



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 320 405**

51 Int. Cl.:
G06K 19/073 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 96 Número de solicitud europea: **00128471 .0**
96 Fecha de presentación : **23.12.2000**
97 Número de publicación de la solicitud: **1113386**
97 Fecha de publicación de la solicitud: **04.07.2001**

54 Título: **Protección de tarjetas inteligentes frente a análisis de potencia de alimentación separada.**

30 Prioridad: **30.12.1999 US 475921**

45 Fecha de publicación de la mención BOPI:
22.05.2009

45 Fecha de la publicación del folleto de la patente:
22.05.2009

73 Titular/es:
YEDA RESEARCH AND DEVELOPMENT Co., Ltd.
The Weizmann Institute of Science
P.O. Box 95
Rehovot 76100, IL

72 Inventor/es: **Shamir, Adi**

74 Agente: **Sagrado Gallastegui, Pedro**

ES 2 320 405 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).

DESCRIPCIÓN

Protección de tarjetas inteligentes frente a análisis de potencia de alimentación separada.

5 **Antecedentes de la invención****Campo de la invención**

La presente invención se refiere a nuevas técnicas, procedimientos y aparatos para la protección de tarjetas inteligentes frente a análisis de potencia cuando son insertadas en un lector de tarjetas, controlado por un adversario.

Técnica anterior

Las tarjetas inteligentes se utilizan típicamente para llevar a cabo cálculos criptográficos basados en claves secretas insertadas en sus memorias no volátiles. Un gran número de ataques sobre tarjetas inteligentes ha sido publicado en la literatura científica. Algunos de estos ataques, por ejemplo, los ataques por fallo, como han descrito D. Boneh, R.A. Demillo y R.J. Lipton, en "Sobre la Importancia de Comprobar Protocolos Criptográficos respecto a Fallos", Proceedings of Eurocrypt 97, SpringerF Verlag, 1997, pp. 37-51, y los ataques por sondeo como han descrito O. Kommerling y M. Jun, en "Principios de Diseño para Procesadores de Tarjetas Inteligentes Resistentes a la Manipulación Inde-

20 bida", [http://www.cl.cam.ac.uk/mgk25/sc99-tamper\[-slides\].pdf](http://www.cl.cam.ac.uk/mgk25/sc99-tamper[-slides].pdf), requieren un equipamiento sofisticado y un know-how detallado para el diseño físico del chip de tarjeta inteligente. Otros ataques, por ejemplo los ataques por temporización, como ha descrito P. Kocher, "Ataques en el Tiempo sobre Implementaciones de DiffieHellman, RSA, DSS, y Otros Sistemas", Proceedings of Crypto 96, SpringerF Verlag, 1996, pp-104-113, y ataques de interferencia como han descrito O. Kommerling y M. Jun, "Principios de Diseño para Procesadores de Tarjetas Inteligentes Resistentes a la Manipulación Inde-

25 bida", Proceedings of USENIX Workshop on Smartcard Technology, USENIX Association, pp. 920, 1999, pueden ser llevados a cabo con una inversión muy pequeña, pero de modo que es relativamente fácil de proteger los elementos de software y de hardware de las tarjetas inteligentes frente a los mismos.

En 1998, Paul Krocher de Cryptography Research publicó un nuevo tipo de ataque conocido como Análisis de Potencia, según fue descrito por P. Kocher y B. Jun en "Introducción a Análisis Diferencial de Potencia y Ataques Relacionados", <http://www.cryptography.com/dpa/technical/index.html>, 1998, que es muy fácil de implementar, pero muy difícil de evitar. El ataque se basa en el análisis exacto de la curva de consumo de potencia de la tarjeta inteligente durante las operaciones criptográficas. En la variante, Análisis Simple de Potencia (SPA) de este ataque, el atacante estudia una curva simple de consumo de potencia y determina (entre otras cosas) la identidad de las instrucciones y el peso Hamming de las palabras de datos leídas a partir de, o escritas en, una memoria en cualquier ciclo de reloj dado. En la variante de este ataque, Análisis de Potencia Diferencial (DPA), el atacante estudia múltiples curvas de consumo de potencia registradas a partir de ejecuciones diferentes con diferentes entradas, y busca las diferencias estadísticas entre subconjuntos de ejecuciones particulares que estén relacionados con bits de claves particulares. El señor Krocher ha constatado que con esta técnica, él interceptó esencialmente todos los sistemas de tarjeta inteligente desplegados por instituciones financieras, compañías de teléfono y de satélite, gobiernos, etc.

