(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 731 591**

(51) Int. CI.:

G06F 21/75 (2013.01)
H04L 9/06 (2006.01)
H04L 9/00 (2006.01)
G01R 31/317 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **11.02.2009 PCT/EP2009/051600**

(87) Fecha y número de publicación internacional: **03.09.2009 WO09106428**

(96) Fecha de presentación y número de la solicitud europea: **11.02.2009 E 09715962 (8)**

(97) Fecha y número de publicación de la concesión europea: **27.03.2019 EP 2248061**

(54) Título: **Procedimiento de prueba de circuitos de criptografía, circuito de criptografía asegurado adecuado para ser probado y procedimiento de cableado de tal circuito**

(30) Prioridad:

25.02.2008 FR 0851184

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.11.2019

(73) Titular/es:

INSTITUT MINES TELECOM (100.0%)
Institut Mines Telecom
75014 Paris, FR

(72) Inventor/es:

GUILLEY, SYLVAIN y
DANGER, JEAN-LUC

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento de prueba de circuitos de criptografía, circuito de criptografía asegurado adecuado para ser probado y procedimiento de cableado de tal circuito

La presente invención se refiere a un procedimiento de prueba de circuitos de criptografía. También se refiere a un circuito de criptografía asegurado adecuado para ser probado.

Los circuitos de criptografía, como la mayoría de los circuitos electrónicos, deben someterse a pruebas antes de su explotación. Las pruebas de los circuitos de criptografía son, por lo tanto, parte del problema general de la prueba de los circuitos electrónicos, pero con ciertas particularidades.
Las pruebas permiten verificar después de la fabricación que los circuitos cumplen bien con sus funciones previstas.
Un circuito puede constar, de hecho, de varios defectos de fabricación, que provienen, en particular:

- de una falta de homogeneidad de las sustancias químicas usadas que conducen a la degradación del rendimiento;
- de la deposición de una impureza tal como el polvo, por ejemplo, que provoca una destrucción local del circuito;
- la omisión de una etapa de fabricación que causa el mal funcionamiento del circuito;
- de una confusión en el uso de máscaras de fabricación.

Entre estos defectos, los problemas más imprevisibles provienen de la deposición de polvo que puede llevar a:

- un cortocircuito, es decir, la conexión no deseada de dos equipotenciales o "nodos";
- o un corte, es decir, la desconexión de un nodo, dando lugar a dos equipotenciales.

En una fase de prueba posterior a la fabricación, un circuito se alimenta con tensión y ciertas de sus entradas, muy específicas, reciben señales de prueba. En respuesta a estas señales de prueba, un dispositivo de prueba puede efectuar verificaciones de funcionamiento. Para que el circuito sea comprobable, debe cumplir dos condiciones:

- el circuito debe ser controlable, es decir, que sea posible llevar el circuito a un estado conocido;
- debe ser observable, es decir, que sea posible comparar una característica del circuito en su estado conocido con una característica de referencia teórica, obtenida por ejemplo por simulación.

La implementación de estas dos condiciones permite que el dispositivo de prueba forme un conjunto de vectores de prueba que son tantas verificaciones diferentes que se deben realizar en el circuito.
Un primer parámetro clave de una prueba es su cobertura. La cobertura expresa la proporción de nodos lógicos efectivamente verificados. Para asegurarse de que un circuito es funcional, se desea una cobertura que tiende hacia el 100 %, pero muy rara vez se logra en la práctica.
Un segundo parámetro clave de la prueba es su coste, que depende, en particular, de dos factores:

- el número de vectores de prueba, debiendo esta cantidad reducirse al mínimo ya que condiciona la duración de la interacción con el circuito, siendo el coste proporcional a esta duración, en particular, es importante que la cadencia de la prueba sea superior al caudal de fabricación de los circuitos, de lo contrario, el factor que limita la producción se convierte en la prueba en sí misma. Esta es, en particular, una de las razones por las que la cobertura nunca es del 100 %;
- la inserción del hardware de prueba, dado que es raro que los circuitos puedan ser probados tales como, según lo convenido de llamar a las pruebas funcionales, a menudo se debe agregar hardware adicional para permitir la controlabilidad o la observabilidad de los circuitos a probar, teniendo este hardware un coste que reduce el atractivo de una solución de hardware en comparación con una solución de software.

Varias técnicas de prueba son conocidas. Para la prueba funcional, no se agrega ningún hardware. Simplemente se verifica que las salidas del circuito a probar sean de acuerdo con una secuencia bien determinada de las entradas de este mismo circuito. Desafortunadamente, este procedimiento de prueba tiene una cobertura baja y requiere una gran cantidad de vectores de entrada. Es, por lo tanto, prácticamente inaplicable.
En el caso de las pruebas en cadena, el circuito se modifica para que pueda cumplir dos papeles, por una parte, su funcionalidad y, por otro lado, la realización de un registro de desfase que conecta todos los elementos secuenciales del circuito, generalmente básculas D o DFF. Por lo tanto, el sobrecoste está relacionado con el número de básculas del circuito, necesitando éstas dos entradas, una primera entrada llamada "test in" y una segunda entrada llamada "test enable", lo que hace crecer la superficie de un circuito. Además, un enrutamiento funcional también se agrega al enrutamiento entre básculas, reduciendo las posibilidades de enrutamiento, propiedad crítica en un circuito restringido por interconexión. Finalmente, debe tenerse en cuenta que la prueba de cadena permite probar los nodos pegados un mismo valor lógico. Este modelo de error no es rigurosamente igual a los verdaderos errores que son los cortocircuitos y los cortes.
En el procedimiento de prueba analógico llamado IDDQ, el circuito a probar se coloca en un estado y luego, con ayuda de un amperímetro, se estudia la corriente consumida por el circuito. Este procedimiento hace posible, en particular, detectar cortocircuitos en función del valor de la corriente consumida. No requiere hardware necesario para la observabilidad. Sin embargo, el procedimiento IDDQ es lento. También es parcial, ya que solo permite detectar los cortocircuitos.
En el llamado procedimiento BIST según la expresión inglesa "Built-In Self Test", se agrega un módulo exterior a la

