(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 405 361**

(51) Int. CI.:

H03K 3/037 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.04.2007 E 07731958 (0)**

(97) Fecha y número de publicación de la concesión europea: **30.01.2013 EP 2016677**

(54) Título: **Componente dotado de un circuito integrado que incluye un criptoprocesador y procedimiento de instalación**

(30) Prioridad:

10.05.2006 FR 0651681

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.05.2013

(73) Titular/es:

EUROPEAN AERONAUTIC DEFENCE AND SPACE COMPANY EADS FRANCE (100.0%)
37, BOULEVARD DE MONTMORENCY
75781 PARIS CEDEX 16, FR

(72) Inventor/es:

BUARD, NADINE;
MILLER, FLORENT;
LAHOUD, IMAD y
RUBY, CÉDRIC

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Componente dotado de un circuito integrado que incluye un criptoprocesador y procedimiento de instalación.

La presente invención tiene por objeto un componente realizado en su totalidad o en parte en forma de un circuito integrado y que dispone de un criptoprocesador, así como su procedimiento de instalación. El componente de la invención está dotado de medios para prevenir la revelación de sus secretos de encriptación. La invención se encamina más en particular a los componentes criptoprocesadores, pero también podría concernir a los circuitos integrados de todo tipo, en los que se pretende impedir que puedan funcionar de una manera inadecuada, ya resulte ese funcionamiento inadecuado de una tentativa deliberada de pervertir su funcionamiento, o bien de la incidencia imprevista de una agresión exterior (eléctrica, electromagnética, térmica, partícula u otro).

La protección de los datos memorizados en un componente electrónico se lleva a cabo desde siempre mediante cifrado con ayuda de una clave. La clave debe permanecer secreta imperativamente.

En un componente electrónico, un criptoprocesador es un procesador especializado para las operaciones de criptografía. Éste contiene en su parte de memoria una o unas claves que deben mantenerse secretas y que le sirven para cifrar y/o descifrar la información que recibe. Se compone entre otras cosas de una memoria no volátil que almacena la clave de manera permanente cuando se halla sin tensión, de una memoria intermedia volátil (por ejemplo de tipo SRAM o báscula D) dentro de la cual se carga la clave mediante el sistema operativo (si lo hay) en la puesta en tensión y de un circuito lógico de tipo microcontrolador o microprocesador capaz de efectuar las operaciones de cifrado y descifrado de los mensajes con ayuda de la clave secreta.

En los componentes electrónicos, la información se almacena y transita en forma de cargas, que son atrapadas o dirigidas en el seno del material semiconductor, silicio, en virtud de la acción de los campos eléctricos. Un transistor MOS, en el cual se fundamenta la mayoría de los circuitos lógicos y digitales, es de hecho un interruptor que deja transitar o no unas cargas entre su fuente y su drenador, en función de la tensión aplicada en su puerta.

Recientemente ha aparecido una nueva clase de amenaza, encaminada a extraer información contenida en un componente criptoprocesador inyectando en él fallos al propio tiempo que analiza el comportamiento obtenido. Son diversos los métodos utilizables de inyección de fallos (elevación de la temperatura del componente, elevación de la tensión de alimentación del componente, pulsos transitorios, partículas...). Los métodos que a día de hoy son analizados como los más peligrosos son aquellos que permiten inyectar fallos en los componentes en ubicaciones controladas, por ejemplo en una parte de memoria estática de acceso aleatorio, SRAM, donde se almacena una clave de cifrado. Tal es el caso de los ataques mediante láser o mediante microhaces de iones.

El ataque de un criptoprocesador mediante inyección de fallos consiste en inyectar localmente unas cargas con objeto de modificar u ocultar la información almacenada o en tránsito. El análisis de la respuesta del criptoprocesador como consecuencia de la inyección de fallos proporciona a los piratas indicaciones que les permiten reducir el número de combinaciones e identificar más rápidamente la clave. Tal análisis es tanto más sencillo cuanto más preciso es el ataque, tanto espacial como temporalmente. Existen pues diferentes técnicas de inyección de fallos, con dificultades variables de puesta en práctica, siendo las más eficaces afortunadamente las más difíciles de llevar a la práctica. A título de indicación, las posibles agresiones contra los circuitos integrados están reseñadas en el documento "Memories: a survey of their secure uses in smart cards" a cargo de Michael Neve, Eric Peeters, David Samyde y Jean-Jacques Quisquater; http://www.dice.ucl.ac.be/crypto y editado por Second International IEEE Security in Storage, Workshop - Proceedings of SISW 2003.

Las técnicas más simples inyectan fallos de manera aleatoria en el componente: tal es el caso de un ataque mediante elevación de temperatura, u ondas electromagnéticas (radar, microondas, radio), o mediante partículas (iones, neutrones o protones). En estos tres casos, el ataque perturba el componente en su conjunto y, si bien es posible determinar un área, no es posible apuntar a un bit ni incluso a varios bits. No obstante, con un tratamiento con soporte lógico y matemático muy avanzado, parece que sea posible explotar los resultados del ataque. El ataque es muy fácil de poner en práctica ya que no precisa de ningún acceso particular y se puede dirigir a distancia.

