(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 269 823**

(51) Int. Cl.:
G06K 7/00 (2006.01)
G06K 19/07 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **02804606 .8**
(86) Fecha de presentación : **11.12.2002**
(87) Número de publicación de la solicitud: **1485857**
(87) Fecha de publicación de la solicitud: **15.12.2004**

(54) Título: **Componente electrónico digital protegido contra análisis de tipo eléctrico.**

(30) Prioridad: **13.12.2001 FR 01 16114**

(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: **NAGRA THOMSON LICENSING**
46 quai Alphonse Le Gallo
92100 Boulogne-Billancourt, FR

(72) Inventor/es: **Dauvois, Jean-Luc y**
Perrine, Jérôme

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Componente electrónico digital protegido contra análisis de tipo eléctico.

Campo técnico

El presente invento se refiere a un componente electrónico numérico protegido contra análisis de tipo eléctrico y/o electromagnético, especialmente en el campo de la tarjeta inteligente.

Estado de la técnica anterior

El campo del invento es el de la puesta en práctica en un componente electrónico numérico, por ejemplo una tarjeta inteligente, de mecanismos para luchar contra extracciones de datos (generalmente una clave de cifrado) por un análisis del consumo de corriente, o por un análisis de la radiación electromagnética emitida. Generalmente estos análisis se denominan SPA ("Simple Power Analysis")/DPA ("Differential Power Analysis") o SEMA ("Simple Electrical Magnetic Analysis")/DEMA ("Differential Electrical Magnetic Analysis").

Con la ayuda de estos análisis se llega a determinar lo que hace la unidad central de una tarjeta inteligente, cuáles son los datos manipulados por ella. Se puede también tener acceso a la o las claves secretas utilizadas para la transmisión de estos datos. Tal intrusión se realiza sin riesgo alguno, pues no será posible, posteriormente, probar que se ha producido, puesto que el componente permanece íntegro.

Como se ha descrito en el artículo de Paul Kocher, Joshua Jaffe y Benjamin Jun titulado "Introduction to differential power analysis and related attack" (sitio Internet: www.cryptography.com, Cryptography Research, 1998), estas técnicas de análisis pueden tener consecuencias importantes, puesto que permiten extraer claves secretas utilizadas para las comunicaciones encriptadas. Además, tales ataques pueden ser preparados rápidamente y puestos en práctica utilizando material fácilmente disponible. La cantidad de tiempo requerido para realizarlos depende del tipo de ataque (DPA, SPA) y varía en función del componente considerado. Un ataque SPA puede llevar algunos segundos por componente mientras que un ataque DPA puede llevar varias horas.

En la actualidad, las electrónicas numéricas están poco o nada protegidas contra tales análisis eléctricos o electromagnéticos. Existen dos grupos de protección: uno es puramente informático (o "software"), el otro es puramente material (o "hardware"). En el caso de datos manipulados por la unidad central de una tarjeta inteligente:

- en el primer grupo, una solución técnica consiste en hacer el consumo de corriente lo más aleatorio posible, estando este consumo de corriente ligado lo menos posible con los datos manipulados por la unidad central. Así se puede hacer aleatorio el desarrollo de las instrucciones, o hacer también lo más aleatorio posible los datos manipulados.
- en el segundo grupo se puede:
  - bien hacer también la corriente lo más uniforme posible, de forma que sea muy difícil establecer una correspondencia entre el consumo de corriente y las instrucciones manipuladas por la unidad central,
  - bien hacer aleatorio el consumo de corriente, de forma que se desincronicen dos funcionamientos idénticos de la unidad central.

En este segundo caso es en el que se sitúa el invento.

Una solicitud de patente europea EP 1.113.386 describe una solución para proteger una tarjeta inteligente contra tales ataques. En esta solución, dos condensadores están incluidos en la tarjeta inteligente, de tal forma que no depende del momento en que uno de los dos sea cargado por una alimentación de energía externa y el otro sea descargado accionando el componente de la tarjeta inteligente. Las tareas de los dos condensadores alternan rápidamente y la alimentación de energía se aísla del componente de la tarjeta inteligente en el sentido en que los análisis del consumo de corriente no dan información sobre el funcionamiento de este componente.

El objeto del invento es resolver el problema expuesto anteriormente haciendo variar de forma aleatoria la velocidad de funcionamiento de un componente electrónico numérico considerado, por ejemplo una tarjeta inteligente, de forma que los análisis SPA/DPA y/o SEMA/DEMA resulten difíciles, incluso imposibles.

Explicación del invento

El invento tiene como objeto un componente electrónico protegido contra análisis de tipo eléctrico y/o electromagnético que comprende un elemento síncrono gobernado por un reloj, caracterizado porque comprende medios de generación de este reloj, cuya frecuencia varía de forma aleatoria entre un valor mínimo y un valor máximo durante al menos un período de tiempo dado, y medios de control del carácter aleatorio del cambio de frecuencia del reloj.

