(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 416 367**

(51) Int. Cl.:

G06K 19/073 (2006.01)
G06F 12/14 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.09.2008** **E 08853741 (0)**

(97) Fecha y número de publicación de la concesión europea: **17.04.2013** **EP 2188762**

(54) Título: **Tarjeta de circuito integrado con tampón de entrada/salida asegurado**

(30) Prioridad:

14.09.2007 FR 0706447

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
31.07.2013

(73) Titular/es:

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

(72) Inventor/es:

BAILLY, ALEXIS;
DECROIX, DAVID;
GONCALVES, LOUIS-PHILIPPE;
PEPIN, CYRILLE y
ROUDIERE, GUILLAUME

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

ES 2 416 367 T3

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).

DESCRIPCION

Tarjeta de circuito integrado con tampón de entrada/salida asegurado

El presente invento concierne a una tarjeta de circuito integrado utilizable principalmente como soporte de datos por ejemplo para constituir un medio de identificación del portador de la tarjeta, un medio de acceso a un lugar o un material, un medio de pago tal como una tarjeta bancaria o una tarjeta de teléfono…

Transfondo del invento

Una tarjeta de circuito integrado incluye generalmente un cuerpo sobre el que está fijado un circuito integrado incluyendo una unidad de tratamiento asociada a una memoria de trabajo y a unos medios de intercambio de datos con un dispositivo externo tal como un lector de tarjeta. Los medios de intercambio incluyen por ejemplo unas zonas conductoras destinadas a cooperar con unos electrodos del dispositivo externo o una antena emisora/receptora para intercambiar señales electromagnéticas con una antena del dispositivo externo. La unidad de tratamiento, un microprocesador, que efectúa operaciones sobre datos, y más particularmente cálculos criptográficos, que van a permitir principalmente a la unidad de tratamiento verificar si está autorizada para realizar una transacción con el dispositivo externo al que los medios de intercambio le conectan. La memoria de trabajo (o RAM del inglés "Random Access Memory", memoria de acceso aleatorio) es utilizada para la memorización de datos que son intercambiados con el dispositivo externo y datos de funcionamiento interno tales como resultados intermedios que son reutilizados en las operaciones efectuadas por la unidad de tratamiento.

EP-A-1 672 566 divulga una tarjeta de circuito integrado incluyendo una unidad de tratamiento asociada a una memoria de trabajo y a medios de intercambio de datos con un dispositivo externo. La memoria de trabajo incluye una zona de memorización dedicada a los datos intercambiados. Las características en el preámbulo de la reivindicaciones 1 y 5 son conocidas de EP-A1 672 566.

Dichas tarjetas contienen a veces informaciones confidenciales, tales como un código secreto, o permiten el acceso a lugares, o a equipos que contienen dichas informaciones, y son a veces sometidas a tentativas de fraude que tienen como objetivo perturbar el funcionamiento de la unidad de tratamiento para llevar a esta a comunicar hacia el exterior datos confidenciales o para revelar su modo de funcionamiento.

Estas tentativas de fraude son generalmente realizadas utilizando la memoria de trabajo para lograr grabar trozos de instrucciones, inofensivos tomados individualmente, que la unidad de tratamiento ensamblará constituyendo así una instrucción que pone en peligro la seguridad de la tarjeta; o para recuperar informaciones que la unidad de tratamiento ha memorizado temporalmente y que no están normalmente destinadas a ser transmitidas al exterior.

Objeto del invento

Un objetivo del invento es suministrar un medio que permita controlar el intercambio de informaciones con el exterior con el fin de asegurar una protección de la tarjeta.

Resumen del invento

A este efecto se prevé, según el invento, una tarjeta de circuito integrado según la reivindicación 1.