Luego están los ataques por mediación de las entradas/salidas del circuito, perturbando las tensiones nominales por medio de un generador de tensión. Estos ataques se pueden dirigir en fase (temporalmente) con relación a los ciclos de funcionamiento del reloj del circuito. La consecuencia del ataque sigue siendo bastante aleatoria, lo cual significa que el número de combinaciones que hay que probar para extraer la clave se mantiene elevado, pero esta técnica es bastante fácil de llevar a la práctica si se tiene acceso al circuito.

Finalmente, unas técnicas permiten inyectar fallos en momentos elegidos y en ubicaciones perfectamente controladas (en teoría con una precisión del orden del bit), lo cual significa que entonces se es capaz por ejemplo de acabar modificando uno a uno los bits que contienen la clave, luego el siguiente y así sucesivamente, o incluso de interrumpir una operación de descifrado. Tal es el caso de los ataques mediante láser o mediante microhaces de iones. Estas técnicas son difíciles de llevar a la práctica, ya que precisan de un acceso al componente, es decir, de

la apertura del encapsulado del componente y la puesta al descubierto del circuito integrado, del chip. Para defenderse de estos ataques, los fabricantes implantan contramedidas más o menos eficaces para impedir el desencapsulado.

Es el propósito de la invención proteger los componentes contra tales ataques.

La activación de un tiristor parásito, llamada latchup, y respectivamente la activación de un transistor bipolar parásito, llamada snapback, son mecanismos que existen de manera inherente en todo componente en circuito integrado de tipo de implantación complementaria, CMOS, o respectivamente no complementaria. Son el resultado de la entrada en conducción de un tiristor, o respectivamente de un transistor bipolar horizontal, parásitos, en respuesta a una introducción local de cargas en el componente. La corriente de alimentación del componente aumenta entonces bruscamente y, debido a la corriente que lo recorre y/o a la caída de tensión de alimentación resultante, el componente deja de ser funcional. En ausencia de limitación de corriente, puede haber una destrucción del circuito por efecto térmico, y es preferible prever una limitación de corriente en la alimentación del circuito. De todas formas, el circuito tan sólo vuelve a ser funcional después de la desconexión de la alimentación y su posterior nueva puesta en tensión. En la continuación de la memoria descriptiva, hablaremos de activación parásita cuando se aluda a la activación de uno u otro de estos fenómenos: activación de un tiristor parásito: latchup y activación de un transistor bipolar parásito: snapback. Estos dos fenómenos están descritos en el documento publicado en 1999 por la Fairchild Semiconductor Corporation y titulado Understanding Latch-up in Advanced CMOS Logic. Un ejemplo para un circuito de protección contra el latchup se da en el documento US6.064.555.

Según la posición de contactos en el componente, el nivel de carga que activa las estructuras parásitas (denominado umbral de latchup o umbral de snapback) puede ser muy variable. Por lo tanto, los fabricantes de componentes intentan en general elevar al máximo este nivel, por cuanto que el mecanismo puede ser activado por un entorno radiativo natural (partículas), por descargas electrostáticas o incluso por ruido en las entradas o salidas. No obstante, parece más fácil para un fabricante (fabricante de componentes) proyectar una tecnología sensible al latchup/snapback que una tecnología insensible.

Por regla general, se observa que con cada salto de generación, los primeros lotes que se fabrican son sensibles al latchup. A continuación los fabricantes corrigen los procedimientos de fabricación o la arquitectura de los circuitos de los componentes para que esos componentes tengan umbrales de activación más elevados. Así es como se encuentran disponibles en el mercado comercial numerosos componentes sensibles al latchup, lo cual obliga a los usuarios de esos componentes en intenso entorno radiativo (como por ejemplo el entorno espacial) a efectuar una selección sistemática de los componentes comerciales.

Se han publicado estudios relativos a la susceptibilidad de los circuitos integrados a experimentar latchup

- en un artículo titulado "Extreme latchup susceptibility in modern commercial off the shelf (COTS) monolithic 1 M and 4 M CMOS static random acces memory (SRAM) devices" a cargo de Thomas E. Page y Joseph M. Benedetto y publicado en Radiation Effects Data Workshop, 2005. IEEE del 11 al 15 de julio de 2005, páginas 1 a 7,
- por IEEE Transactions on Nuclear Science, Vol 50. n.° 3, junio de 2003, en un artículo titulado "Destructive single event effect in semiconductor devices and ICs" de Fred W. Sexton,
- así como en "Proposal for solid state particle detection based on latchup effect" a cargo de A. Gabrielli y publicado en Electronic Letters, 26 de mayo de 2005 Vol. 41, n.° 11.

