(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 675 072**

(51) Int. CI.:

G06F 21/75 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.05.2008 PCT/FR2008/050860**

(87) Fecha y número de publicación internacional: **27.11.2008 WO08142356**

(96) Fecha de presentación y número de la solicitud europea: **19.05.2008 E 08805806 (0)**

(97) Fecha y número de publicación de la concesión europea: **18.04.2018 EP 2162846**

(54) Título: **Criptoprocesador con protección de datos mejorada**

(30) Prioridad:

21.05.2007 FR 0755148

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.07.2018

(73) Titular/es:

INGENICO GROUP (100.0%)
28/32 Boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

COUSSIEU, ALAIN y
ECK, ALAIN

(74) Agente/Representante:

SUGRAÑES MOLINÉ, Pedro

DESCRIPCIÓN

Criptoprocesador con protección de datos mejorada

Campo de la invención

La presente invención se refiere a un circuito electrónico que comprende una memoria RAM en la que se almacenan datos y adaptado para borrar los datos durante la detección de un intento de acceso no autorizado.

Descripción de la técnica anterior

Numerosos sistemas electrónicos comprenden una memoria RAM en la que se almacenan datos denominados sensibles necesarios para el buen funcionamiento del sistema electrónico y que no deben resultar accesibles para un usuario no autorizado. A modo de ejemplo, un lector de tarjetas, por ejemplo, de tarjetas bancarias, comprende generalmente un circuito electrónico, denominado criptoprocesador, que se encarga del almacenamiento de los datos sensibles y de la realización de operaciones aritméticas con los datos sensibles. Los datos sensibles corresponden, por ejemplo, a los códigos confidenciales de las tarjetas introducidas en el lector o a claves utilizadas por el criptoprocesador para la puesta en práctica de algoritmos de encriptación. El criptoprocesador está adaptado para borrar el conjunto de datos sensibles en cuanto se detecta un intento de acceso no autorizado al lector por los dispositivos de seguridad que equipan el lector de manera que se evita que un individuo pueda leer los datos sensibles almacenados en el criptoprocesador.

Los componentes del lector, entre ellos el criptoprocesador, se alimentan generalmente a partir de una única fuente de alimentación, por ejemplo, la alimentación de la red, denominada a continuación alimentación principal. Generalmente, está prevista una fuente de alimentación de emergencia a nivel del lector para alimentar al criptoprocesador aunque se interrumpa la alimentación principal con el fin de permitir la conservación de los datos, el funcionamiento de los dispositivos de seguridad y el borrado de los datos sensibles en caso de detección de un intento de acceso no autorizado. Por ejemplo, la fuente de alimentación de emergencia está constituida por una batería conectada al criptoprocesador y que proporciona una tensión de alimentación de emergencia.

Concretamente debido a la disposición y del tamaño de la fuente de alimentación de emergencia y de las exigencias de seguridad actuales en el campo de los lectores de tarjetas bancarias, la protección de la fuente de alimentación de emergencia necesita dispositivos mecánicos costosos (por ejemplo, tapa con detección de apertura) y, generalmente, no es posible excluir completamente el riesgo de que un individuo consiga acceder a la fuente de alimentación de emergencia sin que esta intrusión se detecte por el criptoprocesador. Según una primera posibilidad, podría concebirse una desactivación de la fuente de alimentación de emergencia, lo que se traduciría en una detención del funcionamiento del criptoprocesador sin que haya podido realizarse el borrado de los datos sensibles almacenados en la memoria RAM del criptoprocesador. Aunque la interrupción de la alimentación de una memoria RAM conlleva, teóricamente, la pérdida de los datos almacenados en la misma, existe un riesgo de que los datos puedan recuperarse debido a fenómenos de remanencia característicos de determinados tipos de memorias RAM utilizadas habitualmente en los lectores. Según una segunda posibilidad, aún menos favorable, puede concebirse, haciendo variar la tensión de alimentación de emergencia, alterar el funcionamiento del criptoprocesador de manera que es posible un acceso al criptoprocesador sin conllevar el borrado de los datos sensibles en la memoria RAM que entonces permanece alimentada. Entonces, una persona no autorizada podría leer los datos sensibles.

El documento GB2195478 describe un sistema electrónico que comprende una memoria principal, una memoria secundaria, y un detector de intrusión. La memoria secundaria se borra tras la detección de una intrusión. El sistema electrónico se alimenta mediante una fuente de alimentación externa.

