(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 287 014**

(51) Int. Cl.:
H04L 9/12 (2006.01)
H04L 9/26 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **00927228 .7**
(86) Fecha de presentación : **19.05.2000**
(87) Número de publicación de la solicitud: **1201056**
(87) Fecha de publicación de la solicitud: **02.05.2002**

(54) Título: **Método para proteger una tarjeta portátil.**

(30) Prioridad: **13.07.1999 NL 1012581**

(45) Fecha de publicación de la mención BOPI:
16.12.2007

(45) Fecha de la publicación del folleto de la patente:
16.12.2007

(73) Titular/es: **Nokia Corporation**
Keilalahdentie 4
02150 Espoo, FI

(72) Inventor/es: **Muller, Frank y**
Roelofsen, Gerrit

(74) Agente: **Curell Suñol, Marcelino**

DESCRIPCIÓN

Método para proteger una tarjeta portátil.

La presente invención se refiere a un método para proteger una tarjeta portátil, provista de por lo menos un criptoalgoritmo para cifrar datos y/o autenticar la tarjeta, contra la obtención de la clave secreta usada, a partir del análisis estadístico de su información que se filtra al mundo exterior en el caso de operaciones criptográficas, tal como datos de consumo de potencia, radiación electromagnética y similares, estando provista la tarjeta de por lo menos un registro de desplazamiento que tiene una función de realimentación lineal y no lineal para crear algoritmos criptográficos, comprendiendo el método la carga de datos a procesar y de una clave secreta en el registro de desplazamiento de la tarjeta.

El uso de una clave secreta para procesar información de entrada y/o para producir información de salida es conocido en general en el caso de los dispositivos criptográficos. El uso de registros de desplazamiento de realimentación también es conocido en general para crear algoritmos criptográficos.

En relación con esto, en uno o más registros de desplazamiento se cargan datos que se van a procesar de forma consecutiva y una clave secreta. En este caso, la secuencia de carga de datos y de la clave es aleatoria.

Subsiguientemente, se aplican la salida del registro de desplazamiento y posiblemente el contenido del registro de desplazamiento, usando una realimentación lineal y/o no lineal, para determinar la salida del algoritmo completo. En este caso, la entrada del registro de desplazamiento, aparte de los datos y la clave, consta también de una combinación lineal y no lineal del contenido del registro de desplazamiento.

En general, dichos registros de desplazamiento se aplican en el caso de tarjetas portátiles, tales como tarjetas chip, tarjetas telefónicas, productos de tarjeta inteligente y similares.

Como la clave secreta no es conocida para terceras partes no autorizadas, básicamente resulta imposible obtener bien la entrada o bien la clave a partir de la salida del algoritmo.

El documento DE 19622533 da a conocer un método para cargar datos de entrada en un algoritmo durante la autenticación entre tarjetas chip en el cual se usa un registro de desplazamiento de realimentación lineal para el algoritmo de autenticación y la función no lineal de dicho registro de desplazamiento se refuerza criptográficamente en combinación con contadores situados después según el sentido de avance.

No obstante, en la actualidad se ha puesto de manifiesto que, para tarjetas chip y similares, es posible, en el caso de cálculos, obtener la clave secreta usada a partir de un análisis estadístico del consumo de potencia de la tarjeta. Dichos métodos se conocen como "Análisis Diferencial de Consumo" (= DPA) y se describen en la publicación de Internet Información Técnica del DPA: "Introduction to Differential Power Analysis and Related Attacks" de P. Kocher *et al*., Cryptography Research, San Francisco, 1998.

Dichos métodos se basan en el hecho de que, en la práctica, con operaciones criptográficas, se filtra al mundo exterior información en forma de datos de consumo de potencia, radiación electromagnética y similares.

De este modo, las unidades lógicas del microprocesador presentan patrones regulares de conmutación de transistores que producen de forma perceptible externamente (es decir, al exterior del microprocesador) una actividad eléctrica.

De esta manera, es posible identificar macrocaracterísticas, tales como la actividad de los microprocesadores, registrando el consumo de potencia y obteniendo información sobre la clave secreta usada por medio de un análisis estadístico de los datos obtenidos de esta manera.