Uno de los aspectos más preocupantes del análisis de potencia consiste en que puede ser llevado a cabo de una manera completamente indetectable. Muchos tipos de tarjetas inteligentes personales son utilizadas insertándolas en lectores de tarjetas inteligentes controlados por entidades posiblemente deshonestas. Una tarjeta ATM puede ser utilizada para retirar dinero en efectivo desde una máquina extraña operada por una institución financiera no familiar, una tarjeta de crédito puede ser utilizada para pagar mercancías en un almacén afiliado a la mafia, y una tarjeta de tipo Mondex puede ser utilizada para transferir dinero a un monedero propiedad de un taxista deshonesto. En alguno de esos casos, las tarjetas inteligentes que no sean devueltas (o que son devueltas con daños evidentes debidos a un fallo o a ataques para sondeos), deberán ser inmediatamente denunciadas. Sin embargo, el análisis de potencia puede ser llevado a cabo sin dejar ningún rastro detectable siempre que se utilice la tarjeta. El resultado de un ataque de ese tipo consiste probablemente en la creación de tarjetas duplicadas o en la generación de pagos no-relacionados, que podrían ser muy difíciles de evitar.

Los ataques de potencia se basan en la observación de que la curva de potencia detallada de una tarjeta inteligente típica (que describe cómo cambia con el tiempo la corriente alimentada desde el exterior), contiene una enorme cantidad de información acerca de su contenido secreto. Resulta fácil observar la secuencia exacta de eventos (en forma de puertas individuales que conmutan a conexión o a desconexión) durante la ejecución de cada instrucción. Por ejemplo, las curvas de consumo de potencia de las operaciones de adición y de multiplicación tienen formas completamente diferentes, y la potencia total consumida al escribir 0..0 y 1..1 en la memoria, es apreciablemente diferente. De hecho, es posible extraer visualmente la clave secreta de una operación RSA de una tarjeta inteligente típica mediante una simple observación de la curva de potencia consumida, y determinar qué partes aparecen como una cuadratura modular y qué partes aparecen como una multiplicación modular.

Descripción de las técnicas protectoras del estado de la técnica anterior

Tras la publicación de las técnicas SPA/DPA de Kocher, los investigadores y los fabricantes de tarjetas inteligentes empezaron a buscar soluciones. Los intentos por hacer que la potencia consumida por las tarjetas inteligentes sea absolutamente uniforme cambiando su diseño físico, han resultado fallidos, puesto que incluso una pequeña falta de

uniformidad en la curva de consumo de potencia podría ser capturada por osciloscopios digitales sensibles, y analizada para revelar una información útil. Adicionalmente, forzar el hecho de que todas las instrucciones conmuten el mismo número de puertas a conexión o a desconexión en los mismos instantes de tiempo, es un requisito muy poco natural, que incrementa el área y el consumo total de potencia del microprocesador, lo ralentiza, y lo hace más vulnerable a otros tipos de ataques.

Otra solución propuesta ha sido la de usar un condensador a través de las líneas de suministro de potencia, para alisar la curva de consumo de potencia. Sin embargo, las limitaciones físicas han restringido el tamaño del condensador, y se ha dejado suficiente falta de uniformidad en la curva de consumo de potencia como para hacer que ésta sea una solución muy parcial, especialmente frente a DPA. Una tarjeta inteligente de ese tipo se encuentra descrita en el documento FR 2 774 492.

Otras técnicas propuestas incluyen técnicas de aleatorización basadas en software, generadores de ruido aleatorios basados en hardware, instrucciones inusuales, ejecución paralela de varias instrucciones, etc. Sin embargo, el software aleatorizado no sirve de ayuda si el atacante puede seguir instrucciones individuales, y el ruido de hardware puede ser eliminado promediando múltiples curvas de consumo de potencia, y de ese modo proporcionan solamente una protección limitada frente a un atacante determinado equipado con dispositivos de medición sensibles.

Una solución diferente consiste en reemplazar la fuente de alimentación externa por una batería interna en la tarjeta inteligente. Si los atenuadores de potencia presentes en la tarjeta inteligente no están conectados al chip, el consumo de potencia no puede ser medido eternamente por el lector de tarjeta cuando comunica con la tarjeta. Sin embargo, la anchura o espesor de una tarjeta inteligente típica es de 0,76 mm solamente. Puesto que las baterías con un espesor como ese son muy caras, duran un tiempo muy corto y son difíciles de reemplazar, ésta no es una solución práctica.

Una solución alternativa consiste en el uso de una batería recargable en cada tarjeta inteligente. Tal batería puede ser cargada mediante una fuente de alimentación externa, siempre que la tarjeta se inserte en un lector de tarjeta, y de ese modo, no hay que sustituirla con frecuencia. Sin embargo, las baterías recargables delgadas drenan rápidamente incluso cuando no están en uso, y con ello, durante el uso intermitente normal existe un retardo de carga inaceptablemente largo antes de que se pueda empezar a alimentar la tarjeta desde su batería interna. Adicionalmente, las baterías recargables típicas se deterioran después de varios cientos de ciclos de carga, y por ello, la tarjeta tiene que ser reemplazada después de un número relativamente corto de transacciones intermitentes.