parte a probar. Su papel es, en particular, tomar el control del circuito a probar y realizar su prueba de forma dinámica. Este procedimiento se aplica a bloques simples, con funcionalidad trivial, como una memoria, por ejemplo, donde se lee precisamente lo que se ha escrito. No es adecuado para un circuito complejo del tipo de criptografía.

Además de su complejidad, los circuitos de criptografía presentan restricciones antinómicas con respecto a su prueba. En efecto, por un lado, un solo error en la funcionalidad puede comprometer la integridad de los secretos, de ahí la necesidad de una prueba exhaustiva, pero, por otro lado, la adición de hardware de prueba que permiten la observabilidad interna, destruye la seguridad del circuito. En particular, un solo bit de una variable intermedia de un algoritmo de criptografía accesible para un atacante puede permitirle volver a los secretos mediante el análisis criptográfico. De este modo, es necesario probar los circuitos asegurados, pero ningún procedimiento de prueba existente es satisfactorio. La prueba funcional no permite una cobertura suficiente, mientras que una cobertura del 100 % es esencial para un circuito de criptografía. La prueba de encadenamiento de básculas DFF abre una vulnerabilidad ya que un atacante puede llegar, lógicamente, además, para leer el estado del procesador de cifrado, más precisamente sus claves o valores intermedios. Para contrarrestar este tipo de ataque, una solución propone hacer aleatoria la estructura de encadenamiento. Sin embargo, este enfoque viola el principio de Kerckhoff que impone la concentración de la seguridad en las claves de tamaño reducido y no en la complejidad y la confidencialidad de la implementación. La prueba IDDQ es demasiado cara y fragmentaria, mientras que la prueba BIST no está adaptado para el cálculo criptográfico.

El documento: PENGYUAN YU, "Implementation of DPA-Resistant Circuit for FPGA", 24 de abril de 2007 (24-04-2007), BLACKSBURG, VIRGINIA, Estados Unidos extraído de rinternet:URL:http://scholar.lib.vt.edu/theses/available/etd-04302007-134556/ unrestricted/Thesis.pdf, describe la implementación de un circuito FPGA resistente a los ataques de análisis de consumo.

Un objeto de la invención es, en particular, permitir la prueba de circuitos de criptografía mediante la superación de las restricciones antinómicas mencionadas anteriormente, y más generalmente los inconvenientes de los procedimientos anteriores. Para tal fin, el objeto de la invención es un procedimiento para probar un circuito de criptografía que consta de registros y puertas lógicas interconectadas por un conjunto de nodos, efectuando dicho procedimiento un análisis diferencial de consumo (DPA) que consta de:

- una fase de adquisición de mediciones de trazas de consumo al nivel de todos los nodos que funcionan como vectores de señales de prueba a la entrada del circuito;
- una fase de análisis de la tasa de actividad de cada nodo a partir de las mediciones de trazas de consumo, considerándose un nodo en buen funcionamiento cuando su tasa de actividad es de acuerdo con un modelo de predicción de su actividad.

En el caso donde el circuito de criptografía no esté asegurado, el análisis diferencial por DPA se efectúa como prueba, como si se tratara de hacer un ataque para encontrar el secreto criptográfico. De este modo, la conformidad de la actividad de cada nodo con un predictor de actividad permite establecer su integridad. Sin embargo, el DPA permanece largo porque el predictor depende del secreto criptográfico, se desconoce, y se requiere un gran número de trazas de consumo (del orden de unos pocos miles). Si el circuito criptográfico dispone de un mecanismo de personalización del secreto, entonces es posible inyectar un secreto criptográfico "conocido" para que la prueba de DPA sea menos larga ya que se necesitan menos trazas de consumo.

La personalización del secreto se hará en este caso después de la prueba para asegurar la protección criptográfica.

En el caso donde el circuito de criptografía está asegurado por una lógica diferencial estructurada en torno a un primer semicircuito asociado a un segundo semicircuito de lógica complementaria, la actividad general del circuito está equilibrada y el análisis diferencial del consumo no puede funcionar. Según la invención, la fuente Vdd1 de alimentación eléctrica del primer semicircuito está disociada de la fuente Vdd2 de alimentación eléctrica del segundo semicircuito, haciéndose el análisis diferencial del consumo posible al medir la actividad en cada semicircuito. El análisis se realiza en paralelo en cada semicircuito, estando las dos alimentaciones reagrupadas en una misma alimentación eléctrica después de la prueba.
Los componentes del primer semicircuito están conectados, por ejemplo, a través de unas líneas de alimentación a una primera fuente Vdd1 de tensión y los componentes del segundo semicircuito se alimentan a través de unas líneas de alimentación a una segunda fuente Vdd2 de tensión, siendo las dos fuentes de tensión distintas, estando las líneas de alimentaciones conectadas después de la prueba. En otro modo de implementación, los componentes del primer semicircuito están conectados, por ejemplo, a través de unas líneas de masa a un primer potencial Gnd1 de referencia y los componentes del segundo semicircuito se alimentan a través de unas líneas de masa a un segundo potencial Gnd2 de referencia, estando los dos potenciales de referencia disociados, estando las líneas de masa conectadas después de la prueba.
Ventajosamente, las fuentes de alimentaciones Vdd1, Vdd2 se puede reagrupar al final de la fase de adquisición.
La prueba de análisis diferencial puede limitarse a los nodos de los registros del circuito que permiten deducir la integridad de los nodos de las puertas lógicas entre estos registros.
Un procedimiento de cableado de la alimentación está asociado con el procedimiento de prueba descrito anteriormente para la lógica asegurada. El primer semicircuito dispone de una primera vía de alimentación eléctrica y una segunda vía de alimentación eléctrica se asigna al segundo semicircuito, de modo que cada semicircuito se pueda probar