Llegado este momento, la invención supera dicho inconveniente y proporciona una tarjeta portátil la cual es resistente a dichos análisis y por lo tanto proporciona una tarjeta segura en cuanto a su uso.

El método según la invención está caracterizado porque se aplica un algoritmo a la tarjeta el cual se construye de tal manera que la recogida de valores de señales registradas de información filtrada es resistente a la obtención de la clave secreta a través del análisis estadístico de dichos valores. De forma ventajosa, después de cargar la clave en el registro de desplazamiento, el registro de desplazamiento se activa subsiguientemente mediante impulsos de reloj, durante un periodo específico de tiempo, varias veces, por lo menos haciendo uso de la función de realimentación lineal.

Una de las alternativas adecuadas según la invención consiste en cargar únicamente la clave en el registro de desplazamiento en el caso de un contenido fijo del registro de desplazamiento.

En una primera forma de realización ventajosa de la invención, en primer lugar se carga la clave, subsiguientemente se realiza la activación mediante impulsos de reloj, después de lo cual se cargan los datos. En otra forma de realización ventajosa de la invención, en primer lugar se carga la clave, subsiguientemente se cargan los datos en el registro de desplazamiento, haciendo uso exclusivo de la función de realimentación lineal y subsiguientemente se realiza la activación mediante impulsos de reloj.

Todavía en otra de las formas de realización ventajosas de la invención, en primer lugar se cargan los datos, subsiguientemente se carga la clave, haciendo uso exclusivo de la función de realimentación lineal, tras lo cual se realiza la activación mediante impulsos de reloj.

A continuación se explicará más detalladamente la invención haciendo referencia a los dibujos y a la descripción a título de ejemplo no limitativo.

La Fig. 1 muestra esquemáticamente un registro de desplazamiento típico como el que se aplica con una tarjeta portátil, tal como una tarjeta chip y similares.

La Fig. 2 muestra esquemáticamente una solución ventajosa según la invención, y

la Fig. 3 muestra esquemáticamente otra solución ventajosa según la invención.

Haciendo referencia a continuación a la Fig. 1, se muestra un registro de desplazamiento de realimentación 1, el cual se aplica, según cualquier forma adecuada para el fin deseado, a una tarjeta portátil, no mostrada en aras de una mayor simplicidad, tal como una tarjeta chip, una tarjeta telefónica y similares, que tiene una entrada 2 y una salida 3.

El registro de desplazamiento de realimentación 1 comprende un registro de desplazamiento 1a, así como una función de realimentación, la cual en este caso consta de una función lineal 1b y una función no

lineal 1c que tiene una salida 3a. Dicho registro de desplazamiento de realimentación, gracias a sus costes relativamente reducidos, es apto para aplicarse a, por ejemplo, tarjetas telefónicas y similares. La función no lineal se puede ocupar de dicha situación de manera que cada bit depende de cada número de bits de la clave.

Los registros de desplazamiento son en general conocidos y por lo tanto su funcionamiento no se describirá de forma detallada. El registro de desplazamiento 1a consta de una serie de bits. La longitud de un registro de desplazamiento se expresa en bits; en el caso de una longitud de n bits, al mismo se le denomina registro de desplazamiento de n bits.

Cada vez que se requiere un bit, todos los bits del registro de desplazamiento se desplazan 1 bit hacia la derecha. El nuevo bit de la izquierda se calcula como una función de los bits que quedan en el registro y de la entrada.

La salida del registro de desplazamiento es 1 bit, con frecuencia el bit menos significativo. El periodo de un registro de desplazamiento es la longitud de la serie de salida antes de que comience la repetición.

Los datos se cargan por medio de la entrada 2; se carga la clave, y se producen resultados por medio de la salida 3 ó, si así se desea, 3a. No obstante, en una situación similar, se puede efectuar un ataque sobre la clave secreta usada, por medio del DPA, basándose en las variaciones de potencia del sistema en el caso de cálculos a través de un análisis estadístico de "datos filtrados" y técnicas de corrección de errores.

En relación con esto, debería indicarse que, desde el punto de vista de la seguridad, es deseable cargar la clave y los datos de forma no lineal en el registro de desplazamiento. No obstante, se ha puesto de manifiesto que en el caso de cálculos, la carga no lineal de la clave y los datos en el registro de desplazamiento hace que aumente la posibilidad de obtener la clave secreta usada a través del análisis estadístico del consumo de potencia.