Estos medios de generación de un reloj pueden comprender un generador de consigna de frecuencia aleatoria que manda un generador de frecuencia.

El generador de frecuencia puede comprender al menos dos sintetizadores de frecuencia, o circuitos PLL ("Phase Locked Loop"), y medios de conmutación entre estos sintetizadores, o circuitos.

El elemento síncrono puede ser la unidad central de una tarjeta inteligente, una memoria, o una función cableada síncrona, por ejemplo de tipo FPGA ("Field Programmable Gate Arrays") o ASIC ("Application Specific Integrated Circuit").

El campo de variación de frecuencias debe ser lo más amplio posible para perturbar al máximo los análisis de tipo DPA/SPA y DEMA/SEMA. La incertidumbre considerada es una incertidumbre verdadera, pues no se trata aquí de una desviación de fase o de frecuencia del reloj, sino de un cambio aleatorio de frecuencia gobernado. Perturbando así el reloj se hace aleatorio el consumo de corriente del elemento síncrono.

Breve descripción de los dibujos

La única figura ilustra un componente electrónico numérico protegido contra ataques de tipo eléctrico y/o electromagnético según el invento.

Explicación detallada de modos de realización particulares

Como se ha ilustrado en la figura, el componen-

te electrónico numérico protegido contra ataques de tipo eléctrico y/o electromagnético según el invento, por ejemplo de una tarjeta inteligente, comprende:

- una unidad central 10 de esta tarjeta inteligente,
- un generador de una consigna de frecuencia aleatoria 11,
- un generador de frecuencia 12, gobernado por este generador 10, que suministra a esta unidad central 10 un reloj H, cuya frecuencia varía de forma aleatoria entre un valor mínimo y un valor máximo,
- un controlador 13 que tiene por objeto medir la frecuencia del reloj H y de verificar el funcionamiento realmente aleatorio del cambio de frecuencia.

La variación de frecuencia del reloj H, que es lo más amplia posible, está comprendida entre 1 MHz y 100 MHz.

En el ejemplo de realización ilustrado en la figura, el generador de frecuencia 12 comprende al menos dos sintetizadores de frecuencia SF1...SFn mandados por señales que proceden de las salidas 15 del controlador 13, y un circuito 20 de multiplexación y de sincronización que recibe las salidas F1...Fn de estos sintetizadores SF1...SFn.

Durante un cambio de frecuencia, antes de seleccionar una de las frecuencias en la salida de los sintetizadores SF1...SFn enviando una señal SEL en el circuito 20 de multiplexación y de sincronización, el controlador 13 verifica que no existen perturbaciones posibles analizando las señales recibidas en las entradas 16.

El controlador 13 puede así funcionar de la siguiente forma:

- petición, al generador de una consigna de frecuencia aleatoria 11, de un nuevo valor,
- valor suministrado por este generador 11 al controlador 13,
- verificación por el controlador 13 del carácter aleatorio de este valor con respecto a los valores precedentes,
- envío de este valor a los sintetizadores SF1...SFn.

El invento permite hacer aleatorio el funcionamiento de la unidad central, que realiza los cálculos, y dar una apariencia de consumo aleatorio de la corriente. Los análisis SPA/DPA y/o SEMA/DEMA son difíciles e incluso imposibles de realizar, pues necesitan un importante aumento del número de análisis de corriente.

El invento permite no modificar la unidad central en sí, lo que permite hacerla funcionar en su propia gama de frecuencias.

La propiedad del invento de protegerse depende del generador de consigna de frecuencia aleatoria y del ciclo de cambio de frecuencia en función de la duración de un ciclo de instrucción de la unidad central.

En un modo de realización ventajoso, el controlador puede ser gobernado por la unidad central.

En una variante de funcionamiento se puede no activar el cambio aleatorio de la frecuencia del reloj H según el invento más que durante un período de tiempo dado en casos considerados como críticos.

REIVINDICACIONES

1. Componente electrónico numérico protegido contra análisis de tipo eléctrico y/o electromagnético, que comprenden un elemento síncrono (10) gobernado por un reloj (H), **caracterizado** porque comprende un generador de consigna de frecuencia aleatoria (11) que manda un generador de frecuencia (12) que suministra este reloj (H), cuya frecuencia varía de forma aleatoria entre un valor mínimo y un valor máximo durante al menos un período de tiempo dado, y medios (13) de control del carácter aleatorio del cambio de frecuencia de este reloj (H).

2. Componente según la reivindicación 1, en el cual el generador de frecuencia comprende al menos dos sintetizadores de frecuencia (SF1...SFn) y medios de conmutación (20).