La inyección de fallos es una inyección local de cargas en un circuito que viene a perturbar su funcionamiento. Se puede definir la cantidad mínima de cargas necesaria para la activación de la perturbación como el umbral de perturbación del circuito. El umbral de latchup o de snapback se define como la cantidad mínima de carga que ha de inyectarse localmente para activar el mecanismo de latchup o de snapback.

En la invención, para solucionar el problema de la protección de los componentes en circuitos integrados con criptoprocesador, se opta por hacer uso de este efecto para proteger la información contenida en un componente frente a inyecciones de fallos. En efecto, si un componente con criptoprocesador en su conjunto (o por lo menos las partes que contienen la clave de manera transitoria) se compone de circuitos escogidos para ser deliberadamente sensibles al latchup, o al snapback, entonces, con un umbral de activación más bajo que el umbral de perturbación de los circuitos por inyección de fallos, el componente se autoprotege. En el caso de una inyección de fallos (es decir, de cargas) por el medio que sea, la estructura parásita se activa. Esta activación lleva a un violento aumento de la corriente de alimentación del circuito.

Esta corriente muy intensa puede deteriorar definitivamente el componente en circuito integrado. Para evitar este último inconveniente, se prevé entonces un simple circuito de detección del latchup (mediante medida de este aumento de la corriente de alimentación del componente). Por ejemplo, este circuito de detección es del tipo del descrito en el último artículo antes citado. Este circuito de detección permite entonces poner en funcionamiento un circuito de limitación de corriente para no destruir el componente. El circuito de limitación de corriente mantiene la

tensión de alimentación de las partes internas del circuito en una tensión inferior a la necesaria para hacerlo funcionar. Por lo tanto, el componente deja de ser funcional hasta la reinicialización, haciendo imposible cualquier extracción de datos. Semejante solución equivale de hecho a utilizar el propio componente criptoprocesador como detector instantáneo del ataque.

La invención tiene pues por objeto un componente en circuito integrado que incluye un criptoprocesador, caracterizado por incluir una o varias estructuras internas de tiristores parásitos y/o de transistores bipolares parásitos susceptibles de activarse y porque un umbral de energía de activación de las estructuras parásitas, tiristores parásitos y/o transistores bipolares parásitos es inferior a una cantidad de energía necesaria para hacer cambiar de estado una báscula del componente.

Ésta tiene asimismo por objeto un procedimiento de instalación de un componente en circuito integrado con criptoprocesador, caracterizado por incluir una operación de selección del componente de un lote de componentes, siendo el criterio de esta selección una susceptibilidad particular del componente a la activación de tiristores parásitos (latchup) o a la activación de transistores bipolares parásitos (snapback), siendo definida esta susceptibilidad con relación a un umbral de activación.

Se comprenderá mejor la invención con la lectura de la descripción que sigue y con la revisión de las figuras que la acompañan. Estas tan sólo se aportan con carácter indicativo y en modo alguno limitativo de la invención. Las figuras muestran:

- Figura 1: una representación esquemática de un componente con circuito integrado según la invención;
- Figura 2: la representación clásica de un fenómeno de activación de un tiristor parásito;
Figuras 3a, 3b y 3c: una sección clásica de un circuito de activación parásita, y su representación esquemática, y una representación clásica del fenómeno de activación de un transistor bipolar parásito, respectivamente; y
- Figura 4: ilustración del nivel de protección del componente cuando son diferentes los niveles umbral de energía relativos a la activación de las estructuras parásitas y al cambio de estado de una báscula por inyección de fallos.

La figura 1 muestra un componente 1 dotado de un circuito integrado electrónico según la invención. El componente puede ser monolítico o híbrido. El conjunto del componente 1 o cada una de sus partes se fabrica, según esta tecnología de los circuitos integrados, mediante implantaciones de impurezas, difusiones de metalizaciones y oxidaciones, selectivas todas ellas, en un cristal semiconductor (e incluso una placa de material semiconductor amorfo). El material semiconductor es principalmente silicio, pero podría ser germanio u otro. La arquitectura de las áreas de implantación, de metalización y de oxidación determina circuitos electrónicos de diferentes funcionalidades. El componente 1 de la invención cuenta así esencialmente con un circuito criptoprocesador 2. De acuerdo con una característica esencial de la invención, el componente 1 incluye estructuras de tiristores parásitos LU (por latchup) y/o de transistores bipolares parásitos (SB por snapback). En el presente caso se han representado cuatro estructuras de este tipo identificadas con 3a a 6b según la ubicación que ocupan en el componente 1. En la práctica, las áreas de activación 3a a 6b se encuentran ubicadas a nivel de los transistores de los circuitos integrados. Típicamente, estas estructuras 5a 5b de tiristores parásitos y/o de transistores bipolares parásitos pueden encontrarse en el mismo seno de los motivos elementales de un área de memoria 7, de tipo memoria estática aleatoria, SRAM, del componente 1.