Los datos intercambiados son los datos recibidos o que se van a emitir. Así, únicamente los datos intercambiados están contenidos en la zona de memorización dedicada y podrán ser intercambiados con el exterior. La seguridad por software asegurada por la unidad de tratamiento permite limitar el riesgo de que esta zona contenga datos perjudiciales para la seguridad de la tarjeta, es decir ya sean trozos de instrucciones, inofensivos tomados individualmente, y que constituyen una instrucción malintencionada una vez unidos, ya sea datos de funcionamiento interno que no deben ser comunicados normalmente al exterior. La unidad de tratamiento impide la presencia simultánea de estos trozos de instrucciones en memoria y la memorización de estos datos de funcionamiento interno. El hecho de tener una zona de memorización dedicada facilita la vigilancia limitando el número de bytes potencialmente peligrosos y no tiene una incidencia notable en el rendimiento de la tarjeta.

Según el invento, la unidad de tratamiento está programada para codificar los datos de la zona de memorización dedicada antes de una transferencia de datos desde el exterior.

Así, se evita que datos recibidos por la tarjeta para un primer comando puedan ser utilizados combinados con datos recibidos para un segundo comando, o utilizados directamente. Unos datos sucesivamente recibidos por la tarjeta no pueden por tanto ser recombinados o utilizados para formar una instrucción malintencionada.

Según una característica preferida, la unidad de tratamiento está programada para bloquear el acceso a la zona de memorización dedicada durante una operación de tratamiento.

Así, durante su funcionamiento, la unidad de tratamiento no puede grabar datos en la zona de memorización dedicada, eliminando el riesgo de que dichos datos, y más particularmente datos secretos o sensibles, sean a continuación trasmitidos al exterior.

Ventajosamente entonces, la unidad de tratamiento está programada para evaluar un estado de datos de la zona de memorización dedicada antes de realizar una operación de tratamiento y de verificar la integridad de los datos después de la operación de tratamiento.

Cualquier grabación de datos en la zona de memorización dedicada conllevaría entonces un fallo de integridad de esta zona y revelaría una tentativa de fraude.

El invento tiene igualmente como objeto un procedimiento según la reivindicación 5.

Otras características y ventajas del invento aparecerán con la lectura de la siguiente descripción de un modo de realización particular no limitativo del invento.

Breve descripción de los dibujos

Se hará referencia a la figura única que representa esquemáticamente una tarjeta conforme al invento.

Descripción detallada del invento

Haciendo referencia a la figura, la tarjeta incluye, de forma en sí conocida, un cuerpo 1 al que está fijado un circuito integrado 2 incluyendo una unidad de tratamiento 3, con la forma de un microprocesador, una memoria de sólo lectura 4, del tipo ROM (del inglés “Read Only Memory”, memoria de sólo lectura) y una memoria de trabajo 5 del tipo RAM (del inglés “Random Access Memory”, memoria de acceso aleatorio). La memoria de sólo lectura 4 contiene un programa de explotación (o varios) que está destinado a ser ejecutado por la unidad de tratamiento 3 con el fin de permitir a esta efectuar operaciones predeterminadas. Esta operación incluye operaciones de recepción de datos, operaciones de tratamiento de datos y operaciones de transmisión de datos. Las operaciones de tratamiento en cuestión son por ejemplo cálculos criptográficos y procedimientos de autentificación. La memoria de trabajo 5 es utilizada por la unidad de tratamiento 3 para memorizar datos. El circuito integrado 2 está unido a una antena 6 que constituye un medio de intercambio de datos con un dispositivo externo D formado aquí por un lector de tarjetas sin contacto.

En la memoria de trabajo 5 está definida una zona de memorización dedicada a los datos intercambiados. La zona de memorización dedicada, referenciada con el 7, está limitada de manera que no pueda ser extendida durante el funcionamiento de la unidad de tratamiento 3.

El programa de explotación ejecutado por la unidad de tratamiento 3 está situado para obligar a la unidad de tratamiento 3 a grabar en la zona de memorización dedicada 7 los datos intercambiados, es decir los datos que recibe de la antena 6 y los datos que está a punto de trasmitir al dispositivo externo D a través de la antena 6.