mediante un análisis diferencial de consumo (DPA) en paralelo al otro semicircuito, siendo las dos vías de alimentación adecuadas para cortocircuitarse.
En un ejemplo de realización particular:

- la primera vía de alimentación consta de un primer anillo conductor periférico adecuado para conectarse a una primera fuente Vdd1 de tensión y conectarse eléctricamente a unas líneas de alimentación de los componentes del primer semicircuito y;
- la segunda vía de alimentación consta de un segundo anillo conductor periférico adecuado para conectarse a una segunda fuente Vdd2 de tensión y conectarse eléctricamente a unas líneas de alimentación de los componentes del segundo semicircuito;

siendo los dos anillos adecuados para cortocircuitarse.
En otro ejemplo de realización:

- la primera vía de alimentación consta de un primer anillo conductor periférico adecuado para conectarse a un primer potencial Gnd1 de masa y conectarse eléctricamente a unas líneas de masa de los componentes del primer semicircuito y;
- la segunda vía de alimentación consta de un segundo anillo conductor periférico adecuado para conectarse a un segundo potencial Gnd2 de masa y conectarse eléctricamente a unas líneas de masa de los componentes del segundo semicircuito;

siendo los dos anillos adecuados para cortocircuitarse.
En estos dos modos de realización, los dos anillos están, por ejemplo, conectados entre sí por antifusibles, estando realizado el cortocircuito entre los dos anillos por la fusión de los antifusibles.
Los dos anillos también pueden cortocircuitarse en la caja del circuito.
La invención también tiene por objeto un procedimiento de cableado de las alimentaciones de un circuito de criptografía asegurado que consta de un primer semicircuito asociado con un segundo semicircuito que funciona en lógica complementaria, siendo una primera vía de alimentación eléctrica asignada al primer semicircuito y siendo una segunda vía de alimentación eléctrica asignada al segundo semicircuito, de modo que cada semicircuito se pueda probar mediante un análisis diferencial de consumo (DPA) independientemente del otro semicircuito, siendo las dos vías de alimentación adecuadas para cortocircuitarse.

Otras características y ventajas de la invención emergerán con ayuda de la siguiente descripción realizada en relación con los dibujos adjuntos que representan:

- la figura 1, una ilustración de un camino de datos combinatorio de un algoritmo de criptografía dentro de un circuito;
- la figura 2, una presentación de las fases de un análisis diferencial de consumo usado por el procedimiento según la invención;
- la figura 3, una ilustración de una estructura de circuito de criptografía asegurado;
- La figura 4, un ejemplo de trazas de consumo adquiridas en las dos mitades de un circuito asegurado provisto de dos alimentaciones separadas;
- la figura 5, un ejemplo de realización de un circuito según la invención y un procedimiento para cortocircuitar las vías de alimentación previamente disociados en un circuito según la invención.

La figura 1 el camino de datos combinatorio de un algoritmo de criptografía dentro de un circuito, entre dos básculas DFF 1, 2 de un registro. Una lógica 10 combinatoria conecta las dos básculas DFF 1, 2. Todas las básculas del circuito están conectadas de este modo. El camino se divide en conos 20 de lógica de tamaño razonable, por ejemplo, inferior a 8 bits, en particular como en el estándar de criptografía DES (Data Encryption Standard). La figura 1 ilustra el caso DES donde los conos 20 tienen tramos 11 de entrada que constan de 6 bits y tramos 12 de salida que constan de 4 bits.
Esta lógica 10 combinatoria, que conecta los registros 1, 2, se realiza a partir de puertas lógicas.
La invención usa el análisis diferencial de consumo para probar el correcto funcionamiento de los circuitos integrados de criptografía, generalmente se usa para atacar los circuitos de criptografía o para caracterizar su nivel de seguridad. El análisis diferencial de consumo, también llamado DPA según el acrónimo en inglés "Differential Power Analysis" permite correlacionar una medición de una cantidad física emitida por un circuito, como su consumo eléctrico instantáneo, por ejemplo, a una parte de su actividad. La técnica DPA se usa generalmente para atacar circuitos de criptografía, como se describe en el artículo de P. Kocher, J. Jaffe y B. Jun "Differential Power Analysis: Leaking Secrets" en Proceedings de CRYPTO'99, volumen 1666 de LNCS, páginas 388-397, Springer-Verlag, o también para evaluar su nivel de seguridad. En particular, se ha demostrado, tanto teórica como experimentalmente, que el DPA permite predecir la actividad de una variable booleana en un circuito, como muestra, en particular, el artículo de S. Guilley, Ph. Hoogvorst, R. Pacalet y J. Schmidt "Improving Side-Channel Attacks by Exploiting Substitution Boxes Properties" en BFCA - http://www.liafa.jussieu.fr/bfca/, páginas 1-25, 2007, mayo 02-04, París. En la tecnología CMOS de 0,13 µm, el número de mediciones, llamadas trazas de consumo, necesarias para realizar el análisis DPA de un bloque cableado tal como un ASIC, por ejemplo, desprotegido, que realiza el algoritmo de cifrado DES es inferior a mil. Este número se presenta en la tabla a continuación, que detalla el número mínimo de trazas a analizar para encontrar 6 bits de clave. El algoritmo DES hace intervenir, para cada ronda, 8 x 6 = 48 bits de clave que entran en una caja de sustitución llamada "sbox".

