándose en vistas al resultado de codificación o que no constituyen más que la base para la fijación del número y/o secuencia de otras operaciones o de la secuencia temporal de etapas parciales permutables del algoritmo sin incidencia en el resultado de la codificación.

El inconveniente de ese procedimiento conocido consiste en la modificación -aleatoria o seudo-aleatoria- del desarrollo temporal del algoritmo. No obstante la incertidumbre relativa de este parámetro de puesta en práctica puede ser inaceptable en el caso de aplicaciones en las que el dominio de todos los parámetros -incluyendo el desarrollo temporal- de funcionamiento del algoritmo resulta necesario.

La invención tiene por objetivo esencialmente proponer medios -procedimiento y dispositivo- perfeccionados apropiados para procurar protección contra ese tipo de ataque DFA.

Con esta finalidad, de acuerdo con uno de sus primeros aspectos, la invención propone un procedimiento basado en un algoritmo de cifrado con repetición de rondas que pone en práctica un número determinado de rondas, utilizando la clave maestra a partir de la cual se generan una o varias subclaves que son inyectadas en las rondas, cuyo procedimiento, de acuerdo con la invención, se caracteriza porque el algoritmo incluye además, como mínimo, un par de rondas suplementarias constituidas por una primera y segunda rondas sin utilidad en el desarrollo del algoritmo y a las cuales se afectan subclaves respectivas y porque se da a las rondas suplementarias un perfil análogo al de las rondas definidas por el algoritmo, siendo gracias a ello que la puesta en práctica de este par como mínimo de rondas suplementarias se puede hacer indetectable.

Por lo tanto, la presente invención propone medios puramente de algoritmo para llegar a la seguridad del desarrollo del algoritmo de cifrado. La introducción de un par de rondas suplementarias no presenta, en principio, ningún problema ni para la puesta en práctica ni para el funcionamiento, y la introducción de varios pares de rondas suplementarias incrementa la seguridad sin introducir dificultad sensible.

En el curso del funcionamiento normal del algoritmo modificado conforme a la invención, el par de rondas suplementarias o cada una de ellas introducida artificialmente en el algoritmo es puramente transparente y no tiene influencia alguna sobre el criptograma obtenido en la salida. Por el contrario, en presencia de un ataque DFA una de las rondas suplementarias tiene el riesgo de ser modificada -siendo tanto más probable dicha modificación de una ronda suplementaria cuando el número de pares de rondas añadido es elevado-, mientras que no existe más que una probabilidad casi nula para que las dos rondas de un par añadido sean simultáneamente modificadas de manera que sus efectos se compensen mutuamente: resulta entonces imposible efectuar comparaciones válidas entre los cálculos de los algoritmos correctos y los afectados voluntariamente de error, y la identificación de la clave resulta imposible.

Los medios propuestos por la invención se muestran relativamente simples de poner en práctica, mientras que su eficacia es elevada. Al ser el perfil de las rondas suplementarias análogo al de las rondas de calculo del algoritmo, estas rondas artificiales pueden no ser descubiertas por medidas del tipo de medición del consumo eléctrico instantáneo (ataque DPA: análisis diferencial de consumo). Además, este procedimiento puede ser utilizado en combinación con la puesta en práctica de mascaras tal como muestra el documento FR-A-2 802 741.

Para evitar una complicación extrema de los cálculos, es deseable que el par de rondas suplementarias esté formado por dos rondas sucesivas, de manera que las dos rondas del algoritmo de encriptado entre las que dicho par de rondas suplementarias ha sido aña-

dido transmiten las mismas informaciones que en el algoritmo no modificado.

En una puesta en práctica ventajosa del procedimiento de la invención, la segunda ronda es la ronda inversa de la primera ronda y está afectada de una subclave (K') diferente de la subclave (K) de la primera ronda, pero independiente de la subclave (K).

En la puesta en práctica específica, la primera ronda es involutiva y la misma subclave (K) está afectada a la ronda y a su inversa. En este caso, las disposiciones de la invención encuentran una aplicación preferente, si bien no limitativa, para la protección del algoritmo iterativo DES compuesto de una permutación IP, de 16 rondas sucesivas, y de la inversa de la permutación IP.