En la Fig. 2 y la Fig. 3, las mismas referencias numéricas que las usadas en la Fig. 1 hacen referencia a los mismos componentes.

La Fig. 2 muestra en este caso una forma de realización ventajosa de la invención, cargándose en primer lugar la clave en el registro de desplazamiento, cargándose subsiguientemente datos, por lo menos de forma inicial, exclusivamente usando la función de realimentación lineal, y a continuación efectuando la activación mediante impulsos de reloj (por ejemplo, 100 veces o más) del registro de desplazamiento. Durante la carga de los datos y, si así se desea, la subsiguiente activación mediante impulsos de reloj, se desactiva la función no lineal del registro de desplazamiento hasta que se haya activado suficientemente mediante impulsos de reloj dicho registro de desplazamiento. A continuación, se pone en marcha una vez más nuevamente la función no lineal.

Al realizar esto, la función de realimentación lineal 1b continúa estando activa.

La desactivación y activación, según sea el caso, de la función no lineal 1c puede tener lugar de cualquier manera adecuada para el fin deseado, por ejemplo, usando conmutadores.

El registro de desplazamiento 1a se activa de forma ventajosa mediante impulsos de reloj un número tal de veces que el contenido de todos los elementos del registro de desplazamiento dependa de gran parte de los bits de la clave.

En otra de las formas de realización ventajosas, después de cargar la clave se realiza en primer lugar una activación mediante impulsos de reloj hasta que el contenido de todos los elementos del registro de desplazamiento dependa de gran parte de los bits de la clave. Únicamente después de dicha activación mediante impulsos de reloj, se permite la carga de los datos en el registro de desplazamiento 1a y se permite también la realización de operaciones no lineales sobre el contenido del registro de desplazamiento.

La activación mediante impulsos de reloj tiene lugar de cualquiera de las maneras conocidas para aquellos expertos en la materia y por lo tanto no se explicará más detalladamente.

Para completar adicionalmente la explicación, debería indicarse que el DPA únicamente puede llevarse a cabo si tiene lugar una operación no lineal de los datos con la clave. Como, adicionalmente, el esfuerzo requerido para el DPA aumenta exponencialmente con el número de bits de la clave del cual dependen los bits del registro de desplazamiento, el mismo se realiza de tal manera que, en el caso de una activación provisional suficiente del registro de desplazamiento 1a mediante impulsos de reloj, la aplicación del DPA no ofrece un resultado satisfactorio a corto plazo.

En la Fig. 3, se muestra una variante ventajosa de la invención, habiéndose cargado la clave con un contenido fijo del registro de desplazamiento (el cual también puede consistir puramente en ceros) y teniendo lugar la activación del registro de desplazamiento mediante impulsos de reloj con una función de realimentación lineal activa y no lineal activa, aunque sin cargarse datos en el registro de desplazamiento durante el periodo de activación mediante impulsos de reloj. Al efectuar esta operación, la entrada de datos al registro de desplazamiento después de cargar la clave se desconecta del registro de desplazamiento y se vuelve a restablecer después de un periodo específico de activación mediante impulsos de reloj. Debido al contenido fijo del registro de desplazamiento, no se permite aplicar ninguna modificación y una tercera parte no autorizada no será capaz de determinar una recogida de diferentes valores de datos filtrados, tales como consumo de potencia, y no podrá someterlos a un análisis estadístico para recuperar la clave.

En esta solución según la invención, la clave, por lo tanto, se puede cargar de forma no lineal, y no será necesaria una desactivación de la función de realimentación no lineal.

En otra de las formas de realización ventajosas de la invención, en el caso de que la clave, después de se hayan cargado datos en el registro de desplazamiento, no se cargue con el contenido fijo del registro de desplazamiento, la clave se carga en el registro de desplazamiento usando únicamente la función de realimentación lineal, después de lo cual se permite que tenga lugar una activación subsiguiente mediante impulsos de reloj.

Después de la descripción expuesta anteriormente, para los expertos en la materia se pondrán de manifiesto varias modificaciones del método según la invención.

