(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 822 298**

(51) Int. CI.:

H04L 9/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **31.10.2002 PCT/FR2002/03756**

(87) Fecha y número de publicación internacional: **08.05.0003 WO03039065**

(96) Fecha de presentación y número de la solicitud europea: **31.10.2002 E 02785576 (6)**

(97) Fecha y número de publicación de la concesión europea: **29.07.2020 EP 1442556**

(54) Título: **Procedimiento de puesta en práctica segura de un módulo funcional en un componente electrónico, y componente electrónico correspondiente**

(30) Prioridad:

31.10.2001 FR 0114132

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.04.2021

(73) Titular/es:

THALES DIS FRANCE SA (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

GUTERMAN, PASCAL;
FEYT, NATHALIE;
CLAVIER, CHRISTOPHE;
PETIT, SÉBASTIEN y
PROUST, PHILIPPE

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de puesta en práctica segura de un módulo funcional en un componente electrónico, y componente electrónico correspondiente

La presente invención concierne a un procedimiento de puesta en práctica segura de un módulo funcional en un componente electrónico.

Asimismo, la invención se refiere al componente electrónico correspondiente.

Se entiende por módulo funcional, un módulo de soporte físico dedicado a la ejecución de una función que puede ser un algoritmo, estando este módulo de soporte físico incluido en un componente electrónico; puede ser, asimismo, un módulo de soporte lógico constituido a partir de un programa encaminado a realizar una función que puede ser un algoritmo, llevándose a la práctica este módulo de soporte lógico en un componente electrónico.

Tales componentes son utilizados especialmente en aplicaciones en las que el acceso a servicios o a datos está fuertemente controlado, tales como las aplicaciones de criptografía.

Tienen una arquitectura llamada lógica, es decir, programable, determinada en torno a un microprocesador y a memorias, entre ellas una memoria de programa no volátil que contiene uno o varios número(s) secreto(s); se trata de una arquitectura no especializada apta para ejecutar cualquier algoritmo. También pueden completarse con una arquitectura llamada física, es decir, que incluye un (o varios) coprocesador(es) dedicado(s) para la ejecución de cálculos específicos o de un solo algoritmo, que presenta la ventaja de ejecutar el algoritmo de manera mucho más rápida que en el caso de una arquitectura lógica.

En el caso, por ejemplo, del algoritmo de criptografía de clave secreta DES, acrónimo anglosajón de "Data Encryption Standard", que puede ser utilizado para cifrar un mensaje, la ejecución es de 1000 a 10 000 veces más rápida cuando está efectuada por un coprocesador.

Estos componentes se utilizan en sistemas informáticos, empotrados o no; se utilizan especialmente en las tarjetas inteligentes, para ciertas aplicaciones de las mismas. Son, por ejemplo, aplicaciones de acceso a ciertos bancos de datos, aplicaciones bancarias, aplicaciones de telepeaje, por ejemplo para la televisión, la distribución de gasolina o también el tránsito de peajes de autopistas.

Por lo tanto, estos componentes o estas tarjetas llevan a la práctica un algoritmo de criptografía para encargarse del cifrado, la autenticación o la firma digital de un mensaje cuando el mismo debe permanecer confidencial.

A partir de este mensaje aplicado como entrada a la tarjeta por un sistema anfitrión (servidor, distribuidor bancario...) y de unos números secretos contenidos en la tarjeta, la tarjeta proporciona de vuelta al sistema anfitrión ese mensaje cifrado, autenticado o firmado, lo cual permite al sistema anfitrión, por ejemplo, autenticar el componente o la tarjeta, intercambiar datos…

Las características de los algoritmos de criptografía pueden ser conocidas: cálculos efectuados, parámetros utilizados. La única incógnita es el o los números secretos. Toda la seguridad de estos algoritmos de criptografía estriba en este(os) número(s) secreto(s) contenido(s) en la tarjeta y desconocido(s) para el mundo exterior a esta tarjeta. Este número secreto no se puede deducir del mero conocimiento del mensaje aplicado como entrada y del mensaje cifrado proporcionado de vuelta.

Ahora bien, se ha puesto de manifiesto que ataques externos basados en magnitudes físicas medibles en el exterior del componente cuando el mismo está desplegando el algoritmo de criptografía permiten a terceros malintencionados encontrar el (los) número(s) secreto(s) contenido(s) en esta tarjeta. Estos ataques se denominan ataques por canal colateral ("Side channel attacks" en inglés); se distinguen, entre estos ataques por canal colateral, los ataques SPA, acrónimo anglosajón para *Single Power Analysis*, basados en una e incluso algunas medidas, y los ataques DPA, acrónimo anglosajón para *Differential Power Analysis*, basados en análisis estadísticos dimanados de numerosas medidas.