De acuerdo con un segundo aspecto, la invención propone perfeccionar el dispositivo que pone en práctica un algoritmo de cifrado con repetición de rondas con un número dado de rondas, utilizando una clave maestra a partir de la cual se generan una o más subclaves que son inyectadas en las rondas, cuyo dispositivo, que está dispuesto de acuerdo con la invención, se caracteriza por incluir además medios para poner en práctica como mínimo un par de rondas suplementarias constituido por una primera y una segunda rondas sin utilidad en el desarrollo del algoritmo y a las cuales se afectan subclaves respectivas y porque las rondas suplementarias poseen un perfil análogo al de las rondas definidas por el algoritmo, siendo gracias a ello que dicho par o pares de rondas suplementarias se pueden hacer indetectables. Preferentemente, el par de rondas suplementarias está formado por rondas sucesivas.

Se puede hacer de manera que la segunda ronda sea la ronda inversa de la primera y que lleve afectada una subclave (K') distinta de la subclave (K) de la primera ronda, pero independiente de la subclave (K).

Cuando ello es posible, es ventajoso que la primera ronda sea involutiva y que la misma subclave (K) esté afectada a la ronda y a su inversa. Este dispositivo encuentra una aplicación preferente, si bien no exclusiva, en la puesta en práctica del algoritmo iterativo DES, compuesto por una permutación IP, de 16 rondas sucesivas, y de la inversa de la permutación IP.

La invención se comprenderá mejor por la lectura de la descripción detallada que sigue de ciertas formas de realización indicadas a título de ejemplo no limitativo. En esta descripción, se hará referencia a los dibujos adjuntos en los cuales:

- la figura 1A muestra de manera muy esquemática, a título de referencia, dos etapas consecutivas de un algoritmo;
- la figura 1B muestra muy esquemáticamente la misma parte del algoritmo que en la figura 1 después de modificación según la invención;
- la figura 2 muestra muy esquemáticamente una parte de un algoritmo modificado según una puesta en práctica ventajosa de los dispositivos de la invención;
- la figura 3A muestra muy esquemáticamente el algoritmo DES; y
- la figura 3B muestra muy esquemáticamente el algoritmo DES modificado según la puesta en práctica específica, preferente, de la invención.

Haciendo referencia inicialmente a la figura 1A, la invención se refiere a un algoritmo de cifrado de repetición de rondas utilizando una clave maestra a partir de la cual se generan una o varias subclaves que son inyectadas en las rondas. En la figura 1 se ha esquematizado una ronda de rango i que recibe datos de d_i (datos de entrada si la ronda es de rango 1; datos de salida de la ronda precedente de rango i-1 en otro caso); a esta ronda de rango i se ha asociado una subclave (K_i). La ronda de rango i facilita datos de d_{i+1} destinados a la ronda siguiente de rango i+1 generada por una subclave (K_{i+1}).

De acuerdo con la invención, se introduce en el algoritmo como mínimo un par de rondas suplementarias r' y r", entre las rondas de rango i y i+1, siendo gestionadas respectivamente las rondas r' y r" por subclaves (K') y (K"). Las rondas r' y r" no tienen utilidad en el desarrollo normal del algoritmo, las claves (K') y (K") son arbitrarias, y se preven medios apropiados para hacer que no se pueda descubrir la puesta en práctica de estas dos rondas suplementarias, especialmente en presencia de un ataque DPA.

Por este hecho, la ronda de rango i emite siempre datos d_{i+1} y la ronda de rango i+1 recibe siempre datos d_{i+1} cuando el algoritmo funciona normalmente, de la misma manera que se ha mostrado en la figura 1A. Por el contrario, en presencia de un ataque DFA, si una de las rondas artificiales r' o r" es modificada, el atacante recupera incógnitas procedentes de la subclave aleatoria (K') o (K") respectivamente asociada a la ronda modificada. Dado que existe una probabilidad casi nula para que las dos rondas suplementarias r' y r" sean modificadas simultáneamente de manera que sus efectos se compensen, el trabajo de criptoanálisis del atacante DFA se hace muy complicado, o incluso imposible.