La solicitud de Patente Europea EP 1 098 267 A1, que reivindica prioridad del 2 de Noviembre de 1999 y que fue publicada el 9 de Mayo de 2001, y que es por lo tanto relevante como técnica anterior según el Artículo 54(3) EPC únicamente, se refiere a un procedimiento para mantener la inviolabilidad de un micro-módulo de tarjeta de chip frente a un análisis de consumo de corriente, y a un micro-módulo correspondiente. Los datos de un micro-circuito están protegidos frente a ataques por medición de corriente con la utilización de una alimentación intermedia para optimizar el consumo eléctrico del micro-circuito. El suministro intermedio está proporcionado por dos condensadores construidos en el micro-circuito. Los condensadores son conmutados alternativamente y en oposición, entre la alimentación de DC y el terminal de alimentación del micro-circuito. En este ámbito, el documento EP 1 098 261 A1 contiene un procedimiento de protección de una tarjeta inteligente que incluye un chip de tarjeta inteligente que realiza el cálculo a partir de los ataques cripto-analíticos basados en análisis de potencia, en el que durante al menos una parte del cálculo que se está realizando, se suministra potencia al chip de tarjeta inteligente a partir de la descarga de un condensador contenido en la tarjeta inteligente, y durante alguna otra parte diferente del cálculo que se está realizando, se carga el condensador desde una fuente de alimentación externa mientras dicho condensador se encuentra desconectado del chip. Dicho procedimiento comprende las etapas de: a) alimentar una tarjeta inteligente, que incluye un chip para realizar cálculos, mediante un condensador de descarga conectado al chip mientras está realizando al menos parte de sus cálculos, b) cambiar las conexiones con el condensador para desconectarlo del chip y permitir su carga, y c) cargar el condensador mientras está desconectado del chip. Además, en el documento EP 1 098 267 A1, se describe un aparato correspondiente.

Sumario de la invención

De acuerdo con la presente invención, se emplean un aparato y un procedimiento novedosos para aislar la potencia alimentada a la tarjeta respecto a la potencia consumida por la tarjeta, utilizando un tipo diferente de elemento separador entre ambos. La idea básica consiste en utilizar uno o más condensadores de tal modo que durante al menos parte del cálculo, el chip de la tarjeta inteligente recibe su potencia desde un condensador de descarga contenido en la tarjeta inteligente, y durante alguna parte diferente del cálculo, la fuente de alimentación externa carga este condensador. De esta manera, la curva de alimentación de potencia solamente describirá el proceso de carga de cada condensador y no la curva de consumo real de potencia del chip de tarjeta inteligente. La conmutación puede ser disparada, ya sea por la tensión del condensador de descarga al caer por debajo de un umbral predeterminado, o ya sea por conteo de un cierto número de instrucciones, o ya sea mediante una combinación de esos factores. Esta liberación puede estar limitada a cálculos críticos de seguridad tales como la evaluación de funciones criptográficas, o ser utilizada continuamente siempre que la tarjeta inteligente sea insertada en el lector de tarjeta.

En una forma de diseño preferida de la invención, los condensadores están contruidos directamente en el chip de tarjeta inteligente. Con un diseño cuidadoso, éstos pueden ser colocados a modo de capas metálicas extra sobre el chip.

ES 2 320 405 T3

Cualquier manipulación indebida de estos condensadores es probable que destruya el chip y que borre su memoria. Sin embargo, esto podría tender a necesitar que el condensador sea muy pequeño, y podría complicar probablemente su proceso de fabricación. Alternativamente, en otro diseño preferido de la invención, se incrustan condensadores estándar planos en una cavidad pequeña de la tarjeta de plástico cerca del chip, o los condensadores se construyen por encima de la superficie completa de la tarjeta inteligente disponiendo en sándwich varias capas de plástico y de aluminio en sus 0,76 mm de anchura. Tales construcciones externas añaden solamente unos pocos céntimos al coste de la tarjeta inteligente, y proporcionan una excelente protección frente a mediciones de potencia indetectables durante las transacciones normales. Obsérvese que estas tarjetas inteligentes pueden ser aún sometidas a análisis de potencia destruyendo sus condensadores, pero es probable que las tarjetas inteligentes deglutidas o dañadas sean denunciadas por sus propietarios y puestas en lista negra por sus emisores.