Análisis \ Sbox nº	S1	S2	S3	S4	S5	S6	S7	S8	Trazas necesarias = Máx
DPA (claro aleatorio)	228	615	736	510	297	55	272	111	736
DPA (claro seleccionado)	5	31	56	16	17	22	4	4	56

Cabe señalar que las mismas mil trazas de consumo permiten encontrar las ocho palabras de 6 bits de clave. Por esta razón, la tabla resume el número de trazas necesarias por el máximo de trazas por "sbox" y no su suma. Cuando se conoce la clave, el análisis puede acelerarse eligiendo una entrada conocida por el algoritmo, llamada "claro". Una manera de proceder se describe en el artículo de G. Perret "A note on the Plaintext Choice in Power Analysis Attacks" Technical Report from the Ecole Normale Supérieure (ENS), Francia, noviembre, 2005, http://www.di.ens.fr/-piret/publ/power.pdf. Los resultados experimentales se indican en la segunda fila de la tabla anterior.

Como se ha indicado anteriormente, la invención usa DPA para probar circuitos de criptografía. Estos últimos manipulan datos sensibles, por ejemplo, secretos tales como claves o gérmenes, en particular.
Existen dos tipos de circuitos de criptografía, los circuitos no asegurados y los circuitos asegurados. Estos últimos constan de contramedidas para protegerse contra ataques en sus implementaciones, estando estas contramedidas destinadas a despedir a los posibles atacantes. La invención se aplica a circuitos no asegurados y a circuitos asegurados.
La prueba de un circuito de criptografía no asegurado se realiza mediante un DPA en todos los nodos del circuito, más particularmente, al nivel de cada nodo de los registros. Un circuito de criptografía puede constar de varios miles de nodos. Existen esencialmente dos tipos de nodos:

- los equipotenciales salidos de las memorias o registros;
- los equipotenciales salidos de las puertas lógicas.

Es posible efectuar un DPA únicamente en los registros para deducir el estado de los nodos combinatorios y, por lo tanto, encontrar el secreto.
La controlabilidad está asegurada por la naturaleza criptográfica del algoritmo. En efecto, cuando el circuito se fabrica correctamente, la esencia del cálculo hace que cada nodo del circuito con una tasa de actividad cercana a ½. El DPA consiste en distinguir entre trazas donde hay actividad para el nodo (según un predictor o una función de selección) y aquellas donde no hay actividades. Esta diferencia es nula para un nodo cualquiera ya que no hay ninguna conexión entre el predictor y este nodo, y no es cero para el nodo probado. Un nodo se considera, por lo tanto, en buen estado de funcionamiento cuando la actividad observada se correlaciona con la actividad predicha. La observabilidad se puede realizar registro por registro usando una función de selección idónea. Tal función se describe en particular en el artículo de S. Guilley y col. anteriormente mencionado. La cobertura de la prueba es del 100 % ya que la actividad general de todas las puertas se agrega a las trazas de consumo. El número de vectores de prueba es de unos pocos cientos, como se muestra en la tabla anterior. Además, en comparación con la prueba IDDQ en particular, donde las mediciones y la prueba deben ser concomitantes, lo que ralentiza el proceso, la prueba DPA se puede dividir en dos tareas. La adquisición, parte "en línea", que solo requiere unos pocos cientos de mediciones, puede ser seguida por el análisis, parte "fuera de línea", que se puede realizar posteriormente. Esta última etapa, posiblemente codiciosa en el cálculo, solo está, por lo tanto, en el camino crítico.

La figura 2 ilustra así las dos fases de un análisis diferencial del consumo de DPA aplicado para las pruebas según la invención.
Una primera fase 11 realiza la adquisición de las mediciones de trazas de consumo a partir de un juego de vectores de señales de prueba a la entrada del circuito a probar. Los vectores de prueba usados pueden ser los usados para un análisis de DPA convencional.
Una segunda fase 12 analiza la tasa de actividad a partir de las mediciones efectuadas en la etapa de adquisición. La extracción bit a bit es realizable, ya que en los circuitos de criptografía los caminos de datos, a menudo grandes, en la práctica se cortan en conos lógicos de menor tamaño. Por ejemplo, en la cifrado DES, el camino de datos tiene 64 bits de ancho y se corta en tramos de 6 bits como se ilustra por la figura 1.