El documento WO 99/40501 describe un sistema electrónico que comprende una sola memoria unida a una fuente de alimentación principal y un detector de intrusión. La memoria secundaria se une a otra fuente de alimentación tras la detección de una intrusión para borrarse.

Sumario de la invención

La presente invención se refiere a un circuito electrónico que comprende una memoria RAM en la que se almacenan datos sensibles que está adaptado para impedir el acceso a los datos sensibles en el caso de una variación de la tensión de alimentación del circuito electrónico.

Así, un modo de realización de la presente invención prevé un circuito electrónico realizado de manera integrada que comprende una primera memoria RAM de almacenamiento de datos; un módulo de tratamiento adaptado para realizar una operación de borrado de la primera memoria RAM; y un terminal de acceso unido al módulo de tratamiento y destinado a recibir una primera señal de alimentación proporcionada por una primera fuente de alimentación externa al circuito electrónico. El circuito comprende, además, una segunda memoria RAM en la que se almacena una clave, encriptándose dichos datos poniendo en práctica dicha clave; y una segunda fuente de

alimentación integrada en el circuito electrónico y adaptada para proporcionar una segunda señal de alimentación al módulo de tratamiento, estando el módulo de tratamiento adaptado para detectar que se produce un intento de acceso no autorizado a partir de la comparación de las señales de alimentación primera y segunda y para borrar dicha clave mientras que el módulo de tratamiento se alimenta mediante la segunda fuente de alimentación.

Según un modo de realización, la segunda fuente de alimentación comprende un elemento capacitivo unido al terminal de acceso y al módulo de tratamiento, comprendiendo el circuito electrónico, además, un dispositivo adaptado para impedir una descarga rápida del elemento capacitivo mediante una acción exterior sobre el terminal de acceso.

Según un modo de realización, el módulo de tratamiento comprende transistores MOS y el elemento capacitivo corresponde a las capacidades parásitas de los transistores MOS.

Según un modo de realización, la capacidad de almacenamiento de la segunda memoria RAM es inferior a la capacidad de almacenamiento de la primera memoria RAM.

Según un modo de realización, la capacidad de almacenamiento de la segunda memoria RAM es inferior a mil bits.

Según un modo de realización, el circuito comprende un terminal de acceso complementario destinado a unirse a una tercera fuente de alimentación, externa al circuito electrónico, que garantiza la alimentación del módulo de tratamiento en un modo de funcionamiento normal del circuito electrónico, garantizando la primera fuente de alimentación la alimentación del módulo de tratamiento cuando la tercera fuente de alimentación está inactiva.

Según un modo de realización, la primera fuente de alimentación comprende una batería conectada al terminal de acceso y un condensador montado en paralelo a los terminales de la batería.

También está previsto un sistema, concretamente un lector de tarjeta, que comprende una carcasa que contiene una fuente de alimentación y un circuito electrónico tal como se definió anteriormente unido a la fuente de alimentación.

También está previsto un procedimiento de protección de datos almacenados en una primera memoria RAM de un circuito electrónico, comprendiendo el circuito electrónico, además, un módulo de tratamiento adaptado para realizar una operación de borrado de la primera memoria RAM y un terminal de acceso unido al módulo de tratamiento y destinado a recibir una primera señal de alimentación proporcionada por una primera fuente de alimentación, externa al circuito electrónico. El procedimiento consiste en proporcionar una segunda memoria RAM a nivel del circuito electrónico en la que se almacena una clave, obteniéndose dichos datos mediante una encriptación que pone en práctica dicha clave y una segunda fuente de alimentación integrada en el circuito electrónico y adaptada para proporcionar una segunda señal de alimentación al módulo de tratamiento. El procedimiento consiste, además, en hacer que el módulo de tratamiento detecte que se produce un intento de acceso no autorizado a partir de la comparación de las señales de alimentación primera y segunda y en borrar dicha clave, alimentándose entonces el módulo de tratamiento mediante la segunda fuente de alimentación.

Según un modo de realización, la primera señal de alimentación corresponde a una primera tensión y la segunda señal de alimentación corresponde a una segunda tensión, detectándose un intento de acceso no autorizado cuando la diferencia entre las tensiones primera y segunda es superior a un umbral dado durante un periodo de tiempo dado.