La unidad de tratamiento 3 está programada para verificar antes de la emisión de un dato que el dato está contenido en la zona de memorización dedicada 7.

El programa de explotación está igualmente ubicado para qué, previamente a cada recepción de datos, la unidad de tratamiento 3 altere los datos contenidos en la zona de memorización dedicada 7. Esta alteración consiste en codificar (“scramble”) los datos contenidos en esta zona. Esta operación es asimilable a un borrado de dichos datos.

El programa de explotación de la unidad de tratamiento 3 está además ubicado para bloquear la zona de memorización dedicada 7 durante las operaciones efectuadas por la unidad de tratamiento 3. Este bloqueo consiste aquí, en primer lugar, en prohibir a la unidad de tratamiento 3, mediante el programa de explotación, memorizar informaciones en la zona de memorización dedicada 7 durante las operaciones de tratamiento. En segundo lugar, el bloqueo incluye las etapas de evaluar un estado de datos de la zona de memorización dedicada 7 antes de realizar una operación de tratamiento y de verificar la integridad de los datos contenidos en la zona de memorización dedicada 7 después de la operación de tratamiento. Esta verificación de integridad es efectuada calculando un polinomio sobre los bytes presentes en la zona de memorización dedicada 7 antes de la operación de tratamiento y recalculando este polinomio después de la operación de tratamiento. Ya sólo falta entonces comparar los dos polinomios obtenidos. Este polinomio, igualmente llamado checksum o código de redundancia cíclica (obtenido del procedimiento CRC del inglés “Cyclic Redundancy Checks” como control de redundancia cíclica) es obtenido de forma clásica tratando un bloque de datos como una serie de coeficientes binarios de un polinomio. Así, cualquier memorización de los datos efectuada después del cálculo de integridad modificará el valor de este. La verificación de integridad revelará esta memorización no autorizada indicativa de un mal funcionamiento.

La tarjeta conforme al invento incluye así una memoria de trabajo provista de una zona de memorización de datos intercambiados y una seguridad por software asegurando un control de la memorización de los datos en esta zona.

Se señalará que la tarjeta conforme al invento únicamente precisa de una zona de memoria dedicada al intercambio de datos, conteniendo esta zona de memoria los datos intercambiados.

Por supuesto, el invento no se limita al modo de realización descrito y se pueden aportar variantes de realización sin salir del marco del invento tal y como se define en las reivindicaciones.

En particular, el invento es aplicable a cualquier tipo de tarjetas, y principalmente a tarjetas de contacto que posean zonas conductoras para cooperar con electrodos de un lector de tarjeta.

Los modos descritos de proveer seguridad pueden ser utilizados independientemente unos de otros o combinados.

Son utilizables otros modos de verificación de integridad.

REIVINDICACIONES

1. Tarjeta de circuito integrado incluyendo una unidad de tratamiento (3) asociada a una memoria de trabajo (5) y a medios de intercambio (6) de datos con un dispositivo externo (D), incluyendo la memoria del trabajo una única zona de memorización (7) dedicada a los datos intercambiados y estando situada la unidad de tratamiento para almacenar en la zona de memorización dedicada los datos intercambiados y para limitar el riesgo de que dicha zona de memorización dedicada contenga datos perjudiciales para la seguridad de la tarjeta, estando caracterizada la tarjeta por qué la unidad de tratamiento (3) está programada para codificar los datos de la zona de memorización dedicada (7) antes de una transferencia de datos desde el exterior con el fin de que datos sucesivos recibidos por la tarjeta no puedan ser recombinados o utilizados para formar una instrucción malintencionada.

2. Tarjeta de circuito integrado según la reivindicación 1, en la que la unidad de tratamiento (3) está programada para bloquear el acceso a la zona de memorización dedicada (7) durante una operación de tratamiento con el fin de que los datos secretos o sensibles no puedan ser transmitidos al exterior por la tarjeta.