O bien estas estructuras 4a 4b de tiristores parásitos y/o de transistores bipolares parásitos pueden encontrarse en el mismo seno de los motivos elementales de un área de memoria intermedia 8 del componente 1. El área intermedia es en general un registro del criptoprocesador 2, y se halla muy cercana al mismo. O bien estas estructuras 3a 3b de tiristores parásitos y/o de transistores bipolares parásitos pueden encontrarse en el mismo seno de las celdas de un área combinatoria del componente. Típicamente, en tal caso, los circuitos 3a y/o 3b están situados en el área de los circuitos del criptoprocesador 2.

O bien estas estructuras 6a 6b de tiristores parásitos y/o de transistores bipolares parásitos pueden encontrarse en un área 9 de circuitos de entradas y/o de salidas del componente 1. Todos los medios de inyección de fallos, de manera localizada o no, activan de manera inherente los tiristores parásitos (mecanismo de latchup) y/o los transistores bipolares parásitos (mecanismo de snapback) en un componente suficientemente sensible, puesto que aquello que los activa es la manifestación del fallo (la introducción de cargas). Sin embargo, ha de encontrarse un equilibrio adecuado para que el mecanismo no se active de manera fortuita ante un ruido, y en este punto definiremos el componente ideal.

La activación de un tiristor parásito o latchup es resultado de la entrada en conducción de un tiristor parásito (p-n-p-n) inherente a la tecnología CMOS (y en particular al inversor CMOS). Si se deposita una cantidad suficiente de cargas en el sustrato y en la proximidad de la unión pozo/sustrato polarizada en sentido inverso, esta estructura puede bloquearse y propiciar el paso de una corriente intensa entre la alimentación y la masa. El paso de esta corriente ocasiona entonces unos daños a menudo irreversibles en el seno de la estructura del componente. Si es

así, el componente pasa a quedar entonces definitivamente inoperante.

La activación de un transistor bipolar parásito o snapback tiene unas consecuencias bastante similares a las del latchup. Esta vez la conducción excesiva no se debe a la entrada en conducción de un tiristor parásito sino a la del transistor bipolar horizontal parásito de los transistores MOS de efecto de campo MOSFETs. Sus difusiones corresponden al drenador, a la fuente y al sustrato del MOSFET. Tal fenómeno se produce en particular en los componentes NMOS para los cuales no se encuentra tiristor (debido a la ausencia de PMOS) y, de manera recíproca, en un componente PMOS (debido a la ausencia de NMOS), y en los componentes sobre sustrato aislante (tecnología SOI).

Estos fenómenos han sido estudiados y observados especialmente en el caso de la agresión, natural o no, de los componentes electrónicos por partículas de tipo neutrones, protones, iones pesados (en los que son calificados de SEL, Single Event Latchup, por suceso aislado de activación de un tiristor parásito, y de SES, Single Event Snapback, por suceso aislado de activación de un transistor bipolar parásito), o incluso radiaciones gamma. No obstante, para los componentes más sensibles, estos pueden producirse asimismo en respuesta a una descarga electrostática, a una variación un tanto violenta de alimentación o en un entorno electromagnético perturbado.

Si definimos el umbral de activación como la cantidad de carga que debe ser introducida localmente para activar el fenómenos de latchup (activación de un tiristor parásito) o de snapback, se podrá considerar protegido el criptoprocesador si el umbral de activación del latchup o de snapback es ligeramente menor o igual que el umbral de cambio de estado de un bit que ha de protegerse en una báscula o, más generalmente, que el umbral de perturbación de cualquier celda o función elemental del circuito.

Así, de acuerdo con la invención, figura 4, preferentemente un umbral de energía 10 (o de cantidad de cargas) de activación de una estructura parásita (latchup o snapback) es inferior a una cantidad de energía 11 (o de carga) necesaria para hacer cambiar de estado una báscula del componente, ya quede situada esta báscula en una memoria SRAM o intermedia, en un registro del criptoprocesador, en una parte lógica combinatoria del criptoprocesador 2, en un circuito de entrada-salida 9, o cualquier otra parte.

La idea de la invención está en que el fenómeno de activación de las estructuras parásitas se produce, inhibiendo el funcionamiento del componente 1, incluso antes de que este último haya experimentado cualquier modificación de los estados eléctricos de sus circuitos. En otras palabras, cualquier inyección de fallo empezará inhibiendo el componente, volviéndolo no funcional, incluso antes de modificar el estado de una de sus celdas de memoria que han de protegerse. En el caso en que el umbral de activación parásita 10 es superior al umbral de cambio de estado 11 de una báscula, el componente no está protegido, ya que existen niveles de energía para los cuales es posible modificar el estado de las básculas sin activar las estructuras parásitas. En el caso en que el umbral de activación parásita 10 es inferior al umbral de cambio de estado 11 de una báscula, el componente está protegido, ya que su funcionamiento queda inhibido antes de haber podido modificar el estado de sus básculas.