Breve descripción de los dibujos

Estos objetos, características y ventajas, así como otros, se expondrán en detalle en la siguiente descripción de un ejemplo de realización particular realizada a modo no limitativo en relación con las figuras adjuntas en las que:

la figura 1 representa un ejemplo habitual de criptoprocesador de un lector de tarjetas; y
la figura 2 representa un ejemplo de realización de un criptoprocesador de lector de tarjetas según la invención.

Descripción detallada

Por motivos de claridad, se han designado elementos iguales mediante referencias iguales en las diferentes figuras.

Ahora va a describirse un ejemplo habitual de criptoprocesador en relación con la figura 1. A modo de ejemplo, se considera un criptoprocesador que equipa un lector de tarjetas, por ejemplo, tarjetas bancarias. No obstante, la presente invención puede aplicarse a cualquier tipo de criptoprocesador.

El criptoprocesador 10 corresponde a un circuito integrado que comprende un terminal de alimentación B1 al que se aplica una tensión de alimentación principal VDD proporcionada, por ejemplo, a partir de la alimentación de la red. A modo de ejemplo, la tensión de alimentación principal VDD es del orden de 2 voltios. El criptoprocesador 10 comprende un microprocesador 12 (μP) que realiza, en funcionamiento normal, las operaciones habituales

características del criptoprocesador 10. Para ello, el criptoprocesador 10 comprende uno o varios terminales de acceso (representándose un solo terminal B2 en la figura 1) por medio de los cuales el microprocesador 12 intercambia datos con otros componentes del lector. El criptoprocesador 10 comprende, además, una memoria RAM 14 (RAM) en la que el microprocesador 12 está adaptado para leer y escribir datos, concretamente datos denominados sensibles. El tamaño de la memoria 14 depende de la cantidad de datos tratados por el criptoprocesador 10 y es, de manera habitual, del orden de algunos kilooctetos, por ejemplo 8 kilooctetos.

El criptoprocesador 10 comprende además un módulo de seguridad 16 (módulo de seguridad) o autómata. El módulo de seguridad 16 es un circuito lógico que tiene una estructura más simple que la estructura del microprocesador 12 y que puede comprender de algunos millares a algunas decenas de millares de puertas lógicas. El módulo de seguridad 16 puede intercambiar datos con el microprocesador 12 y al menos realizar operaciones de escritura en la memoria 14. El módulo de seguridad 16 puede, además, intercambiar datos con otros componentes del lector por medio de terminales de acceso (representándose un solo terminal B3 en la figura 1). Generalmente, está previsto un módulo de interfaz entrada/salida 18 (PIO) entre el módulo de seguridad 16 y el terminal de acceso B3. A modo de ejemplo, el módulo de seguridad 16 puede recibir mediante el terminal de acceso B3 señales transmitidas por dispositivos de seguridad que equipan el lector. Un ejemplo de dispositivo de seguridad corresponde a un circuito de tipo enrejado que comprende una pista conductora cuya interrupción, que representa un intento de acceso no autorizado al lector, conlleva la provisión de una señal de alarma al criptoprocesador 10. Otro ejemplo de dispositivo de seguridad corresponde a una tecla de teclado falsa que garantiza de manera permanente un contacto eléctrico entre dos pistas conductoras en funcionamiento normal, representando una interrupción del contacto un intento de acceso no autorizado y conllevando la provisión de una señal de alarma al criptoprocesador 10. Otro dispositivo de seguridad corresponde a un sensor de temperatura, representando una temperatura excesiva un mal funcionamiento o un intento de acceso no autorizado y conllevando la provisión de una señal de alarma al criptoprocesador 10. El módulo de seguridad 16 puede decidir que se produce un intento de acceso no autorizado tras la recepción de una señal de alarma en el terminal B3, tras la detección de una variación de la tensión de alimentación principal VDD, tras la detección de un mal funcionamiento del microprocesador 12, etc. Cuando el módulo de seguridad 16 detecta un intento de acceso no autorizado, ordena el borrado de los datos almacenados en la memoria 14. El criptoprocesador 10 comprende un módulo, no representado, de provisión de una señal de reloj que marca el ritmo de los elementos del criptoprocesador 10, concretamente el módulo de seguridad 16.