3. Tarjeta según la reivindicación 2 en la que la unidad de tratamiento (3) está programada para calcular una integridad sobre los datos de la zona de memorización dedicada (7) antes de realizar una operación de tratamiento y para verificar la integridad de los datos después de la operación de tratamiento.

4. Tarjeta según la reivindicación 1, en la que la unidad de tratamiento (3) está programada para verificar antes de una emisión de un dato que el dato está contenido en la zona de memorización dedicada (7).

5. Procedimiento de gestión de una memoria de trabajo (5) de una tarjeta de circuito integrado (2) incluyendo una unidad de tratamiento (3) a la que están asociadas la memoria de trabajo y los medios de intercambio (6) de datos con un dispositivo externo (D), incluyendo las etapas de:

-definir en la memoria de trabajo una única zona dedicada (7) a datos intercambiados,

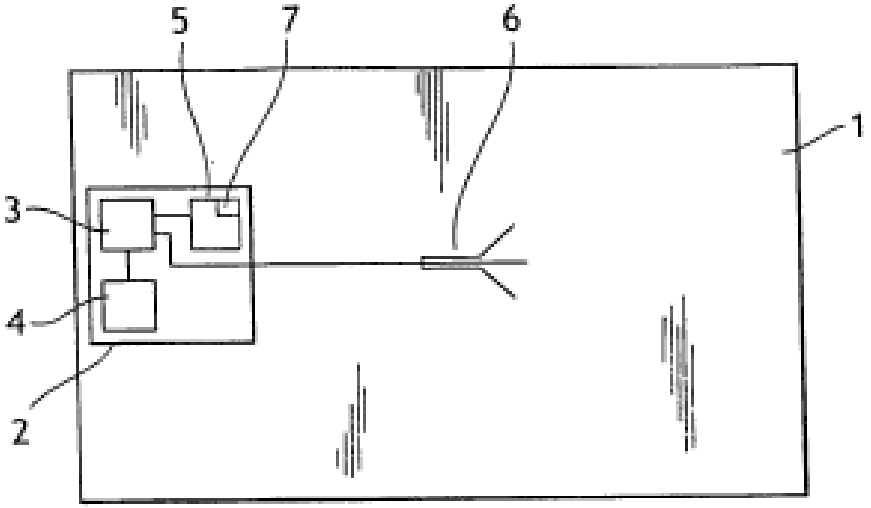
-controlar la unidad de tratamiento para almacenar los datos intercambiados en esta zona y para limitar el riesgo de que dicha zona dedicada contenga datos perjudiciales para la seguridad de la tarjeta,

caracterizada por que la limitación del riesgo de que la zona contenga datos perjudiciales incluye una fase de codificación de los datos de la zona de memorización dedicada (7) antes de una transferencia de datos desde el exterior con el fin de que datos sucesivos recibidos por la tarjeta no puedan ser recombinados o utilizados para formar una instrucción malintencionada.

6. Procedimiento de gestión según la reivindicación 5, en el que la limitación del riesgo de que la zona contenga datos perjudiciales incluye una fase de bloqueo del acceso a la zona de memorización dedicada (7) durante una operación de tratamiento con el fin de que los datos secretos o sensibles no pueden ser transmitidos al exterior por la tarjeta.

7. Procedimiento de gestión según la reivindicación 6, en el que la limitación del riesgo de que la zona contenga datos perjudiciales incluye las fases de evaluar un estado de los datos de la zona de memorización dedicada (7) antes de realizar una operación de tratamiento y de verificar la integridad de los datos después de la operación de tratamiento.

8. Procedimiento de gestión según la reivindicación 6, en el que la limitación del riesgo de que la zona contenga datos perjudiciales incluye la fase de verificar una emisión de un dato antes de que el dato esté contenido en la zona de memorización dedicada (7).


5
7
6
1
3
4
2