El principio de estos ataques por canal colateral reside, por ejemplo, en el hecho de que el consumo de corriente del microprocesador y/o del coprocesador que ejecuta instrucciones varía según la instrucción o el dato manipulado.

Este tipo de ataque es factible especialmente con los algoritmos de criptografía de clave secreta como, por ejemplo, el algoritmo DES, o de clave pública como, por ejemplo, el algoritmo RSA, por el nombre de sus autores (Rivest, Shamir y Adleman).

Ciertos procedimientos de contramedida que permiten hacer frente a los ataques encaminados a obtener la clave secreta consisten en no manipular directamente la clave secreta.

Consiste otra contramedida en aleatorizar temporalmente el consumo de corriente del componente, utilizando el módulo funcional sensible en instantes aleatorios; el atacante, entonces, no puede localizar fácilmente el inicio de la utilización del módulo sensible. Se dice que esta contramedida es no determinista.

También se puede aleatorizar en amplitud el consumo de corriente del componente, activando y luego desactivando diversos elementos de la tarjeta que asimismo consumen corriente. La señal de interés, entonces, se encuentra oculta entre las señales de estos elementos de la tarjeta.

Finalmente, el documento EP 1263163 propone proteger un algoritmo de repetición de rondas en las cuales la introducción de fallos (Differential Fault Attack) puede conducir a una determinación de la clave, introduciendo pares de rondas suplementarias ficticias que utilizan claves falsas y siempre empiezan después del final de una ronda correcta.

La finalidad de la presente invención es, pues, proteger un módulo funcional sensible de una arquitectura lógica y/o física de ataques que intervienen en su ejecución, especialmente de ataques por canal colateral, tales como los ataques DPA.

La invención tiene por objeto un procedimiento de puesta en práctica segura de un módulo funcional, en un componente electrónico, principalmente caracterizado porque consiste, por cada puesta en práctica de dicho módulo, en realizar, en un orden aleatorio, m ejecuciones correctas y n ejecuciones ficticias de dicho módulo, siendo m y n enteros positivos no nulos, comenzando cada una de las m + n ejecuciones en un instante aleatorio.

Ventajosamente, $m < n$.

De acuerdo con una forma preferente de realización de la invención, las n ejecuciones ficticias son idénticas.

De acuerdo con una característica de la invención, las n ejecuciones ficticias se determinan en función de la ejecución correcta.

De acuerdo con una característica adicional de la invención, el número P de puestas en práctica de las m + n ejecuciones del módulo es limitado.

De acuerdo con otra característica de la invención, las m + n ejecuciones del módulo funcional son de código constante y de tiempo constante.

De acuerdo con una forma de realización de la invención, comprendiendo el componente elementos consumidores de corriente, uno o varios de estos elementos son activados y luego desactivados en orden a aleatorizar el consumo de corriente del componente.

El módulo funcional puede tener por función un algoritmo de criptografía.

De acuerdo con una forma de realización de la invención, el algoritmo de criptografía utiliza una clave K y cada una de las m ejecuciones correctas consiste en ejecutar dicho algoritmo utilizando la clave K y cada una de las n ejecuciones ficticias consiste en ejecutar dicho algoritmo utilizando respectivamente una clave falsa K'_1, ..., K'_n.

Las claves falsas son preferentemente idénticas, $K'_1 = ... = K'_n = K'$.

La invención tiene asimismo por objeto un componente electrónico que incluye unos medios de puesta en práctica segura de un módulo funcional tales y como se han descrito anteriormente.

Incluye, ventajosamente, un coprocesador dedicado a la puesta en práctica del módulo funcional.

La invención concierne también a una tarjeta inteligente que incluye un componente electrónico tal y como está descrito.

El procedimiento según la invención está encaminado a proteger un módulo funcional de ataques que intervienen en su ejecución, especialmente de los ataques por canal colateral tales como los ataques DPA.

Cuando la función del módulo funcional es un algoritmo, éste puede ser un algoritmo de verificación del código "PIN" a través de un terminal, o un algoritmo de criptografía, como por ejemplo el algoritmo DES.

Más adelante en la descripción, se va a considerar más en particular, como módulo funcional, un módulo físico dedicado a la ejecución de un algoritmo de criptografía de tipo DES; estará designado, en lo que sigue, por DES.

A partir del mensaje M proporcionado como entrada al módulo físico, en el caso concreto que nos ocupa, un coprocesador designado por "CoDES", éste proporciona a su salida el mensaje MC cifrado por medio de una clave secreta K.