La eficacia de las disposiciones de la invención es tanto mejor cuanto el número de pares de rondas suplementarias introducidas en el algoritmo queda incrementado. Se puede multiplicar de esa manera los pares de rondas suplementarias introducidas cada una entre dos rondas consecutivas, o incluso se pueden introducir varios pares de rondas suplementarias sucesivas entre dos rondas consecutivas.

No obstante, para no complicar excesivamente el funcionamiento del algoritmo, es preferible no separar las dos rondas de un par suplementario y constituir el par de rondas suplementarias por dos rondas consecutivas r' y r", tal como se ha mostrado en la figura 1B.

En una forma de realización preferente que se ha mostrado en la figura 2, la segunda ronda es la ronda inversa r^{-1} de la primera ronda r y está afectada a esta ronda inversa r^{-1} una subclave (K') que es diferente de la subclave (K) de la primera ronda, pero que depende de esta subclave (K)(indicada K'(K) en la figura 2).

Las disposiciones que se han explicado no tienen en cuenta el carácter involutivo o no involutivo de las rondas del algoritmo y se aplican por lo tanto a cualquier algoritmo de cifrado con repetición de rondas generadas cada una de ellas por una subclave generada a partir de una clave maestra.

No obstante, en el caso en que las rondas son involutivas, se puede simplificar la puesta en práctica de la invención dando la misma subclave aleatoria (K) a la ronda suplementaria r y a su inversa r^{-1}.

Las disposiciones de la invención que se han explicado son aplicables de forma especialmente interesante, si bien no exclusiva, en la protección del algoritmo DES corrientemente puesto en práctica en las tarjetas de encriptado ("cartes à puce"). Tal como se ha mostrado en la figura 3A, el algoritmo DES presenta una etapa de entrada constituida por un permutador

de entrada o permutador inicial IP que facilita, a partir de un dato de entrada E, una parte izquierda de 32 bits y una parte derecha de 32 bits, constituyendo operandos los 32 bits mencionados. Cada etapa i presenta:

- un elemento de expansión a^i_d que aumenta las dimensiones de la parte derecha.
- un conjunto b^i_d que tiene en cascada un operador o EXCLUSIVO o XOR sobre el operando derecho expandido y una subclave (Ki) de igual longitud derivada de la clave maestra y de las tablas de substitución o "S boxes" c_i, afectada cada una a un grupo de bits y con lectura en un orden arbitrario.
- y un operador XOR di sobre el contenido leído en las tablas c_i y el operando izquierdo expandido a^i_g para dar origen a una parte de la izquierda de 32 bits que constituye la salida de la derecha de la etapa, estando constituida la otra salida, salida de la izquierda, de la etapa por el operando derecho expandido a^i_d.

El algoritmo de cifrado DES pone en práctica un número de n=16 etapas en cascada constituidas tal como se ha explicado, estando seguida la última etapa de un permutador que efectúa la operación inversa IP^{-1} y que facilita el criptograma de salida S.

De acuerdo con la invención, se introduce entre las etapas de rango i e i+1, una ronda r y su inversa r^{-1} consecutivas y gestionadas por la misma subclave (K) aleatoria, tal y como se ha mostrado en la figura 3B, no teniendo las rondas r y r^{-1} individualmente ninguna utilidad en el desarrollo del algoritmo.

REIVINDICACIONES

1. Procedimiento basado en un algoritmo de cifrado con repetición de rondas utilizando un número determinado de rondas, utilizando una clave maestra a partir de la cual se genera una o varias subclaves (K_i) que son inyectadas en las rondas (i),

caracterizado porque el algoritmo incluye además, como mínimo, un par de rondas suplementarias constituido por una primera y segunda rondas (r',r") sin utilidad en el desarrollo del algoritmo y a las que están afectadas subclaves respetivas (K',K") y porque se confiere a las rondas suplementarias un perfil análogo al de las rondas definidas por el algoritmo, siendo gracias a ello que la utilización de este par de rondas suplementarias mínimo se puede hacer indetectable.

2. Procedimiento, según la reivindicación 1, **caracterizado** porque el par de rondas suplementarias está formado por rondas sucesivas.