La alternativa de condensador tiene las claras ventajas que siguen frente a la alternativa de batería:

1. Los condensadores son más pequeños que las baterías, y son más fáciles de incrustar en el chip o en la tarjeta de plástico cerca del chip;
2. Los condensadores son más baratos que las baterías, y solamente cuestan unos pocos céntimos;
3. Los condensadores pueden ser recargados un número ilimitado de veces, mientras que las baterías se deterioran después de varios cientos de ciclos de carga;
4. Los condensadores no tiene los efectos memoria de las baterías recargables, y pueden ser recargados sin efectos colaterales incluso aunque no hayan sido completamente descargados;
5. Los condensadores pueden ser cargados en una fracción de segundo, y de ese modo, su uso intermitente no representa ningún problema;
6. Cuando los condensadores se cargan y se descargan alternativamente, el promedio de corriente consumida desde la fuente de alimentación es aproximadamente igual al promedio de corriente consumida por el chip.

Los lectores estándar de tarjetas pueden ser incapaces de suministrar la gran cantidad de corriente inicial que se necesita si se pretende cargar la batería durante el primer segundo, y después utilizarla para alimentar el chip durante diez segundos.

La única desventaja de la alternativa de condensador consiste en que solo puede alimentar potencia al chip durante unas decenas de microsegundos antes de que su tensión sea demasiado baja. Sin embargo, puesto que los condensadores pueden ser recargados repetidamente desde la fuente de alimentación externa, esto no es un problema incluso aunque el cálculo global sea mucho más largo.

Si un atacante intenta llevar a cabo un análisis de potencia sobre la corriente alimentada a la tarjeta, solamente podrá ver la curva de caída exponencial estándar de un condensador de carga, y no las diminutas fluctuaciones de potencia causadas por la ejecución de instrucciones en el chip de tarjeta inteligente. La única información que puede obtener es la corriente total consumida por todas las operaciones del chip durante el período de descarga, puesto que esto afectará al siguiente período de carga. Por esta razón, este período se hace tan grande como sea posible, con el fin de minimizar la fuga residual de información. Un simple cálculo muestra que un condensador estándar de 0,1 microfaradios puede suministrar los 5 miliamperios requeridos por un chip de tarjeta inteligente típica durante un período de 20 microsegundos con una caída de tensión de solo 1 voltio (es decir, desde 6 voltios hasta 5 voltios). A la velocidad de reloj estándar de 5 megahertzios, el chip realiza alrededor de 100 instrucciones en 20 microsegundos, y de ese modo, la información residual que puede ser estudiada es la potencia total consumida por el chip durante 100 operaciones consecutivas, lo que no resulta muy informativo. Para hacer que sea incluso menos informativo, las instrucciones y los datos utilizados en tales lotes de 100 instrucciones pueden ser equilibrados cuidadosamente, lo que resulta mucho más fácil que equilibrar la potencia consumida por el chip en todos los instantes posibles durante la ejecución de todas las instrucciones posibles. Alternativamente, se puede añadir una circuitería simple al chip para descargar el condensador hasta una tensión prefijada durante una duración de tiempo prefijada con anterioridad a conectarlo a la fuente de alimentación externa como parte del proceso de conmutación. Por ejemplo, la fuente de alimentación externa puede cargar el condensador desde 4,5 hasta 6 voltios, el chip lo descarga hasta $5 \pm 0,3$ voltios, y la circuitería de conmutación lo descarga rápidamente hasta 4,5 voltios exactamente. En ese caso, las mediciones externas de potencia son inútiles, puesto que los condensadores de carga están siempre en el mismo estado con independencia del programa ejecutado o de los datos procesados en el chip.

Otras ventajas y objetos adicionales de la invención, se pondrán de manifiesto a partir de la descripción detallada que sigue de realizaciones preferidas cuando se toman junto con los dibujos anexos.

Breve descripción de los dibujos

La Figura 1 es un diagrama de circuito esquemático que muestra una tarjeta inteligente de acuerdo con la invención, que utiliza dos condensadores, y

La Figura 2 es un diagrama de circuito esquemático que muestra una tarjeta inteligente de acuerdo con la invención, que utiliza un condensador.

Descripción detallada de las realizaciones preferidas

Haciendo ahora referencia a los dibujos, las realizaciones preferidas van a ser descritas con mayor detalle. La primera realización, descrita en la Figura 1, muestra una tarjeta 10 inteligente que contiene un chip 1 de tarjeta inteligente. El objeto de la primera realización está previsto que permita al chip de tarjeta inteligente (señalado mediante 1) operar continuamente sin estar conectado directamente a la fuente de alimentación externa (indicada mediante 2) durante la totalidad, o durante una parte, de su cálculo. Ésta contiene dos condensadores (indicados mediante 3 y 4), los cuales están conectados a contactos (indicados mediante 7) del chip de tarjeta inteligente. Estos contactos 7 están conectados a través de cuatro transistores de potencia (indicados como conmutadores 8), los cuales están controlados por medio de una lógica de conmutación (indicada mediante 9), según se describe en lo que sigue, ya sea a la fuente (2) de alimentación externa, o ya sea a través de dos diodos (indicados mediante 5 y 6) al resto del chip (1a) de tarjeta inteligente.