Como se ha indicado anteriormente, los circuitos asegurados constan de contramedidas para evitar los ataques y, en particular, los ataques de tipo DPA descritos anteriormente. En consecuencia, el procedimiento de prueba expuesto anteriormente no es aplicable, ya que en este caso la posibilidad de prueba implica la posibilidad de un ataque por DPA. Para la prueba de circuitos asegurados, por lo tanto, no es posible probar los valores intermedios mediante un análisis directo del consumo como para los circuitos no asegurados.
La protección de los circuitos asegurados generalmente usa lógicas del tipo DPL (Dual Rail with Precharge Logic). Se conocen dos tipos:

- la lógica de consumo constante, como WDDL (Wave Dynamic Differential Logic) y;
- la lógica de consumo constante promedio, como MDLP (Masked DLP)

En los dos casos, estas lógicas se pueden implementar con celdas estándar, distribuidas por los fabricantes en un kit de diseño. Más precisamente, las puertas que procesan señales complementarias son separables en dos mitades, o

dos redes, estructuras lógicas complementarias, formando una puerta de doble riel de puertas elementales, estando cada puerta elemental asociada con una puerta doble. Una primera mitad que puede llamarse vehículo "real", la cadena de señales útiles, la otra mitad, que puede llamarse vehículo "falso", lleva señales complementarias. Estas puertas de doble riel, que vehicularizan señales lógicas complementarias, impiden los análisis de consumo efectuados por DPA. De hecho, la actividad eléctrica, en términos de consumo, es constante e independiente de los datos lógicos, ya que cuando una puerta pasa a un estado lógico, la puerta dual permanece en el mismo estado y viceversa. Cualquier intento de correlación por análisis DPA está condenado al fracaso.

La figura 3 ilustra tal estructura de circuitos de criptografía asegurados. Esta figura presenta, a modo de ejemplo, dos puertas 21, 22 de doble riel separables en dos mitades que vehicularizan señales complementarias. La primera puerta 21 de doble riel es una puerta "o" (211, 212). La puerta elemental "o" 211 de la primera mitad, recibe señales no complementadas, mientras que la puerta doble "y" 212 de la segunda mitad recibe las señales complementadas. Para cada puerta lógica elemental, cuando un nodo conmuta, el nodo correspondiente de su puerta 212 dual no se conmuta, enmascarándose las dos mitades mutuamente.
En paralelo con esta primera puerta 21 doble riel, se representa una segunda puerta 22 de doble riel "y" (213, 214), funcionando de la misma manera en complementariedad.
Las tensiones eléctricas se suministran a estas puertas 211, 212, 213, 214 lógicas mediante unas líneas 23, 24, 25 de alimentación. Las puertas están conectadas, por otra parte, a unas líneas 26, 27 de masa que vehicularizan el potencial cero de referencia para las alimentaciones. Las líneas 26, 27 de masa están conectadas entre sí con un potencial de referencia, que puede ser el potencial de masa. Las líneas 23, 24, 25 de alimentación, teniendo, por ejemplo, un nivel de tensión de 1,2 voltios en tecnología de 130 nm, están conectadas entre sí con una alimentación eléctrica.

El enmascaramiento mutuo del funcionamiento de las dos mitades de un riel doble impide un análisis de tipo DPA y, por lo tanto, también una prueba de funcionamiento tal como se describió anteriormente.

En un circuito según la invención, las líneas de alimentación de un riel 21, 22 doble se disocian durante la fabricación. Es decir, que la línea 23 de alimentación que alimenta la primera mitad de un riel 21 doble, representado por la puerta 211 "o" se disocia físicamente de la línea 24 de alimentación que alimenta la segunda mitad, representada por la puerta 212 "y". De este modo, la primera línea 23 de alimentación está conectada a una primera fuente Vdd1 de tensión y la segunda línea Vdd2 de alimentación está conectada a una segunda fuente Vdd2 de tensión distinta de la anterior. Es lo mismo para las líneas 24, 25 de alimentación de las otras puertas de doble riel 22.
Para hacer el circuito de criptografía comprobable por DPA, por lo tanto, la invención propone alimentar a las dos mitades 211, 212 por fuentes Vdd1 de tensiones de alimentación diferentes, Vdd2, cada uno entrega, por otra parte, un nivel de tensión necesario para el funcionamiento de las puertas. De este modo, en modo de prueba, las dos fuentes Vdd1 y Vdd2 de alimentaciones están disociadas, lo que permite realizar un DPA sobre las dos mitades en paralelo. Las dos mitades reciben señales que pueden entrecruzarse debido al hecho de que las inversiones se realizan mediante hilos cruzados entre la mitad que recibe las entradas complementadas y la que recibe las entradas no complementadas.

La figura 5 ilustra mediante dos curvas 41, 42 los cronogramas de las corrientes Idd1 e Idd2 que provienen respectivamente de las tensiones Vdd1 y Vdd2 de alimentación para diferentes valores de una señal de doble riel correspondiente a los dos nodos de salida de las dos mitades. Cuando el valor lógico pasa a 1, se consume un pico 43 de corriente.
Los 2 nodos que componen la señal de doble riel son, por lo tanto, verificables por separado mediante la adquisición simultánea de las dos trazas de consumo. Cuando las 2 tensiones de alimentación están conectadas entre sí, la corriente se convierte en la suma Idd1 + Idd2 que siempre tiene la misma forma, independientemente del valor del nodo.