3. Procedimiento, según la reivindicación 1 ó 2, **caracterizado** porque la segunda ronda es la ronda inversa (r^{-1}) de la primera ronda (r) y porque está afectada a la misma una subclave (K') distinta de la subclave (K) de la primera ronda, pero dependiente de la subclave (K).

4. Procedimiento, según la reivindicación 4, **caracterizado** porque la primera ronda es involutiva y porque la misma subclave (K) está afectada a la ronda y a su inversa.

5. Procedimiento, según la reivindicación 4, **caracterizado** porque el algoritmo de cifrado es el algoritmo iterativo DES, compuesto por una permutación IP, de 16 rondas sucesivas, y de la inversa de la permutación IP.

6. Dispositivo que utiliza un algoritmo de cifrado con repetición de rondas con un número determinado de rondas, que utiliza una clave maestra a partir de la cual se generan una o varias subclaves (K_i) que son inyectadas en las rondas (i),

caracterizado porque el dispositivo incluye además medios para poner en práctica como mínimo un par de rondas suplementarias constituido por una primera y una segunda rondas (r') y (r") sin utilidad en el desarrollo del algoritmo y a las que están afectadas subclaves respectivas (K',K") y porque las rondas suplementarias poseen un perfil análogo al de las rondas definidas por el algoritmo, siendo gracias a ello que como mínimo un par de rondas suplementarias se puede hacer indetectable.

7. Dispositivo, según la reivindicación 6, **caracterizado** porque el par de rondas suplementarias está formado por rondas sucesivas.

8. Dispositivo, según la reivindicación 6 ó 7, **caracterizado** porque la segunda ronda es la ronda inversa (r^{-1}) de la primera ronda (r) y porque está afectada a la misma una subclave (K') distinta de la subclave (K) de la primera ronda, pero dependiente de la subclave (K).

9. Dispositivo, según la reivindicación 8, **caracterizado** porque la primera ronda es involutiva y por que la misma subclave (K) está afectada a la ronda y a su inversa.

10. Dispositivo, según la reivindicación 9, **caracterizado** porque el algoritmo de cifrado es el algoritmo iterativo DES, compuesto de una permutación IP, de 16 rondas sucesivas, y de la inversa de la permutación IP.