En la realización preferida de la nueva invención, las conexiones de los dos condensadores alternan de una forma periódica: durante los períodos impares, el primer condensador, ya sea 3 ó 4, está conectado a la alimentación, y el segundo condensador, ya sea 4 ó 3, respectivamente, está conectado al chip, y durante los períodos pares las conexiones se invierten. La secuencia preferida de acciones de los transistores de potencia que están controlados por la lógica de conmutación, es:

1. El primer condensador está desconectado de la alimentación externa;
2. El primer condensador está conectado al chip;
3. El segundo condensador está desconectado del chip;
4. El segundo condensador está conectado a la fuente de alimentación externa.

Con esta secuencia de acciones, el chip de tarjeta inteligente está siempre alimentado por al menos un condensador, pero la fuente de alimentación externa no está nunca conectada directamente al chip de tarjeta inteligente. Los condensadores están conectados a través de diodos para evitar fugas desde el condensador cargado hasta el condensador descargado durante el breve instante en que están conectados en paralelo con el chip.

Otra realización preferida de la presente invención ha sido descrita en la Figura 2. Ésta utiliza solamente un condensador (11), el cual se conecta alternativamente al chip (12) de la tarjeta (20) inteligente y a la alimentación (13) externa por medio de dos transistores (14) de potencia bajo el control de una lógica (15) de conmutación. En esta realización, el chip (12) ha de ser interrumpido y desconectado de la alimentación después de cada ciclo de descarga, lo que ralentiza su funcionamiento, y podría provocar posiblemente problemas con algunos tipos de memorias volátiles incluidas en chips.

Aunque la presente invención ha sido mostrada y descrita en términos de realizaciones preferidas, cambios y modificaciones resultarán, no obstante, evidentes para los expertos en la materia, a partir del conocimiento de la descripción y de las enseñanzas de la misma.

Referencias citadas en la descripción

La lista de referencias citadas por el solicitante se proporciona únicamente por conveniencia para el lector. Ésta no forma parte del documento de Patente Europea. Incluso aunque se ha puesto un gran cuidado en el listado de las referencias, no se excluyen los errores u omisiones y la EPO declina toda responsabilidad en ese sentido.

Documentos de Patente citados en la descripción

- FR 2774492
- EP 1098267 A1

Literatura no de patentes citada en la descripción

- Sobre la Importancia de Comprobar Protocolos Criptográficos respecto a Fallos. D. **BONEH**; R.A. **DEMILLO**; R.J. **LIPTON**. Proceedings of Eurocrypt 97. *Springer Verlag*, 1997, 37-51.

- O. **KOMMERLING**; M. **KUHN**. Principios de Diseño para Procesadores de Tarjeta Inteligente Resistentes a la Manipulación Indebida, [http://www.cl.cam.ac.uk/~mgk25/sc99-tamnpaper\[-slides\].pdf](http://www.cl.cam.ac.uk/~mgk25/sc99-tamnpaper[-slides].pdf)

- Temporización de Ataques sobre Implementaciones de DiffieHellman, RSA, DSS, y Otros Sistemas. P. **KOCHER**. Proceedings of Crypto 96. *Springer Verlag*, 1996, 104-113.

ES 2 320 405 T3

- Principios de Diseño para Procesadores de Tarjeta Inteligente Resistentes a la Manipulación Indebida. O. **KOMMERLING**; M. **KUHN**. Proceedings of USENIX Workshop on Smartcard Technology. *USENIX Association*, 1999, 9-20.

5 - PAUL **KOCHER**; P. **KOCHER**; J. **JAFFE**; B. **JUN**. Introducción al Análisis de Potencia Diferencial y Ataques Relacionados. *Cryptography Research*, 1998, <http://www.cryptography.com/ldpa/technical/index.html>