En un circuito integrado tal como se ilustra parcialmente en la figura 3, las puertas 211, 212, 213, 214 lógicas y sus nodos de conexiones asociadas, las líneas de alimentación y las líneas de masa forman carriles, cada puerta de un riel está conectada entre una línea de alimentación y una línea de masa. El dualismo de las puertas, en particular, para protegerse contra los ataques de DPA, crea un segundo riel auxiliar al riel principal, formando un riel 21 doble tal como se describió anteriormente y se ilustra en la figura 3. Un riel constituye la mitad "verdadera" y el otro riel constituye la mitad "falsa". Los carriles dobles están, por ejemplo, dispuestos en paralelo. La figura 3 muestra así un segundo riel 22 doble paralelo al anterior 21. En este caso, para disociar las conexiones a las fuentes Vdd1 y Vdd2 de tensión como se describió anteriormente, una línea 23, 25 de alimentación de cada dos, por ejemplo, está conectada a la primera fuente Vdd1 y las otras líneas, intercaladas, por ejemplo, están conectados a la segunda fuente Vdd2 de tensión.
Un semicircuito, tal como se evocó anteriormente, está compuesto por el conjunto de rieles "verdadero" y el otro semicircuito está compuesto por el conjunto de rieles "falsos", alimentados por Vdd1 y Vdd2, respectivamente. Estos semicircuitos pueden enredarse como se ilustra en el ejemplo de realización de la figura 3, pero pueden no serlo.
Cabe señalar que también es posible separar las líneas 26, 27 de masa. En este caso, una de cada dos líneas de masa estaría conectada a un primer potencial Gnd1 de referencia y las otras líneas de masa, intercaladas, estarían conectada a un segundo potencial Gnd2 de referencia.

La figura 5 ilustra un primer ejemplo de realización de un circuito asegurado según la invención. También presenta un posible procedimiento para cortocircuitar las alimentaciones Vdd1 y Vdd2 después de la fase de pruebas. Para tal fin, la figura presenta únicamente las líneas de alimentación o de masa, siendo el conjunto realizado en un circuito

integrado, por ejemplo, de silicio. Después de las pruebas, es necesario cortocircuitar las alimentaciones Vdd1 y Vdd2 para asegurar el circuito de criptografía y, en particular, para que sea invulnerable a los análisis maliciosos por DPA. Las puertas del primer semicircuito y las puertas duales del segundo semicircuito son entonces alimentadas por una misma fuente de tensión, de acuerdo con el funcionamiento de un circuito asegurado.

La figura 5 ilustra el caso donde las alimentaciones Vdd1 y Vdd2 que disociadas, estando las líneas 26, 27 de masa todas conectadas a un mismo potencial de masa o de referencia. La figura muestra las líneas de alimentación 23, 25 y de masa 26, 27 realizadas por pistas. Las líneas 26, 27 de masa están conectadas, por ejemplo, a un primer anillo equipotencial 31. Este primer anillo, dispuesto, por ejemplo, en la periferia del circuito, está conectado a un potencial de masa o referencia. Las conexiones de las líneas de masa a este anillo 31 están ilustradas por los puntos 30 de contacto. Las líneas 23, 25 de alimentaciones están conectadas a un anillo 32, 33 doble, situado él también, por ejemplo, en la periferia del circuito. Un primer anillo 32 conectado eléctricamente a las líneas 23 de alimentación del primer semicircuito forma una primera vía de alimentación adecuada para conectarse a una primera fuente de alimentación. Un segundo anillo 33 conectado eléctricamente a las líneas 25 de alimentación del segundo semicircuito forma una segunda vía de alimentación adecuada para conectarse a una segunda fuente de alimentación.
El primer anillo 32 está así conectado, por ejemplo, a la fuente Vdd1 de tensión y el segundo anillo 33 está conectado a la fuente Vdd2 de tensión, estando la conexión asegurada por los puntos 30 de contacto. Una línea 23 de alimentación está conectada a través del primer anillo 32 a la alimentación Vdd1 y la siguiente línea 25 de alimentación está conectada a través del segundo anillo a la alimentación Vdd2. De una manera general, las líneas de alimentación pares están conectadas, por ejemplo, a Vdd1 a través del primer anillo 32 y las líneas de alimentación impares, por ejemplo, están conectadas a Vdd2 a través del segundo anillo 33. Los dos anillos 32, 33 del doble anillo de alimentación están conectados entre sí por antifusibles 34. Estos últimos se controlan para poner los dos anillos 32, 33 en cortocircuito después de la fase de prueba y así conectar las vías de alimentación de los dos semicircuitos. Por lo tanto, el cortocircuito entre las dos vías de alimentación se puede realizar en el silicio mediante antifusibles, como se muestra en la figura 5 o en la caja del circuito integrado por un enrutamiento adaptado. Existen muchas soluciones conocidas para sellar un circuito en un estado determinado.
Las líneas de alimentaciones, incluyendo los anillos 31, 32, 33 están, por ejemplo, enrutados en las capas altas del circuito. Los antifusibles deben ser lo suficientemente grandes como para conducir toda la integridad de la corriente necesaria para el funcionamiento correcto del circuito. La figura 5 muestra una distribución de pequeños antifusibles 34, también es posible proporcionar un solo antifusible siempre que pueda pasar la misma cantidad de corriente. Ciertas tecnologías permiten obtener contactos de aproximadamente 500 ohmios para un antifusible 34 después de que se haya quemado. Existen otras tecnologías donde el contacto de poscombustión puede ser del orden de 80 ohmios. Para la comparación, la resistencia de los puntos de contacto pasantes 30 es del orden de 1 ohmio. De este modo, una buena conexión entre los anillos 32, 33 de alimentación requiere muchos más antifusibles 34 que los puntos 30 de contacto. Las conexiones se pueden realizar desde abajo, como se ilustra en la figura 4 o superior, incluso en ambas caras al mismo tiempo.
Un circuito de criptografía asegurado, según la invención, consta, por ejemplo, de un anillo de alimentación adicional. El aumento de ancho corresponde entonces a la adición de este anillo, o bien, de alrededor de 10 µm, alrededor de un bloque de criptografía grande de aproximadamente 1 mm. El aumento que es, por lo tanto, solo del orden del 1 %.
La integración de la desolidarización de las alimentaciones de las líneas pares, en Vdd1, e impares, en Vdd2, en un flujo de diseño de circuitos existentes es trivial. En efecto, en lugar de generar dos anillos, se producen tres. Esta operación se realiza generalmente en herramientas CAD profesionales en una sola línea de código.
En otro modo de realización, las líneas 26, 27 de masa también pueden ser disociadas. Una primera vía de alimentación consta entonces de un primer anillo conductor periférico adecuado para conectarse a un primer potencial Gnd1 de masa, conectado eléctricamente a las líneas 26 de masa de los componentes 211, 214 del primer semicircuito, y una segunda vía de alimentación consta de un segundo anillo conductor periférico adecuado para conectarse a un segundo potencial Gnd2 de masa, conectado eléctricamente a las líneas 27 de masa de los componentes 212, 213 del segundo semicircuito. Como en el caso anterior, siendo los dos anillos adecuados para cortocircuitarse.