De acuerdo con la invención, preferentemente, el componente 1 incluye un circuito limitador de corriente de alimentación 12 acoplado al circuito de activación de las estructuras parásitas. Por ejemplo, de una manera muy esquemática, el limitador de corriente 12 incluye una resistencia 13 puesta en serie en el circuito de alimentación cuando se detecta una activación de una de las estructuras parásitas. A tal efecto, se interconecta un detector de corriente 14, acoplado de una u otra manera a los circuitos 3a a 6b. Cuando el detector 14 no detecta, provoca la conducción de un transistor 15 que une en serie una alimentación 16 a los circuitos 2, 7, y otros, del componente 1. Cuando se detecta una activación parásita, un transistor 17 complementario del transistor 15 pone en funcionamiento la resistencia 13 en el camino de alimentación. De ello se derivan dos efectos. Por una parte, el componente 1 no se destruye, puesto que la corriente que lo recorre está limitada por la resistencia 13. Por otra parte, la tensión útil aguas abajo de la resistencia 13 se hace tan baja que el componente 1 deja de ser funcional.

El limitador 12 es tal que, una vez activado el circuito de activación, el componente deja de ser funcional y su alimentación debe ser reinicializada para que funcione de nuevo.

La fabricación de un componente 1 de este tipo no es difícil. Un fabricante es capaz de ajustar los parámetros de procedimiento e incluso de tensión de alimentación para proyectarlo voluntariamente. Pero se puede incluso encontrarlo en venta: en la medida en que los componentes electrónicos se someten a prueba de iones pesados antes de ser embarcados en satélites y en que están disponibles bases de datos de resultados de pruebas con aceleradores de partículas, basta con elegir un componente cuyo umbral 10 es inferior al umbral 11, e incluso con elegir la tensión de alimentación del componente, para que éste presente esa propiedad. Otro medio es utilizar para identificarlos un banco de pruebas láser. En cualquier caso, puede ser útil, por ejemplo mediante láser, identificar el área sensible del componente y comprobar que queda perfectamente asegurada la protección de la información.

Las áreas que puede ser interesante hacer sensibles al latchup o al snapback son especialmente: el área de memoria 7, el área de memoria intermedia 8, el área combinatoria 2, las entradas-salidas 9.

Para las memorias SRAM, en el artículo "Extreme ..." antes citado se encontrarán ejemplos de referencias de componentes de diversas tecnologías que presentan esa característica. Se podrán encontrar igualmente microcontroladores que cumplen estas condiciones. Por otro lado, se puede estimar que en la actualidad, para las tecnologías 0,18 µm y 0,13 µm, aproximadamente el 10 % de los componentes presentes en el mercado presentarán esa característica. En la invención, se toma ventaja de esta situación optando por instalar en placas madre 18, tarjetas chip 18 o en cualquier otro aparato 18 un componente 1 elegido de este modo. El componente 1 se elige de tal manera que su umbral de activación 10 de una estructura parásita (tiristor parásito o transistor bipolar parásito) sea inferior a un umbral crítico 11. Por ejemplo, se somete unos candidatos a componentes a pruebas de fallos con un nivel energético de agresión crítico y se seleccionan tan sólo aquellos de esos componentes que han mostrado que se volvían no funcionales. Cuanto más bajo sea el umbral crítico, más autoprotegido quedará el componente (pero más riesgo correrá de averiarse a menudo). En un ejemplo preferido, este umbral es por su parte inferior al umbral 11 que permite el basculamiento de un estado eléctrico del componente 1.

Las figuras 3a, 3b y 3c muestran, para el caso de la activación de un tiristor parásito, la presencia de un tiristor parásito n-p-n-p realizado en un sustrato de tipo n y, para el caso de la activación de un transistor bipolar parásito, la presencia de una estructura bipolar parásita en un transistor MOS.

En la invención, se eligen en la fabricación unos parámetros de fabricación, tiempo de implantación, temperatura, naturaleza de las impurezas, tensión eléctrica de implantación susceptibles de propiciar la sensibilidad del componente a las activaciones de estructuras parásitas (tiristores parásitos y/o transistores bipolares parásitos). Preferentemente, la elección es tal que un umbral de energía de activación de estas estructuras parásitas es inferior a una cantidad de energía necesaria para hacer cambiar de estado una báscula del componente. En la medida que sea necesario, en la fabricación o en la utilización, se ajustan estos parámetros de funcionamiento (por ejemplo la tensión de polarización). El criterio de este ajuste es una susceptibilidad del componente a la activación de los tiristores parásitos (latchup) y/o a la activación de los transistores bipolares parásitos, siendo esta susceptibilidad superior a un umbral.