En funcionamiento normal, el módulo de seguridad 16 se alimenta mediante la tensión de alimentación principal VDD. Cuando la tensión de alimentación principal VDD no está presente, el módulo de seguridad 16 se alimenta mediante una fuente de alimentación de emergencia que proporciona una tensión de alimentación de emergencia VDD_BU a un terminal B4 del criptoprocesador 10. En el presente ejemplo de realización, la fuente de alimentación de emergencia comprende una batería P de la que un terminal se conecta al terminal B4 y de la que otro terminal se conecta a una fuente de un potencial de referencia, por ejemplo, la masa GND del lector. Además, un condensador C1 está montado en paralelo a los terminales de la batería P. Se disponen, por debajo de una línea en trazos discontinuos 20, los elementos del criptoprocesador 10 que no funcionan cuando la tensión de alimentación principal VDD no está presente y, por encima de la línea 20, los elementos del criptoprocesador 10 que, cuando la tensión de alimentación principal VDD no está presente, continúan funcionando alimentándose mediante la tensión de alimentación de emergencia VDD_BU, eventualmente en un modo de funcionamiento diferente del modo de funcionamiento normal. En particular, el módulo de provisión de la señal de reloj funciona de manera permanente. Cuando la tensión de alimentación principal VDD no está presente, el módulo de seguridad 16, alimentado por la batería P, continúa funcionando y, por tanto, puede borrar los datos almacenados en la memoria 14 cuando se detecta un intento de acceso no autorizado. En el caso en el que la batería P se desactivara, el módulo de seguridad 16 sigue alimentándose un tiempo determinado mediante el condensador C1. La disminución de la tensión en los terminales del condensador C1 se detecta mediante el módulo de seguridad 16 que reacciona, tal como para la detección un intento de acceso no autorizado, mediante el borrado de los datos sensibles almacenados en la memoria 14. La capacidad del condensador C1, que, generalmente, corresponde a un componente discreto, es suficiente para permitir la realización de la operación de borrado de la memoria 14 mediante el módulo de seguridad 16.

Generalmente, el lector comprende una carcasa formada por una parte superior de carcasa (a nivel de la cual se encuentran la pantalla de visualización y el teclado del lector) y por una parte inferior de carcasa. La carcasa contiene una placa base, conectándose los componentes electrónicos del lector a una u otra de las caras de la placa base. En particular, el criptoprocesador 10 y el condensador C1 se conectan, generalmente, a la cara de la placa base orientada hacia la parte superior de carcasa o cara superior. Por motivos de volumen ocupado, la batería P se conecta generalmente a la cara de la placa base orientada hacia la parte inferior de carcasa o cara inferior. Aunque los dispositivos de seguridad puedan disponerse en las dos caras de la placa base, generalmente se considera que el nivel de seguridad de los componentes conectados a la cara inferior de la placa base es menos elevado que el de los componentes conectados a la cara superior de la placa base puesto que una intrusión realizada del lado de la parte superior de carcasa generalmente es visible durante una manipulación habitual de la carcasa.

Por tanto, existe un riesgo de que un individuo pueda acceder a la batería P sin que se detecte un intento de acceso no autorizado. Entonces, teóricamente sería posible modificar el valor de la tensión de alimentación de emergencia

VDD_BU mientras que la tensión de alimentación principal VDD no está presente. Esto podría alterar el funcionamiento del módulo de seguridad 16 que entonces ya no estaría en condiciones de detectar un intento de acceso no autorizado y de borrar en consecuencia los datos sensibles almacenados en la memoria 14. Entonces, sería posible un acceso a estos datos.

Además, aunque el condensador C1 está dispuesto, generalmente, en la cara superior de la placa base que presenta un nivel de seguridad más elevado que la cara inferior, se trata de un componente discreto distinto del criptoprocesador 10. Por tanto, siempre existe un riesgo de que un usuario consiga acceder al condensador C1 sin que se detecte un intento de acceso no autorizado. Una desconexión del condensador C1, y de la batería P, conlleva entonces la caída casi instantánea de la tensión de alimentación de emergencia VDD_BU y, por tanto, cuando la tensión de alimentación principal VDD no está presente, una detención del funcionamiento del módulo de seguridad 16 sin que haya podido realizarse una operación de borrado de los datos sensibles almacenados en la memoria 14. Aunque la interrupción de la alimentación de la memoria RAM 14 conlleva teóricamente una pérdida de los datos que se almacenan en la misma, existe un riesgo, debido a fenómenos de remanencia de determinados tipos de memoria RAM, de que los datos sensibles, o una parte de los mismos, puedan recuperarse. La línea 22 discontinua delimita los elementos del lector 10, más concretamente la batería P, el condensador C1 y la unión eléctrica entre la batería P, el condensador C1 y el terminal de acceso B4, que necesitan una protección particular para garantizar el buen funcionamiento del criptoprocesador 10.