La implementación del procedimiento de prueba según la invención es fácil. Las mediciones de traza de consumo en los circuitos de salida de fabricación para el análisis DPA simplemente necesitan aparatos estándar, por ejemplo:

- un ordenador para pilotar el circuito bajo prueba, equipado con;
- una tarjeta de adquisición de ancha banda pasante, generalmente algunos gigahercios.

La invención puede ser usada ventajosamente por los fabricantes de circuitos de criptografía asegurados, en particular los fabricantes:

- de tarjetas con chip, en particular, para las aplicaciones TPM, SIM, pasaportes electrónicos, etiquetas, RFID, tokens de autenticación;
- los sistemas en chip para aplicaciones de telecomunicaciones.

REIVINDICACIONES

1. Procedimiento de prueba de un circuito de criptografía que integra un secreto y que consta de registros (1, 2) y de puertas (10, 211, 212, 213, 214) lógicas interconectadas por un conjunto de nodos, **caracterizado porque** dicho procedimiento efectúa un análisis diferencial de consumo (DPA) que consta de:

- una fase (11) de adquisición de mediciones de trazas de consumo al nivel de todos los nodos que funcionan como vectores de señales de prueba a la entrada del circuito;
- una fase (12) de análisis de la tasa de actividad de cada nodo a partir de las mediciones de trazas de consumo, considerándose un nodo en buen funcionamiento cuando su actividad es de acuerdo con un modelo de predicción de actividad.

2. Procedimiento según la reivindicación 1, **caracterizado porque** como el secreto del circuito de criptografía es personalizable, el análisis (11, 12) diferencial de consumo se realiza con un secreto conocido, después, se efectúa una personalización del secreto después de la prueba.

3. Procedimiento según la reivindicación 1, **caracterizado porque** como el circuito de criptografía está asegurado, constando de un primer semicircuito (211, 214) asociado con un segundo semicircuito (212, 213) que funciona en lógica complementaria, la alimentación (Vdd1, 23, 25) eléctrica del primer semicircuito está disociada de la alimentación (Vdd2, 24) eléctrica del segundo semicircuito, realizándose el análisis diferencial de consumo en paralelo en cada semicircuito, estando las dos alimentaciones reagrupadas en una misma alimentación eléctrica después de la prueba.

4. Procedimiento según la reivindicación 2, **caracterizado porque** los componentes (211, 214) del primer semicircuito están conectados a través de unas líneas (23, 25) de alimentación a una primera fuente (Vdd1) de tensión y los componentes (212, 213) del segundo semicircuito se alimentan a través de unas líneas (24) de alimentación a una segunda fuente (Vdd2) de tensión, siendo las dos fuentes de tensión distintas, estando las líneas (23, 24, 25) de alimentaciones conectadas después de la prueba.

5. Procedimiento según una cualquiera de las reivindicaciones 1 a 4, **caracterizado porque** los componentes (211, 214) del primer semicircuito están conectados a través de unas líneas (26) de masa a un primer potencial (Gnd1) de referencia y los componentes (212, 213) del segundo semicircuito se alimentan a través de unas líneas (27) de masa a un segundo potencial (Gnd2) de referencia, estando los dos potenciales de referencia disociados, estando las líneas (26, 27) de masa conectadas después de la prueba.

6. Procedimiento según una cualquiera de las reivindicaciones 1 a 5, **caracterizado porque** las alimentaciones (Vdd1, Vdd2) se reagrupan después de la fase de adquisición.

7. Procedimiento según una cualquiera de las reivindicaciones anteriores, **caracterizado porque** la adquisición de las mediciones de trazas de consumo se efectúa únicamente en los registros (1, 2).

8. Circuito de criptografía asegurado que consta de un primer semicircuito (211, 214) asociado con un segundo semicircuito (212, 213) que funciona en lógica complementaria, **caracterizado porque** consta de una primera vía (23, 25, Vdd1) de alimentación eléctrica asignada al primer semicircuito y una segunda vía (24, Vdd2) de alimentación eléctrica asignada al segundo semicircuito, de modo que cada semicircuito se pueda probar mediante un análisis diferencial de consumo (DPA) independientemente del otro semicircuito, siendo las dos vías de alimentación adecuadas para cortocircuitarse.