Cuando un umbral de energía 11 que permite el cambio de estado de una báscula del componente es inferior a un umbral de energía 10 de la activación de un tiristor parásito y/o de activación de un transistor bipolar parásito, y para una energía inferior al umbral de energía 11 que permite el cambio de estado de una báscula del componente, no es posible activar las estructuras parásitas ni provocar el cambio de estado de una báscula del componente. Para una energía entre el umbral de energía 11 que permite el cambio de estado de una báscula del componente y el umbral de energía 10 de la activación de un tiristor parásito y/o de activación de un transistor bipolar parásito, puede producirse el cambio de estado de una báscula del componente. Las estructuras parásitas no se activan. Por lo tanto, el componente no está protegido. Para niveles de energía superiores a un umbral de energía 10 de la activación de un tiristor parásito y/o de activación de un transistor bipolar parásito, las estructuras parásitas se activan.

Cuando un umbral de energía 11 que permite el cambio de estado de una báscula del componente es superior a un umbral de energía 10 de la activación de un tiristor parásito y/o de activación de un transistor bipolar parásito, y para niveles de energía inferiores al umbral de energía 10 de la activación de un tiristor parásito y/o de activación de un transistor bipolar parásito, no es posible activar las estructuras parásitas ni provocar el cambio de estado de una báscula del componente. El componente está protegido. Para una energía comprendida entre el umbral de energía 10 de la activación de un tiristor parásito y/o de activación de un transistor bipolar parásito y un umbral de energía 11 que permite el cambio de estado de una báscula del componente, las estructuras parásitas se activan, pero no es posible el cambio de estado de una báscula del componente. El componente está protegido. Para niveles de energía superiores al umbral de energía 11 que permite el cambio de estado de una báscula del componente, las estructuras parásitas se activan y las básculas cambian de estado, pero el componente deja de ser funcional.

REIVINDICACIONES

1. Componente (1) en circuito integrado que incluye un criptoprocesador (2), **caracterizado por** incluir una o varias estructuras internas (3a-6b) de activación parásita de tipo activación de un tiristor parásito y/o activación de un transistor bipolar parásito y porque un umbral de energía de activación (10) de las estructuras parásitas, tiristores parásitos y/o transistores bipolares parásitos, es inferior a una cantidad de energía (11) necesaria para hacer cambiar de estado una báscula del componente.

2. Componente según la reivindicación 1, **caracterizado por** incluir un circuito limitador de corriente de alimentación (12) acoplado al circuito de activación de los tiristores parásitos y/o de activación de los transistores bipolares parásitos de tal manera que, una vez activado este circuito, el componente deja de ser funcional y su alimentación debe ser reinicializada para que funcione de nuevo.

3. Componente según una de las reivindicaciones 1 a 2, **caracterizado porque** las estructuras de activación de los tiristores parásitos y/o de activación de los transistores bipolares parásitos se hallan situadas en un área de memoria SRAM (7) del componente.

4. Componente según una de las reivindicaciones 1 a 3, **caracterizado porque** las estructuras de activación de los tiristores parásitos y/o de activación de los transistores bipolares parásitos se hallan situadas en un área de memoria intermedia (8) del componente.

5. Componente según una de las reivindicaciones 1 a 4, **caracterizado porque** las estructuras de activación de los tiristores parásitos y/o de activación de los transistores bipolares parásitos se hallan situadas en un área combinatoria (2) del componente.

6. Componente según una de las reivindicaciones 1 a 5, **caracterizado porque** las estructuras de activación de los tiristores parásitos y/o de activación de los transistores bipolares parásitos se hallan situadas en un área (9) de circuitos de entradas y/o de salidas del componente.

7. Procedimiento de instalación de un componente (1) en circuito integrado con criptoprocesador (2), **caracterizado por** incluir una operación de selección del componente de un lote de componentes y/o un ajuste de sus parámetros de funcionamiento, en particular su tensión de polarización, siendo el criterio de esta selección y/o ajuste una susceptibilidad del componente a la activación de tiristores parásitos y/o a la activación de transistores bipolares parásitos, siendo esta susceptibilidad superior a un umbral (10), por incluir en la fabricación una elección de parámetros susceptibles de propiciar la sensibilidad del componente a la activación de un tiristor parásito y/o activación de un transistor bipolar parásito y porque esta elección es tal que un umbral de energía de activación (10) de un tiristor parásito y/o activación de un transistor bipolar parásito es inferior a una cantidad de energía (11) necesaria para hacer cambiar de estado una báscula del componente.