10

15

20

25

30

35

40

45

50

55

60

65

REIVINDICACIONES

1. Un procedimiento de protección de una tarjeta (10) inteligente frente a ataques cripto-analíticos basados en análisis de potencia, incluyendo la tarjeta (10) inteligente un chip (1) de tarjeta inteligente que realiza cálculos, incluyendo el procedimiento, durante al menos parte del cálculo que se está realizando, proporcionar potencia al chip (1) de tarjeta inteligente desde un condensador (3, 4) de descarga contenido en la tarjeta (10) inteligente, y durante alguna parte diferente del cálculo que se está realizando, cargar el condensador (3, 4) desde una fuente de alimentación externa.
2. El procedimiento de la reivindicación 1, en el que el chip (1) de tarjeta inteligente no se conecta directamente a la fuente (2) de alimentación externa en ningún momento durante el cálculo.
3. El procedimiento de la reivindicación 1, en el que el chip (1) de tarjeta inteligente no se conecta directamente a la fuente (2) de alimentación externa cuando procesa datos secretos.
4. El procedimiento de la reivindicación 1, en el que el chip (1) de tarjeta inteligente no se conecta directamente a la fuente (2) de alimentación externa cuando realiza cálculos criptográficos.
5. El procedimiento de la reivindicación 1, en el que la tarjeta (10) inteligente contiene un condensador (3, 4), que se conecta alternativamente al chip (1) de tarjeta inteligente y a la fuente (2) de alimentación externa.
6. El procedimiento de la reivindicación 5, en el que el chip (1) de tarjeta inteligente opera durante aquellos instantes en los que está conectado al condensador (3, 4), y se interrumpe durante aquellos instantes en los que el condensador (3, 4) está conectado a la fuente (2) de alimentación externa.
7. El procedimiento de la reivindicación 1, en el que la tarjeta (10) inteligente contiene al menos dos condensadores (3, 4), que están conectados de tal manera que en cualquier instante dado, uno de los al menos dos condensadores (3, 4) está conectado al chip (1) de tarjeta inteligente, y otro de los al menos dos condensadores (3, 4) está conectado a la fuente (2) de alimentación externa.
8. El procedimiento de la reivindicación 7, en el que las conexiones de los dos condensadores (3, 4) se invierten repetidamente, y el chip (1) de tarjeta inteligente opera de forma continuada.
9. El procedimiento de la reivindicación 7, en el que las conexiones de los dos condensadores (3, 4) se invierten repetidamente de una manera periódica, y el chip (1) de tarjeta inteligente opera de forma continuada.
10. El procedimiento de la reivindicación 1, en el que la tarjeta (10) inteligente contiene al menos tres condensadores, los cuales están conectados de tal manera que en cualquier momento dado, al menos uno de los al menos tres condensadores está conectado al chip (1) de tarjeta inteligente, y al menos otro de los al menos tres condensadores está conectado a la fuente (2) de alimentación externa.
11. Un procedimiento de protección de una tarjeta (20) inteligente frente a ataques cripto-analíticos basados en análisis de potencia, incluyendo la tarjeta (20) inteligente un chip (12) para realizar cálculos, y un condensador (11), que se conecta alternativamente al chip (12) de tarjeta inteligente y a una fuente de alimentación externa, comprendiendo el procedimiento las etapas de:
 - a) alimentar el chip (12) de tarjeta inteligente mediante dicho condensador (11) de descarga conectado al chip (12) mientras realiza al menos parte de sus cálculos;
 - b) cambiar las conexiones con dicho condensador (11) para desconectarlo del chip (12) y permitirle que cargue, y
 - c) cargar el citado condensador (11) mientras está desconectado del chip (12).
12. El procedimiento de la reivindicación 1 u 11, en el que se dispara un cambio en el suministro de potencia al chip (1; 12) de tarjeta inteligente para cargar el condensador (3, 4; 11) mediante una tensión a través del condensador (3, 4; 11) que exceda de, o que caiga por debajo de, un cierto umbral.
13. El procedimiento de la reivindicación 1, 11 ó 12, en el que se dispara un cambio en la carga del condensador (3, 4; 11) para suministrar potencia al chip (1; 12) de tarjeta inteligente mediante una tensión a través del condensador (3, 4; 11) que exceda de, o que caiga por debajo de, un cierto umbral.
14. El procedimiento de la reivindicación 1 u 11, en el que se dispara un cambio en el suministro de potencia al chip (1; 12) de tarjeta inteligente para cargar el condensador (3, 4; 11) mediante el conteo de un número de ciclos de reloj.