3. Componente según la reivindicación 1, en el cual el generador de frecuencia comprende al menos dos circuitos PLL y medios de conmutación.

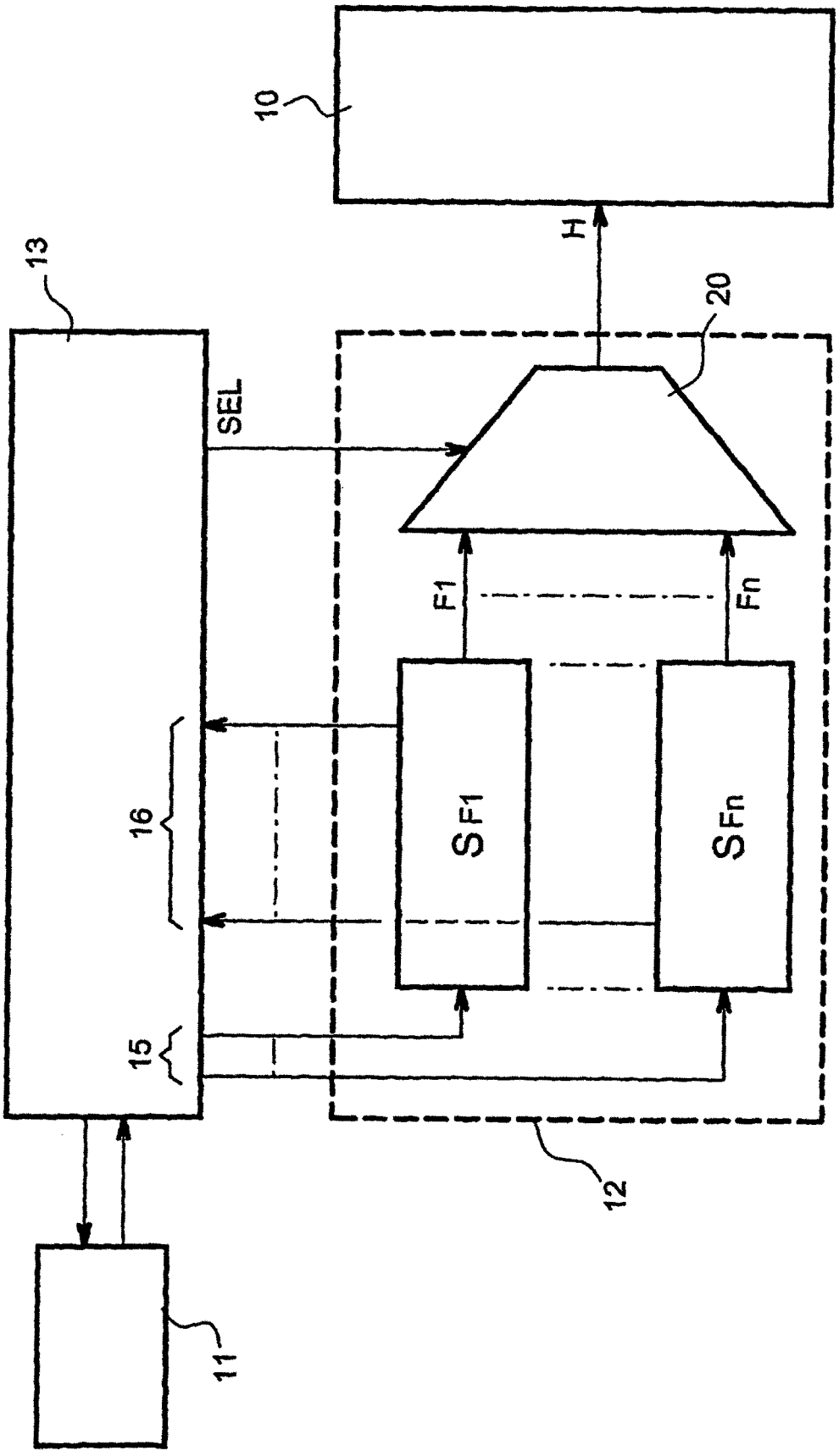
4. Componente según la reivindicación 1, en el cual el elemento síncrono es la unidad central (10) de una tarjeta inteligente.

5. Componente según la reivindicación 4, en el cual el controlador (13) esta gobernado por la unidad central.

6. Componente según la reivindicación 1, en el cual el elemento síncrono (10) es una memoria.

7. Componente según la reivindicación 1, en el cual el elemento síncrono (10) es una función cableada síncrona.

8. Componente según la reivindicación 1, en el cual la variación de frecuencia del reloj (H) está comprendida entre 1 MHz y 100 MHz.


10
H
13
20
SEL
F1
Fn
SF1
SFn
16
15
12
11