De acuerdo con la invención, cada vez que se debe llevar a la práctica el DES, se ejecuta el DES varias veces, en un orden aleatorio, m veces de manera correcta, es decir, utilizando la clave secreta K, y n veces de manera ficticia, utilizando claves falsas K'_1, K'_2, ..., K'_n en orden a engañar a un atacante.

A partir de una arquitectura física, una ejecución del DES es muy rápida: ésta se puede repetir entonces varias veces, por ejemplo 8 veces, sin que ello sea realmente gravoso.

Se elige preferentemente m << n, por ejemplo, m = 1 y n = 7.

Ejecutar el DES m + n veces en un orden aleatorio significa que, por cada ejecución del DES, la clave se elige de manera aleatoria de entre las claves restantes, es decir, de entre las claves que aún no se hayan utilizado. Como se verá más adelante para diversas formas de realización de la invención, el orden aleatorio también puede consistir en elegir la primera clave de manera aleatoria, estando determinada la elección de las claves siguientes, o también en determinar una secuencia aleatoria.

De acuerdo con una forma de realización de la invención, las claves verdadera y falsas K, K'_1, ..., K'_7 se almacenan en una tabla Claves y se indican con un índice i que varía de 0 a 7, y los resultados correspondientes a cada una de las claves se almacenan en una tabla Res en una ubicación indicada, por ejemplo, con el mismo índice i.

El índice de la primera clave se elige de manera aleatoria. La primera clave tiene, por ejemplo, el índice 2; se trata, por tanto, de K'_2. El DES se ejecuta entonces una primera vez con esta primera clave K'_2 para cifrar, por ejemplo, el mensaje M, y el resultado obtenido R_2 se almacena en la tabla Res en el índice 2. A continuación, se ejecuta el DES con la siguiente clave, la clave K'_3 para cifrar el mensaje M, y el resultado R_3 se almacena en la tabla Res en el índice 3, etc. La 7ª ejecución del DES se efectúa con la clave K'_1 para cifrar el mensaje M, y la última, con la clave K.

La ubicación del debido resultado R en la tabla Res que corresponde a aquella de la debida clave en la tabla Claves se conoce de antemano: en nuestro ejemplo, se trata de la ubicación indicada con el índice 1. Pero, naturalmente, no se conoce el instante en que se almacena este resultado R.

Cuando las claves falsas son diferentes, como ocurre en la forma de realización que se acaba de describir, las señales de consumo de corriente que les corresponden difícilmente son localizables: cada una de estas señales son prácticamente equivalentes, pues tienen, en cierto modo, el mismo peso. Pero no constituyen un engaño frente a ataques de tipo DPA.

Esta es la razón por la que, de acuerdo con otra forma de realización preferente de la invención, las n utilizaciones ficticias son idénticas, es decir, las claves falsas K'_1, K'_2, ..., K'_n son idénticas e iguales a K'.

De este modo, en el caso de ataques estadísticos tales como los ataques DPA, la señal correspondiente a la clave K' es más marcada (n veces) que la correspondiente a la clave K; la señal correspondiente a la clave verdadera K está inmersa en el ruido de cálculo de aquella de la clave falsa K'.

En este caso, la tabla Claves no incluye más que dos claves, la clave verdadera K y la clave falsa K'. Igualmente, la tabla Res no incluye más que dos resultados. Asimismo, el DES se ejecuta 8 veces, 7 veces con la clave falsa y una vez con la clave verdadera.

Cuando la clave K está indicada con el índice 0, y la clave K', con el índice 1, la elección aleatoria de las claves puede obtenerse de la siguiente manera. Se elige un número aleatorio de 8 bits que incluye 7 bits en 1 y un bit en cero, por ejemplo, 11101111. Las tres primeras y cuatro últimas ejecuciones del DES se efectúan con la clave indicada con el índice 1, es decir, la clave falsa, y la cuarta ejecución se efectúa con la clave verdadera, indicada con el índice 0.

Se pueden realizar otras variantes, como por ejemplo aquella que consiste en que algunas claves falsas sean idénticas, en tanto que las otras claves falsas difieran unas de otras.

Por otro lado, de acuerdo con una forma particular de realización, el algoritmo de criptografía es de código constante y de tiempo constante, es decir, que siempre ejecuta las mismas instrucciones y que los datos manejados no interactúan en la duración del algoritmo.