Se considerará que dichas modificaciones quedan comprendidas dentro del alcance de la invención.

REIVINDICACIONES

1. Método para proteger una tarjeta portátil provista de por lo menos un algoritmo criptográfico para cifrar datos y/o autenticar la tarjeta, contra la obtención de la clave secreta usada, a partir del análisis estadístico de su información que se filtra al mundo exterior en el caso de operaciones criptográficas, tal como datos de consumo de potencia, radiación electromagnética y similares, estando provista la tarjeta de por lo menos un registro de desplazamiento (1, 1a) que tiene una función de realimentación lineal (1b) y no lineal (1c) para crear algoritmos criptográficos, comprendiendo el método la carga de datos que se deben procesar y de una clave secreta en el registro de desplazamiento (1, 1a) de la tarjeta, **caracterizado** porque la clave secreta se carga usando únicamente la función de realimentación lineal (1b), o porque los datos se cargan usando únicamente la función de realimentación lineal (1b).

2. Método para proteger una tarjeta portátil provista de por lo menos un algoritmo criptográfico para cifrar datos y/o autenticar la tarjeta, contra la obtención de la clave secreta usada, a partir del análisis estadístico de su información que se filtra al mundo exterior en el caso de operaciones criptográficas, tal como datos de consumo de potencia, radiación electromagnética y similares, estando provista la tarjeta de por lo menos un registro de desplazamiento (1, 1a) que tiene una función de realimentación lineal (1b) y no lineal (1c) para crear algoritmos criptográficos, comprendiendo el método la carga de datos que se deben procesar y de una clave secreta en el registro de desplazamiento (1, 1a) de la tarjeta, **caracterizado** porque la clave secreta se carga en el registro de desplazamiento (1, 1a) con un contenido fijo del registro de desplazamiento (1, 1a).

3. Método según la reivindicación 1 ó 2, **caracterizado** porque, después de que la clave se ha cargado en el registro de desplazamiento (1, 1a), el registro de desplazamiento (1, 1a), durante un periodo específico, se activa mediante impulsos de reloj varias veces, por lo menos usando la función de realimentación lineal (1b), y porque subsiguientemente los datos se cargan usando únicamente la función de realimentación lineal (1b) y el registro de desplazamiento (1, 1a) se activa subsiguientemente mediante impulsos de reloj.

4. Método según la reivindicación 3, **caracterizado** porque durante la primera materialización de la activación mediante impulsos de reloj, el registro de desplazamiento (1, 1a) se activa mediante impulsos de reloj durante un tiempo tal que el contenido de todos los elementos del registro de desplazamiento (1, 1a) depende en gran parte de los bits de la clave.

5. Método según la reivindicación 1 ó 2, **caracterizado** porque, después de que la clave se ha cargado en el registro de desplazamiento (1, 1a), el registro de desplazamiento (1, 1a), durante un periodo específico, se activa mediante impulsos de reloj varias veces, y porque la activación mediante impulsos de reloj del registro de desplazamiento (1, 1a) tiene lugar con una función de realimentación lineal activa (1b) y no lineal activa (1c) del registro de desplazamiento (1, 1a), aunque, durante, o antes del periodo de activación mediante impulsos de reloj o antes de la carga de la clave no se cargan datos en el registro de desplazamiento (1, 1a).

6. Método según cualquiera de las reivindicaciones anteriores, **caracterizado** porque la entrada de datos al registro de desplazamiento (1, 1a) después de la carga de la clave en el registro de desplazamiento (1, 1a) se desconecta del registro de desplazamiento (1, 1a) y se restablece después del periodo específico mencionado anteriormente.

7. Método según cualquiera de las reivindicaciones anteriores, **caracterizado** porque, si la clave no se carga con un contenido fijo del registro de desplazamiento (1, 1a), la clave se carga en el registro de desplazamiento usando únicamente la función de realimentación lineal (1b), después de lo cual tiene lugar la activación mediante impulsos de reloj.