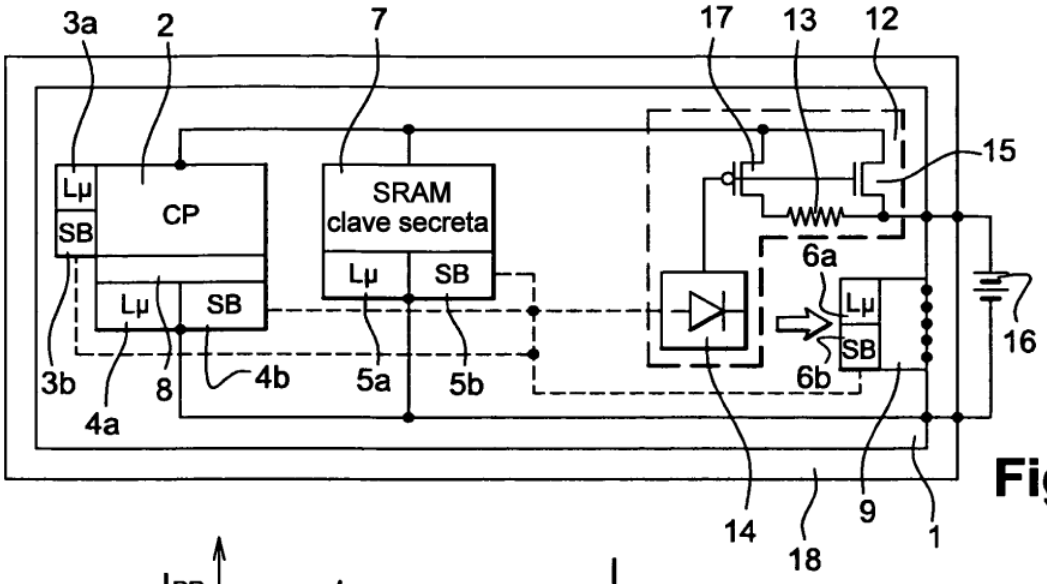

Fig. 1

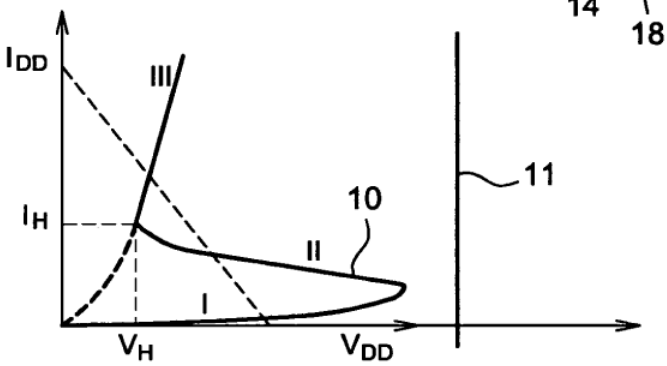

Fig. 2

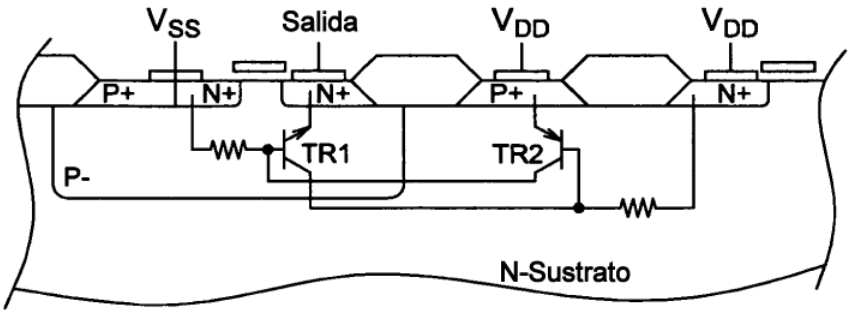

Fig. 3a

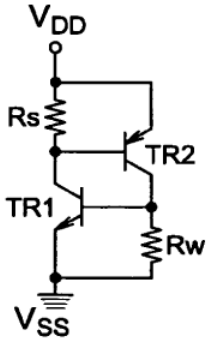

Fig. 3b

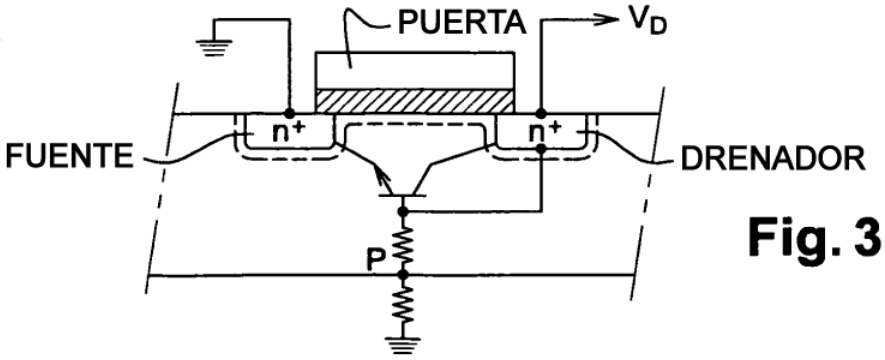

Fig. 3c

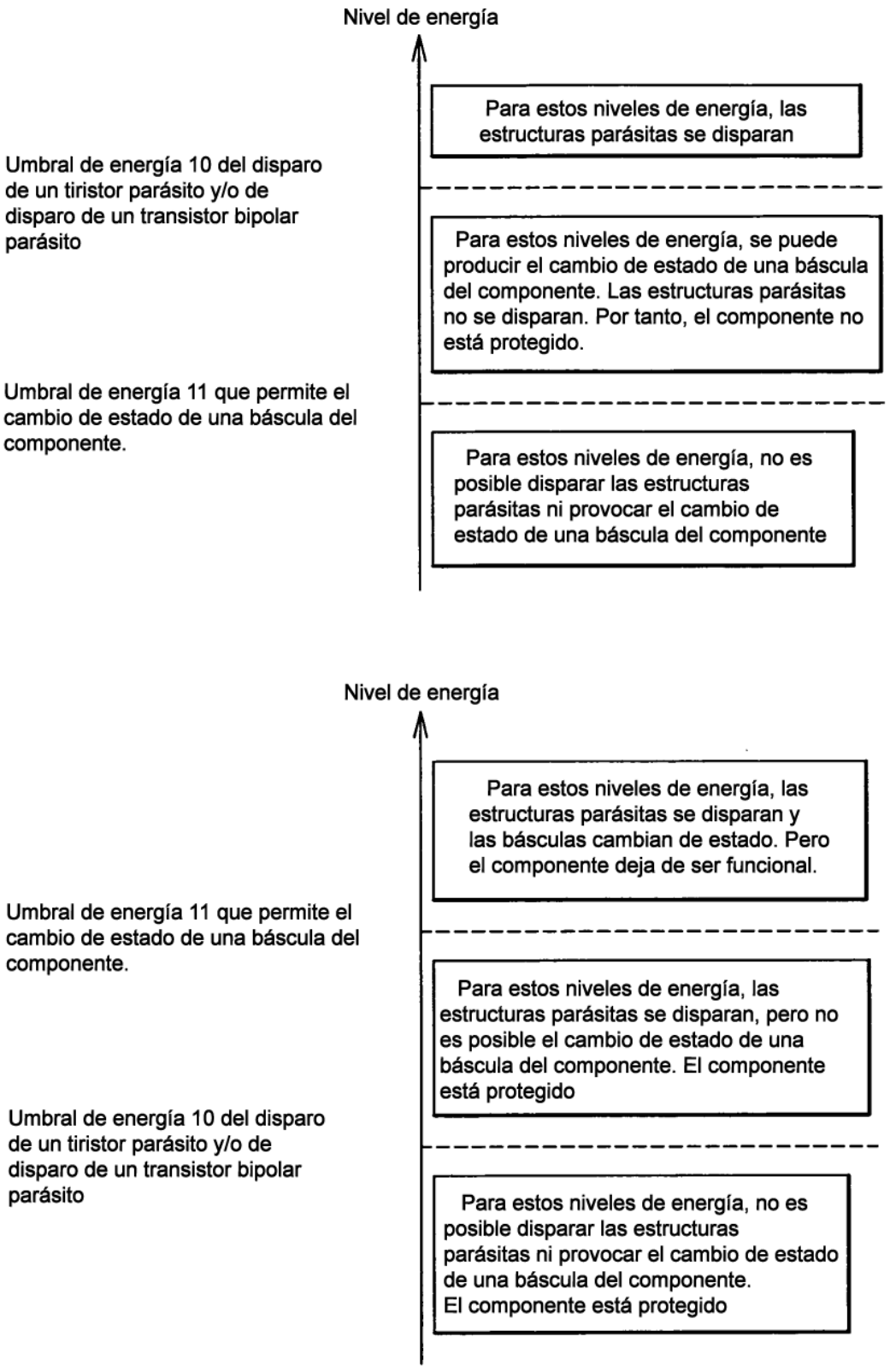
Nivel de energía
Para estos niveles de energía, las estructuras parásitas se disparan
Umbral de energía 10 del disparo de un tiristor parásito y/o de disparo de un transistor bipolar parásito
Para estos niveles de energía, se puede producir el cambio de estado de una báscula del componente. Las estructuras parásitas no se disparan. Por tanto, el componente no está protegido.
Umbral de energía 11 que permite el cambio de estado de una báscula del componente.
Para estos niveles de energía, no es posible disparar las estructuras parásitas ni provocar el cambio de estado de una báscula del componente
Nivel de energía
Para estos niveles de energía, las estructuras parásitas se disparan y las básculas cambian de estado. Pero el componente deja de ser funcional.
Umbral de energía 11 que permite el cambio de estado de una báscula del componente.
Para estos niveles de energía, las estructuras parásitas se disparan, pero no es posible el cambio de estado de una báscula del componente. El componente está protegido
Umbral de energía 10 del disparo de un tiristor parásito y/o de disparo de un transistor bipolar parásito
Para estos niveles de energía, no es posible disparar las estructuras parásitas ni provocar el cambio de estado de una báscula del componente. El componente está protegido

Fig. 4