Adicionalmente, entre una vez y otra, es decir, entre una puesta en práctica de las m + n ejecuciones y otra, el orden de las ejecuciones correctas y ficticias es aleatorio. Cuando m = 1; en una primera puesta en práctica de las n + 1 DES, que comienza en el tiempo t_1, la ejecución correcta (con la clave K) tiene lugar en 3ª posición, siendo las otras n ejecuciones, ejecuciones ficticias con las claves falsas K'_1, K'_2, ..., K'_n (eventualmente iguales a K'); en la segunda puesta en práctica de las n + 1 DES, que comienza en el tiempo t_2, la ejecución correcta (con la clave K) tiene lugar en 1ª posición, siendo las otras n ejecuciones, ejecuciones ficticias con las claves falsas K'_1, K'_2, ..., K'_n (eventualmente iguales a K'); ...; en la P-ésima puesta en práctica de las n + 1 DES, que comienza en el tiempo t_P, la ejecución correcta (con la clave K) tiene lugar en 2ª posición, siendo las otras n ejecuciones, ejecuciones ficticias con las claves falsas K'_1, K'_2, ..., K'_n (eventualmente iguales a K').

Ventajosamente, se limita el número P de puestas en práctica de las m + n ejecuciones del DES en orden a contrarrestar los intentos del atacante, los cuales, en el caso de un ataque de tipo DPA, consistirían en aumentar el número de adquisiciones de señales.

De acuerdo con una forma preferente de realización, las claves falsas K'_1, K'_2, ..., K'_n (eventualmente iguales a K') se determinan en función de la clave verdadera K. Cuando se cambia la clave K, se regeneran las claves falsas K'_1, K'_2, ..., K'_n (eventualmente iguales a K').

Las claves falsas K'_1, K'_2, ..., K'_n (eventualmente iguales a K') generalmente están almacenadas en memoria, como se ha visto en los ejemplos de realización anteriores; no obstante, pueden ser recalculadas o sacadas al azar entre una vez y otra.

Cuando m > 1, por ejemplo, m = 2, es posible comparar los m resultados correctos obtenidos con el fin de detectar un ataque por fallo, es decir, en el caso de un error inyectado. Se trata, entonces, de detectar un ataque por fallo protegiéndose al propio tiempo de los ataques por canal colateral.

De acuerdo con otra forma de realización, se agrega una aleatorización temporal del consumo de corriente del componente, utilizando el DES en instantes aleatorios y/o se agrega una aleatorización en amplitud, activando y luego desactivando diversos elementos de la tarjeta que también consumen corriente.

REIVINDICACIONES

1. Procedimiento de puesta en práctica segura de un módulo funcional, que tiene por función un algoritmo de criptografía, en un componente electrónico, utilizando el algoritmo de criptografía una clave K, y que consiste, por cada puesta en práctica de dicho módulo, en realizar, en un orden aleatorio,

- m ejecuciones correctas de dicho módulo, consistiendo cada ejecución correcta en ejecutar dicho algoritmo utilizando dicha clave K, y

- n ejecuciones ficticias de dicho módulo, consistiendo cada ejecución ficticia en ejecutar dicho algoritmo utilizando respectivamente una clave falsa K'_1, ..., K'_n,

siendo m y n enteros positivos no nulos,

y caracterizado por que dichas m + n ejecuciones comienzan cada una de ellas en un instante aleatorio.

2. Procedimiento según la reivindicación anterior, caracterizado por que m < n.

3. Procedimiento según una cualquiera de las reivindicaciones anteriores, caracterizado por que las n ejecuciones ficticias son idénticas.

4. Procedimiento según una cualquiera de las reivindicaciones anteriores, caracterizado por que las n ejecuciones ficticias se determinan en función de la ejecución correcta.

5. Procedimiento según una cualquiera de las reivindicaciones anteriores, caracterizado por que el número P de puestas en práctica de las m + n ejecuciones de dicho módulo es limitado.

6. Procedimiento según la reivindicación anterior, caracterizado por que las m + n ejecuciones de dicho módulo funcional son de código constante y de tiempo constante.

7. Procedimiento según una cualquiera de las reivindicaciones anteriores, caracterizado por que, comprendiendo dicho componente elementos consumidores de corriente, uno o varios de dichos elementos son activados y luego desactivados en orden a aleatorizar el consumo de corriente del componente.

8. Procedimiento según la reivindicación 1, caracterizado por que las claves falsas son idénticas, $K'_1 = ... = K'_n = K'$.

9. Componente electrónico que incluye unos medios de puesta en práctica segura de un módulo funcional según una cualquiera de las reivindicaciones anteriores.

10. Componente electrónico según la reivindicación anterior, caracterizado por incluir un coprocesador dedicado a la puesta en práctica de dicho módulo funcional.

11. Tarjeta inteligente que incluye un componente electrónico según una cualquiera de las reivindicaciones 9 ó 10.