ES 2 320 405 T3

15. El procedimiento de la reivindicación 1, 11 ó 14, en el que se dispara un cambio en la carga del condensador (3, 4; 11) para el suministro de potencia al chip (1; 12) de tarjeta inteligente mediante el conteo de un número de ciclos de reloj.
- 5 16. El procedimiento de la reivindicación 1 u 11, en el que se dispara un cambio en el suministro de potencia al chip (1; 12) de tarjeta inteligente para la carga del condensador (3, 4; 11) mediante una tensión a través del condensador (3, 4; 11) que exceda de, o que caiga por debajo de, un cierto umbral al principio de un ciclo de reloj.
- 10 17. El procedimiento de la reivindicación 1, 11 ó 16, en el que se dispara un cambio en la carga del condensador (3, 4; 11) para el suministro de potencia al chip (1; 12) de tarjeta inteligente mediante una tensión a través del condensador (3, 4; 11) que exceda de, o que caiga por debajo de, un cierto umbral al comienzo de un ciclo de reloj.
- 15 18. El procedimiento de la reivindicación 1 u 11, en el que una circuitería adicional en la tarjeta (10; 20) inteligente descarga el condensador (3, 4; 11) hasta una tensión prefijada, con anterioridad a un cambio en el suministro de potencia al chip (1; 12) de tarjeta inteligente para la carga del condensador (3, 4; 11).
- 20 19. Tarjeta (10; 20) inteligente, que dispone de medios para protegerla frente a ataques cripto-analíticos basados en análisis de potencia, conteniendo la tarjeta inteligente:
- 25 a) un chip (1; 12) de tarjeta inteligente para realizar cálculos;
- b) un condensador (3, 4; 11);
- 25 c) contactos para conectar una fuente de alimentación externa al condensador, y que se **caracteriza** porque comprende además,
- d) una lógica (9, 15) de conmutación para conectar alternativamente el condensador,
- 30 a. al chip de tarjeta inteligente para alimentar el citado chip durante al menos parte del cálculo que se está realizando, y
- b. a una fuente de alimentación externa para ser cargado por la citada fuente de alimentación.
- 35 20. Tarjeta inteligente de acuerdo con la reivindicación 19, en la que el condensador se carga durante alguna parte diferente del cálculo que se está realizando.
21. Tarjeta inteligente de acuerdo con la reivindicación 19 ó 20, en la que el chip (1; 12) de tarjeta inteligente no está conectado directamente a la fuente (2; 13) de alimentación externa en ningún momento durante el cálculo.
- 40 22. Tarjeta inteligente de acuerdo con la reivindicación 19 ó 20, en la que el chip (1; 12) de tarjeta inteligente no está conectado directamente a la fuente (2; 13) de alimentación externa cuando se procesan datos secretos.
23. Tarjeta inteligente de acuerdo con la reivindicación 19 ó 20, en la que el chip (1; 12) de tarjeta inteligente no está conectado directamente a la fuente (2; 13) de alimentación externa cuando se realizan cálculos criptográficos.
- 45 24. Tarjeta inteligente de acuerdo con la reivindicación 19 ó 20, en la que la tarjeta (20) inteligente contiene solamente un condensador (11), que se conecta alternativamente al chip (12) de tarjeta inteligente y a la fuente (13) de alimentación externa.
- 50 25. Tarjeta inteligente de acuerdo con la reivindicación 19 ó 21, en la que la tarjeta (10; 20) inteligente contiene al menos dos condensadores (3, 4), los cuales están conectados de tal modo que en cualquier momento dado, uno de los al menos dos condensadores (3, 4) está conectado al chip (1; 12) de tarjeta inteligente, y otro de los al menos dos condensadores (3, 4) está conectado a la fuente (2; 13) de alimentación externa.
- 55 26. Tarjeta inteligente de acuerdo con la reivindicación 25, en la que la lógica (9; 15) de conmutación es tal que las conexiones de los dos condensadores (3, 4) se invierten repetidamente, y el chip (1; 12) de tarjeta inteligente opera de forma continuada.
- 60 27. Tarjeta inteligente de acuerdo con la reivindicación 19 ó 20, en la que la lógica (9; 15) de conmutación es tal que el cambio de conexión se dispara mediante una tensión a través del condensador (3, 4; 11) que exceda de, o que caiga por debajo de, un cierto umbral.
28. Tarjeta inteligente de acuerdo con la reivindicación 19 ó 20, en la que la lógica (9; 15) de conmutación es tal que el cambio de conexión se dispara por conteo de un número de ciclos de reloj.
- 65 29. Tarjeta inteligente de acuerdo con la reivindicación 19 ó 20, en la que la lógica (9; 15) de conmutación es tal que la tarjeta (10; 20) inteligente descarga el condensador (3, 4; 11) hasta una tensión prefijada, antes de conectarlo a la fuente (2; 13) de alimentación externa como parte del proceso de conmutación.

ES 2 320 405 T3

30. Tarjeta inteligente de acuerdo con la reivindicación 19 ó 20, en la que la lógica (9; 15) de conmutación es tal que el cambio de conexión se dispara mediante una tensión a través del condensador (3, 4; 11) que exceda de, o que caiga por debajo de, un cierto umbral al comienzo de un ciclo de reloj.

- 5 31. Tarjeta inteligente de acuerdo con la reivindicación 19 ó 20, en la que la tarjeta (10; 20) inteligente contiene al menos tres condensadores, los cuales están conectados de tal manera que, en cualquier momento dado, uno de los al menos tres condensadores está conectado al chip (1; 12) de tarjeta inteligente, y otro de los al menos tres condensadores está conectado a la fuente (2; 13) de alimentación externa.