La figura 2 representa un ejemplo de realización de un criptoprocesador 30 según la invención que permite impedir el acceso a los datos sensibles durante variaciones de la tensión de alimentación de emergencia VDD_BU. Los elementos comunes con el criptoprocesador 10 de la figura 1 se designan mediante las mismas referencias. El criptoprocesador 30 comprende el conjunto de los elementos del criptoprocesador 10 y comprende, además, un condensador complementario C2 del que un terminal está unido a una fuente de un potencial de referencia, por ejemplo la masa GND del lector, y del que el otro terminal está unido por un lado a un terminal Al del módulo de seguridad 16 y por otro lado al terminal B4 por medio de un dispositivo R (por ejemplo una resistencia, un diodo u otro) lo que prohíbe una descarga rápida del condensador C2 mediante una acción exterior sobre el terminal B4. Además, el terminal B4 está unido directamente a un terminal RAZ del módulo de seguridad 16. Se denomina DIFF a la tensión entre los terminales Al y RAZ y V_{Al} a la tensión en los terminales del condensador C2. El módulo de seguridad 16 comprende una memoria RAM complementaria 32 (registro) de capacidad reducida con respecto a la memoria RAM 14 y para la que pueden realizarse las operaciones de escritura y de lectura por el módulo de tratamiento 16 a un pequeño número de ciclos de reloj y a un bajo coste energético. Por ejemplo, se trata de un registro de algunos centenares de bits, por ejemplo, de 256 bits.

En el presente ejemplo de realización, los datos sensibles se almacenan en la memoria 14 en una forma encriptada, poniendo en práctica el procedimiento de encriptación utilizado al menos una clave, llamada clave primaria. La clave primaria se almacena en la memoria complementaria 32 del módulo de seguridad 16. En funcionamiento normal, cuando el microprocesador 12 desea utilizar un dato sensible almacenado en la memoria 14, también lee la clave primaria almacenada en la memoria complementaria 32 para desencriptar el dato sensible almacenado en la memoria 14. Cuando se detecta un intento de acceso no autorizado, el módulo de seguridad 16 borra en primer lugar la clave primaria almacenada en la memoria complementaria 32, después, eventualmente, borra los datos sensibles almacenados en la memoria 14.

En el caso de una interrupción de la alimentación VDD principal, el microprocesador 12 deja de funcionar y el módulo de seguridad 16 continúa funcionando alimentándose por la batería P. El condensador C2 se carga mediante la tensión de alimentación de emergencia VDD_BU aplicada al terminal B4. Entonces, la tensión V_{Al} es igual a la tensión de alimentación de emergencia VDD_BU. Entonces, la tensión DIFF es sustancialmente nula. En el caso en el que la tensión de alimentación de emergencia VDD_BU varíe, lo que corresponde, por ejemplo, a una desactivación de la batería P o a una manipulación voluntaria de la tensión VDD_BU, la tensión en el terminal RAZ varía mientras que la tensión V_{Al} en el terminal Al se mantiene a un valor sustancialmente constante por el condensador C2. El aumento en valor absoluto de la tensión DIFF se detecta por el módulo de seguridad 16 como un intento de acceso no autorizado, por ejemplo, cuando es superior a un umbral determinado durante un número dado de ciclos de reloj. Al haber podido disminuir la tensión de alimentación de emergencia VDD_BU, el módulo de seguridad 16 se alimenta entonces por el condensador complementario C2 hasta que éste se descargue. Al haber detectado un intento de acceso no autorizado, el módulo de seguridad 16 borra en primer lugar la clave primaria almacenada en la memoria 32 secundaria. A continuación, si su alimentación es suficiente, el módulo de seguridad 16 trata de borrar los datos sensibles almacenados en la memoria 14.