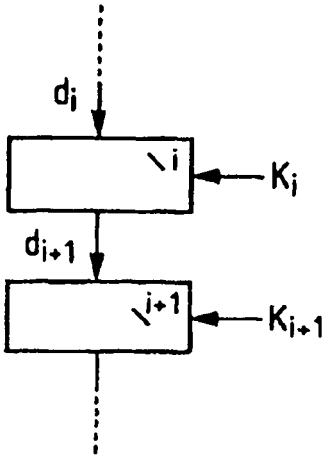

FIG. 1A

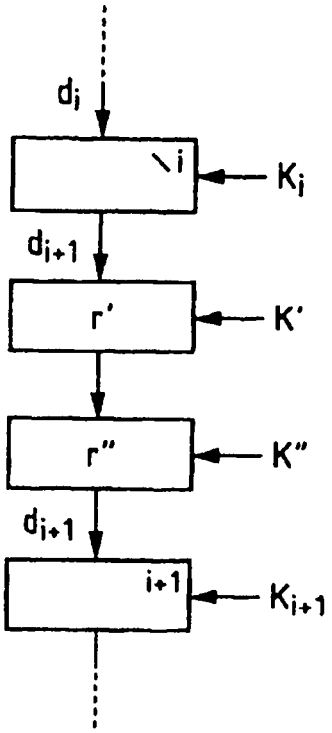

FIG. 1B

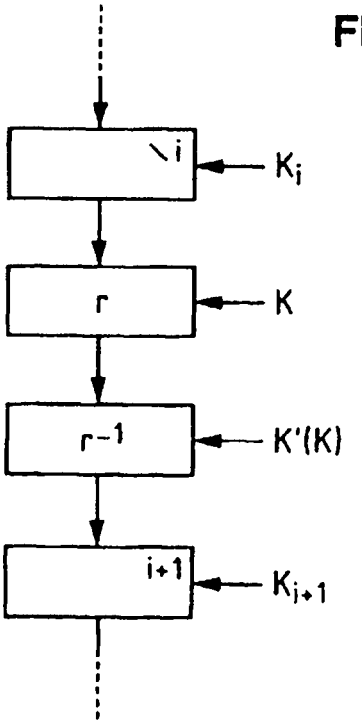

FIG. 2

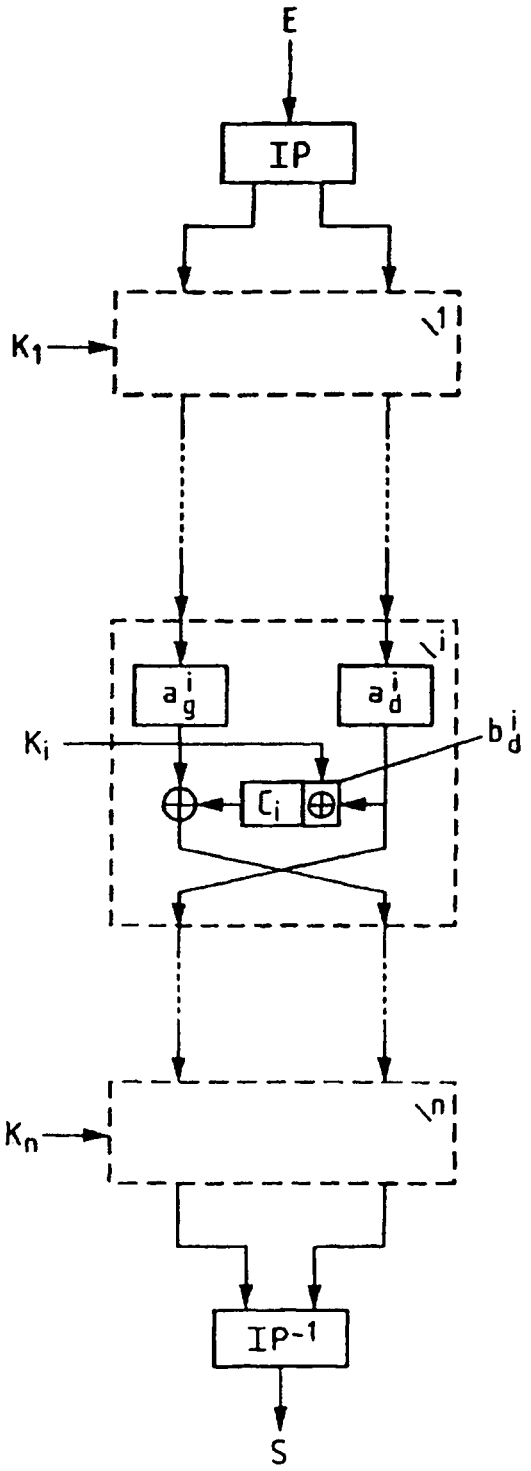

FIG. 3A

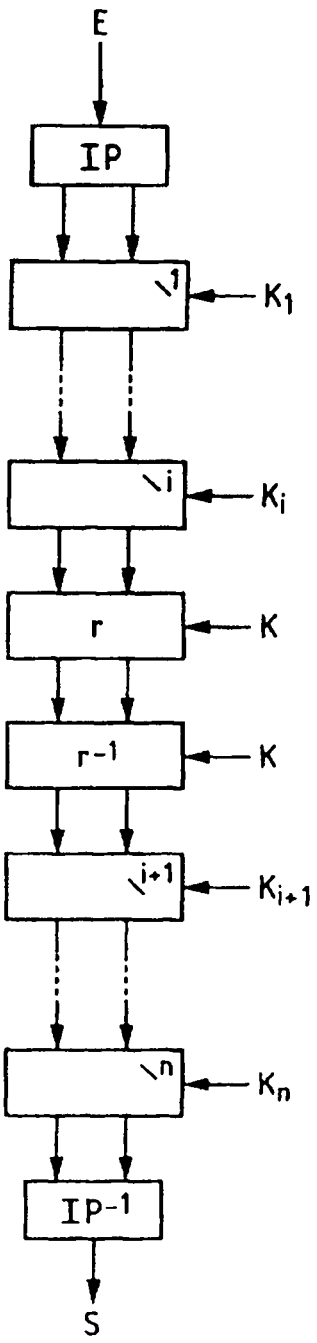

FIG. 3B