10

15

20

25

30

35

40

45

50

55

60

65

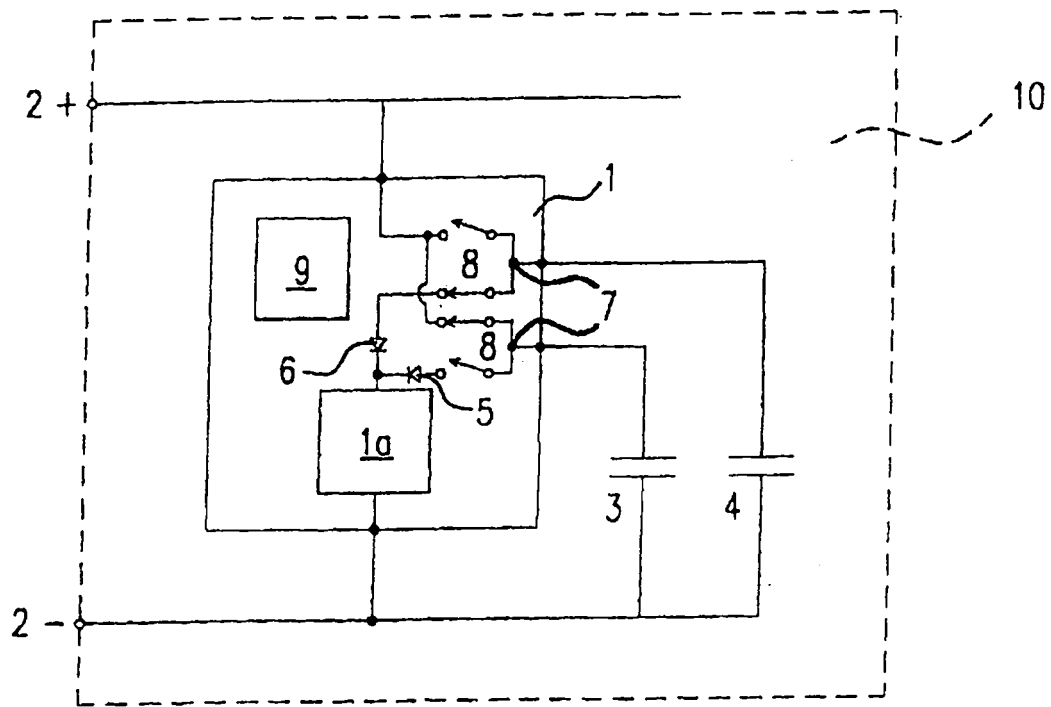


FIG. 1

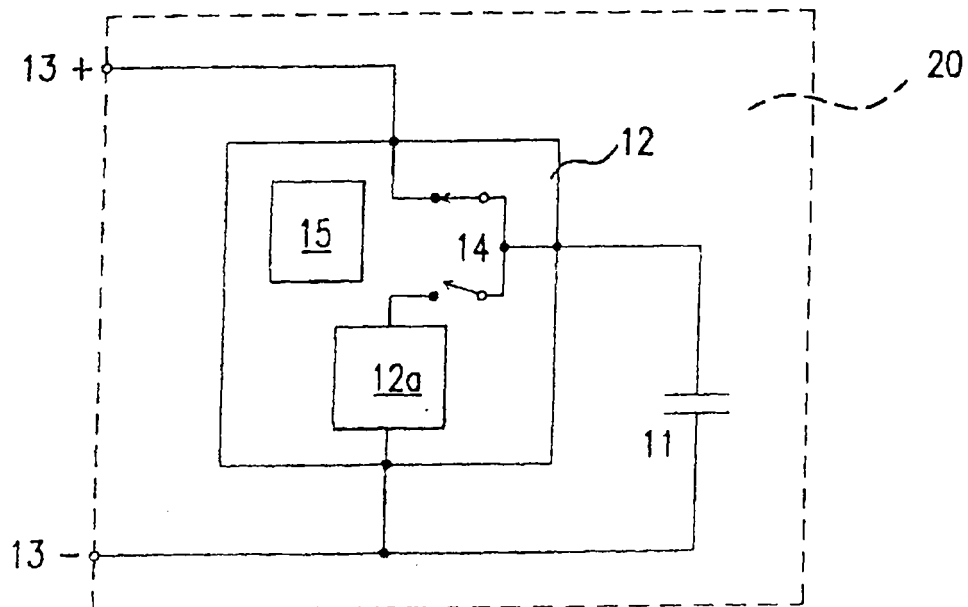


FIG. 2