Al ser pequeño el tamaño de la memoria complementaria 32, la operación de borrado de los datos almacenados en la memoria complementaria 32 puede realizarse rápidamente con un bajo coste energético. En particular, puede realizarse, aunque el módulo de seguridad 16 solamente se alimente por el condensador C2. Por el contrario, según el tamaño de la memoria RAM 14, la capacidad del condensador C2 puede no ser lo bastante importante como para garantizar una alimentación suficiente del módulo de seguridad 16 que permita el borrado de la totalidad de los datos sensibles almacenados en la memoria 14. No obstante, aunque la alimentación del módulo de seguridad 16 mediante el condensador C2 sea insuficiente como para permitir el borrado de todos los datos sensibles almacenados en la memoria 14 y aunque la tensión de alimentación de emergencia VDD_BU se lleve a un valor

para el que el funcionamiento del módulo de seguridad 16 se ve alterado de manera que ya no está en condiciones de borrar los datos sensibles restantes almacenados en la memoria 14, los datos sensibles restantes almacenados en la memoria 14 ya no pueden usarse ya que la clave primaria almacenada en la memoria complementaria 32 se ha borrado. Entonces, ya no puede accederse a los datos sensibles restantes en la memoria 14.

A modo de ejemplo, la capacidad del condensador C2 puede ser inferior a algunos picofaradios. Una capacidad de este tipo es suficiente para garantizar una corriente de alimentación del módulo de seguridad 16 del orden de algunos centenares de nanoamperios durante algunos ciclos de reloj. Esto es suficiente para garantizar el funcionamiento del módulo de seguridad 16 durante los algunos ciclos de reloj necesarios para la detección de un intento de intrusión y para el borrado de la memoria complementaria 32. En particular, cuando la memoria complementaria 32 corresponde a un registro, el borrado de los datos almacenados en la memoria 32 puede realizarse en un solo ciclo de reloj. El condensador C2 puede realizarse de manera integrada con los otros elementos del módulo de seguridad 16. A modo de ejemplo, el condensador C2 puede corresponder a las capacidades parásitas de transistores MOS que constituyen el módulo de seguridad 16. Además, al garantizar el condensador C2 la alimentación del módulo de seguridad 16, las restricciones de protección de la batería P, del condensador C1 y de la unión eléctrica entre la batería P, el condensador C1 y el terminal de acceso B4 pueden ser menos estrictas que para el circuito representado en la figura 1.

Se han descrito modos de realización particulares de la presente invención. Diversas variantes y modificaciones serán evidentes para el experto en la técnica. En particular, aunque la presente invención se haya descrito en el caso de un criptoprocesador unido a una fuente de alimentación principal y a una fuente de alimentación de emergencia, es evidente que puede aplicarse a un criptoprocesador unido a una única fuente de alimentación, cargándose entonces el condensador complementario integrado en el criptoprocesador mediante la única fuente de alimentación, y comparándose la tensión proporcionada por la única fuente de alimentación con la tensión en los terminales del condensador complementario mediante el módulo de seguridad para la detección de un intento de acceso no autorizado.

REIVINDICACIONES

1. Circuito electrónico (30) realizado de manera integrada, que comprende:

una primera memoria RAM (14) de almacenamiento de datos;
una segunda memoria RAM (32) en la que se almacena una clave, encriptándose dichos datos poniendo en práctica dicha clave;
un módulo de tratamiento (16) adaptado para realizar una operación de borrado de la primera memoria RAM; y
un terminal de acceso (B4) unido al módulo de tratamiento y destinado a recibir una primera señal de alimentación (VDD_BU) proporcionada por una primera fuente de alimentación (P, C1) externa al circuito electrónico,
en el que una segunda fuente de alimentación (C2) integrada en el circuito electrónico está adaptada para proporcionar una segunda señal de alimentación (VAl) al módulo de tratamiento, estando el módulo de tratamiento adaptado para detectar que se produce un intento de acceso no autorizado a partir de la comparación de las señales de alimentación primera y segunda y para borrar dicha clave mientras que el módulo de tratamiento se alimenta mediante la segunda fuente de alimentación,
en el que la segunda fuente de alimentación comprende un elemento capacitivo (C2) unido al terminal de acceso (B4) y al módulo de tratamiento (16), comprendiendo el circuito electrónico, además, un dispositivo (R) adaptado para impedir una descarga rápida del elemento capacitivo mediante una acción exterior sobre el terminal de acceso,

caracterizado por que el módulo de tratamiento (16) comprende transistores MOS y **por que** el elemento capacitivo (C2) corresponde a las capacidades parásitas de los transistores MOS.