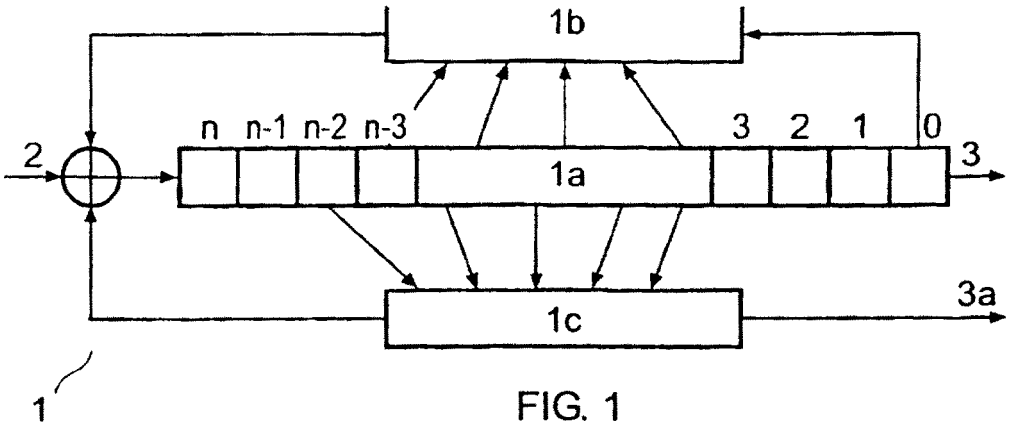

FIG. 1

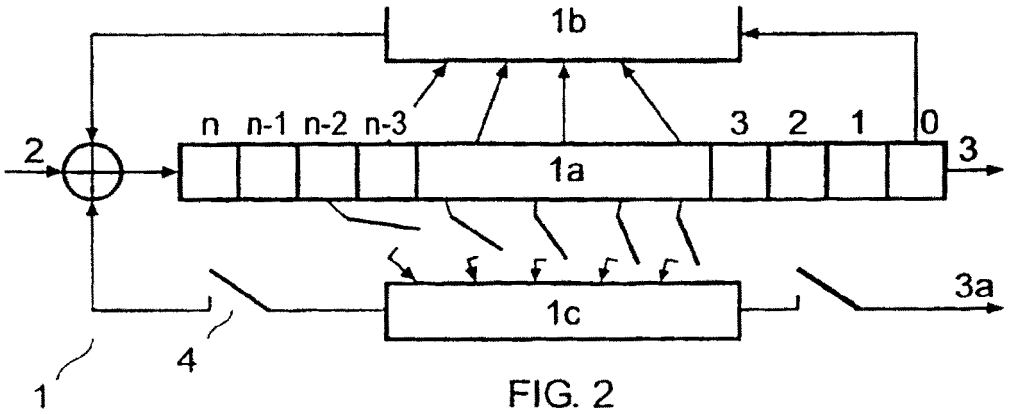

FIG. 2

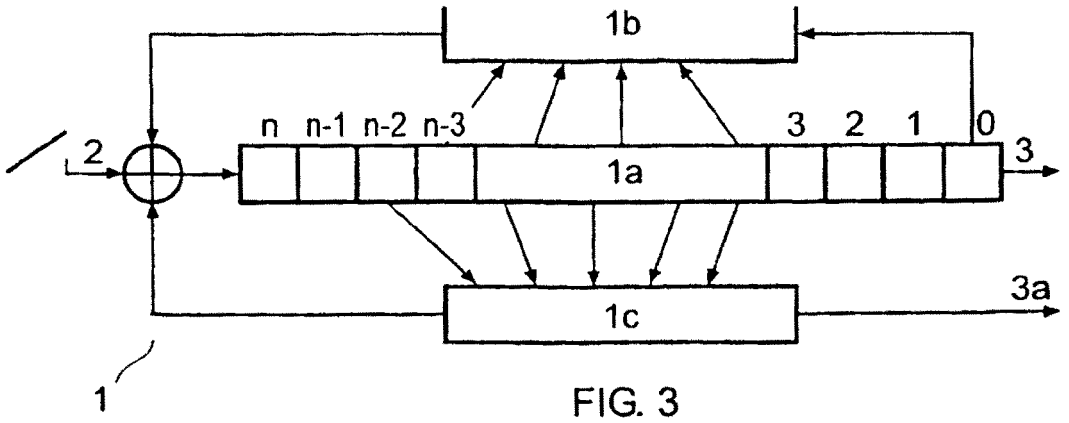

FIG. 3