2. Circuito electrónico según la reivindicación 1, en el que la capacidad de almacenamiento de la segunda memoria RAM (32) es inferior a la capacidad de almacenamiento de la primera memoria RAM (14).

3. Circuito electrónico según una cualquiera de las reivindicaciones anteriores, en el que la capacidad de almacenamiento de la segunda memoria RAM (32) es inferior a mil bits.

4. Circuito electrónico según una cualquiera de las reivindicaciones anteriores, que comprende un terminal de acceso complementario (B1) destinado a unirse a una tercera fuente de alimentación, externa al circuito electrónico (30), que garantiza la alimentación del módulo de tratamiento (16) en un modo de funcionamiento normal del circuito electrónico, garantizando la primera fuente de alimentación (P, C1) la alimentación del módulo de tratamiento cuando la tercera fuente de alimentación está inactiva.

5. Circuito electrónico según una cualquiera de las reivindicaciones anteriores, en el que la primera fuente de alimentación comprende una batería (P) conectada al terminal de acceso (B4) y un condensador (C1) montado en paralelo a los terminales de la batería.

6. Sistema, concretamente lector de tarjeta, que comprende una carcasa que contiene una fuente de alimentación (P, C1) y un circuito electrónico (30) según una cualquiera de las reivindicaciones 1 a 5 unido a la fuente de alimentación.

7. Procedimiento de protección de datos almacenados en una primera memoria RAM (14) de un circuito electrónico (30), comprendiendo el circuito electrónico, además, una segunda memoria RAM (32) a nivel del circuito electrónico (30) en la que se almacena una clave, obteniéndose dichos datos mediante una encriptación que pone en práctica dicha clave, un módulo de tratamiento (16) adaptado para realizar una operación de borrado de la primera memoria RAM y un terminal de acceso (B4) unido al módulo de tratamiento y destinado a recibir una primera señal de alimentación (VDD_BU) proporcionada por una primera fuente de alimentación (P, C1), externa al circuito electrónico, en el que una segunda fuente de alimentación (C2) está integrada en el circuito electrónico y adaptada para proporcionar una segunda señal de alimentación (VAl) al módulo de tratamiento, consistiendo el procedimiento en hacer que el módulo de tratamiento detecte que se produce un intento de acceso no autorizado a partir de la comparación de las señales de alimentación primera y segunda y en borrar dicha clave, alimentándose entonces el módulo de tratamiento mediante la segunda fuente de alimentación, en el que la segunda fuente de alimentación comprende un elemento capacitivo (C2) unido al terminal de acceso (B4) y al módulo de tratamiento (16), comprendiendo el circuito electrónico, además, un dispositivo (R) adaptado para impedir una descarga rápida del elemento capacitivo mediante una acción exterior sobre el terminal de acceso,
caracterizado por que el módulo de tratamiento (16) comprende transistores MOS y **por que** el elemento capacitivo (C2) corresponde a las capacidades parásitas de los transistores MOS.

8. Procedimiento según la reivindicación 7, en el que la primera señal de alimentación corresponde a una primera tensión (VDD_BU) y en el que la segunda señal de alimentación corresponde a una segunda tensión (VAl), detectándose un intento de acceso no autorizado cuando la diferencia entre las tensiones

primera y segunda es superior a un umbral dado durante un periodo de tiempo dado.

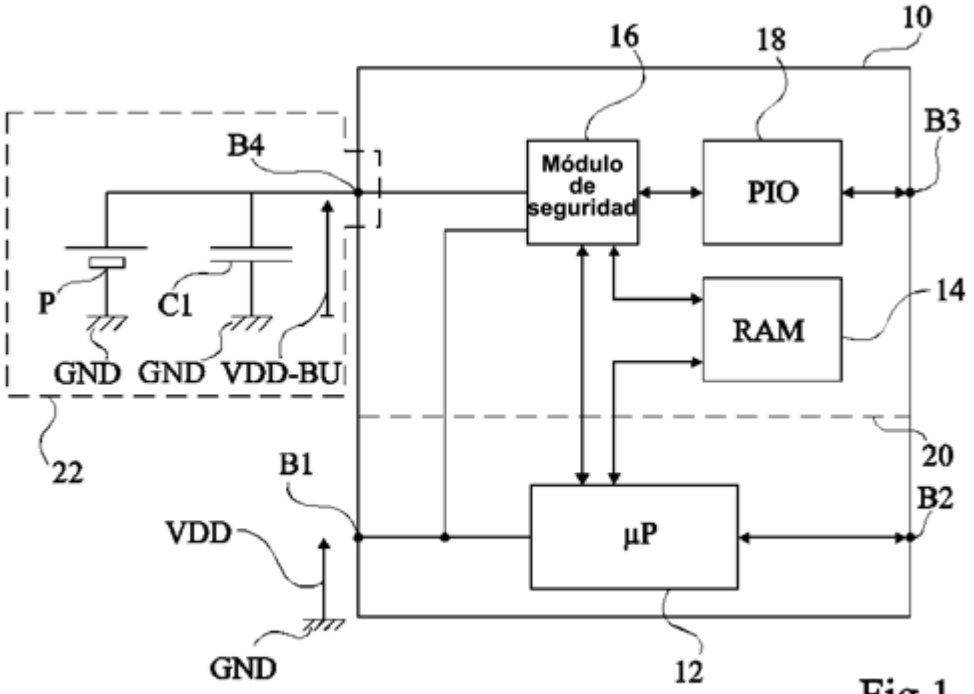
16
18
10
B4
Módulo de seguridad
PIO
B3
P
C1
RAM
14
GND
GND
VDD-BU
22
20
B1
B2
VDD
µP
GND
12

Fig 1

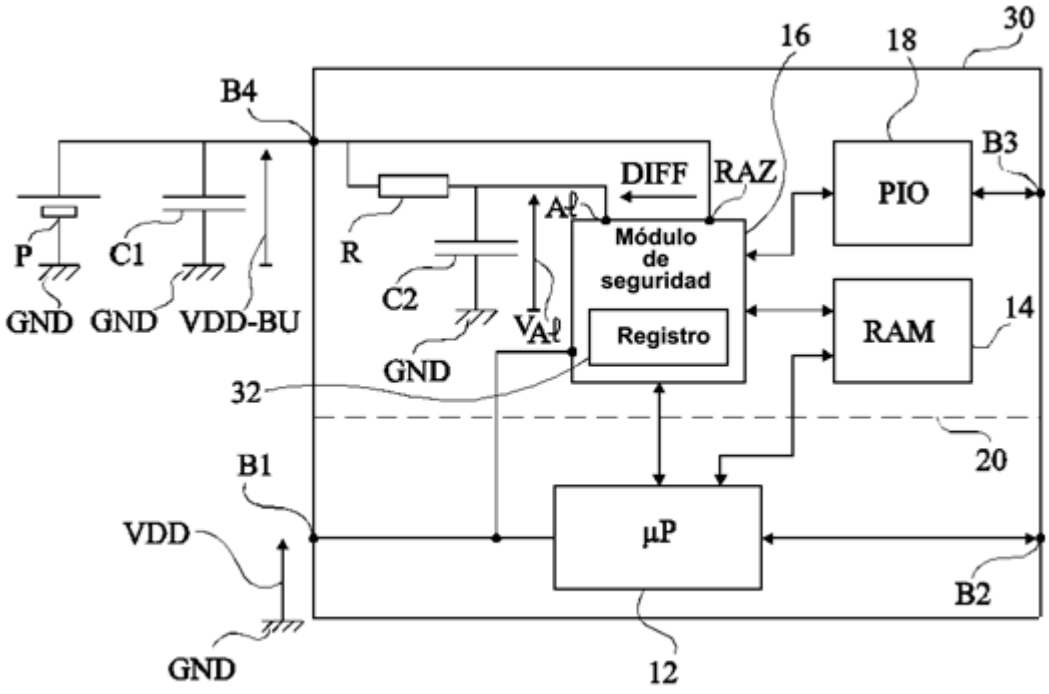
30
16
18
B4
DIFF
RAZ
PIO
B3
P
C1
R
Módulo de seguridad
RAM
14
C2
GND
GND
VDD-BU
Registro
32
20
B1
VDD
µP
B2
GND
12

Fig 2