9. Circuito según la reivindicación 8, **caracterizado porque**:

- la primera vía de alimentación consta de un primer anillo (32) conductor periférico adecuado para conectarse a una primera fuente (Vdd1) de tensión y conectarse eléctricamente a unas líneas (23, 25) de alimentación de los componentes (211, 214) del primer semicircuito y;
- la segunda vía de alimentación consta de un segundo anillo (33) conductor periférico adecuado para conectarse a una segunda fuente (Vdd2) de tensión y conectarse eléctricamente a unas líneas (24) de alimentación de los componentes (212, 213) del segundo semicircuito;

siendo los dos anillos adecuados para cortocircuitarse.

10. Circuito según una cualquiera las reivindicaciones 8 o 9, **caracterizado porque**:

- la primera vía de alimentación consta de un primer anillo conductor periférico adecuado para conectarse a un primer potencial (Gnd1) de masa y conectarse eléctricamente a unas líneas (26) de masa de los componentes (211, 214) del primer semicircuito y;
- la segunda vía de alimentación consta de un segundo anillo conductor periférico adecuado para conectarse a un segundo potencial (Gnd2) de masa y conectarse eléctricamente a unas líneas (27) de masa de los componentes (212, 213) del segundo semicircuito;

siendo los dos anillos adecuados para cortocircuitarse.

11. Circuito según una cualquiera de las reivindicaciones 8, 9 o 10, **caracterizado porque** la conexión de las vías de alimentación entre sí se asegura mediante una tecnología denominada antifusible que permite el paso del estado aislante al estado conductor de una manera irreversible después de fusión.

12. Circuito según una cualquiera de las reivindicaciones 9, 10 u 11, **caracterizado porque** los anillos (26, 27, 32, 33) están conectados entre sí mediante antifusibles, estando realizado el cortocircuito entre los dos anillos por la fusión de los antifusibles (34).

13. Procedimiento de cableado de las alimentaciones de un circuito de criptografía asegurado que consta de un primer semicircuito (211, 214) asociado con un segundo semicircuito (212, 213) que funciona en lógica complementaria, **caracterizado porque** una primera vía (23, 25, Vdd1) de alimentación eléctrica se asigna al primer semicircuito y una segunda vía (24, Vdd2) de alimentación eléctrica se asigna al segundo semicircuito, de modo que cada semicircuito se pueda probar mediante un análisis diferencial de consumo (DPA) independientemente del otro semicircuito, siendo las dos vías de alimentación adecuadas para cortocircuitarse.

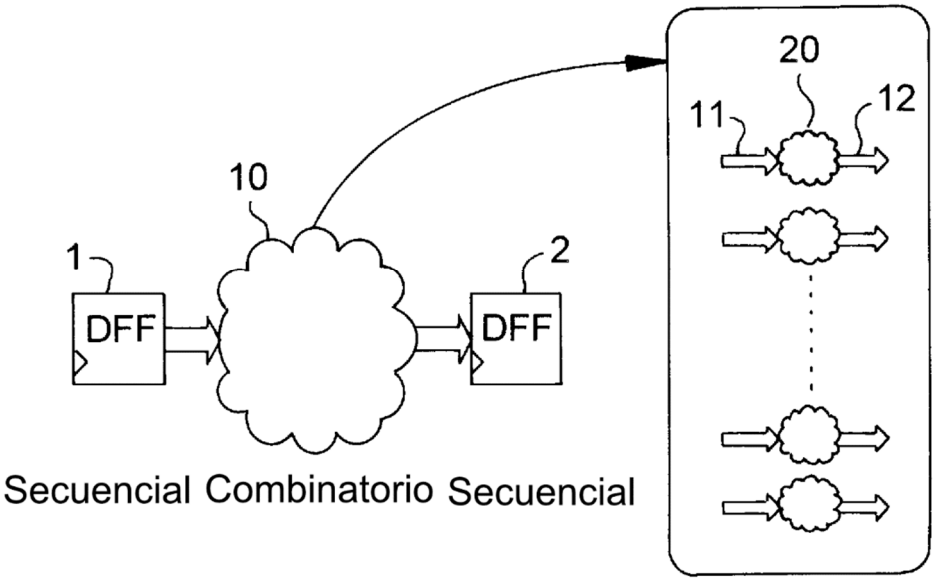
20
11
12
10
1
2
DFF
DFF
Secuencial
Combinatorio
Secuencial

FIG.1

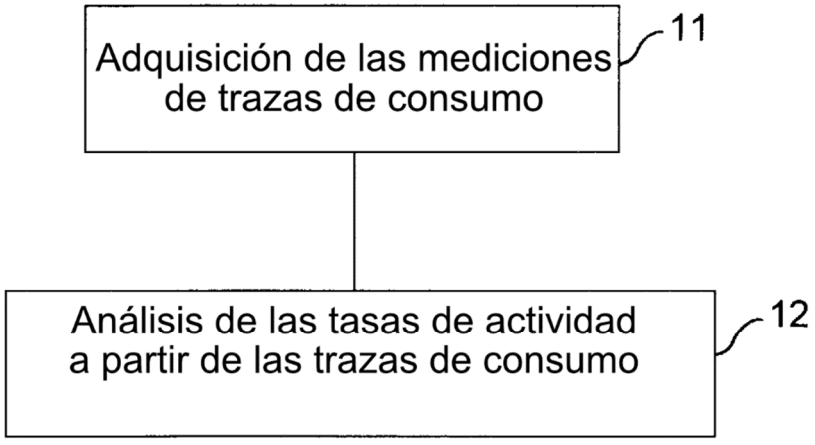
Adquisición de las mediciones de trazas de consumo
11
Análisis de las tasas de actividad a partir de las trazas de consumo
12

FIG.2

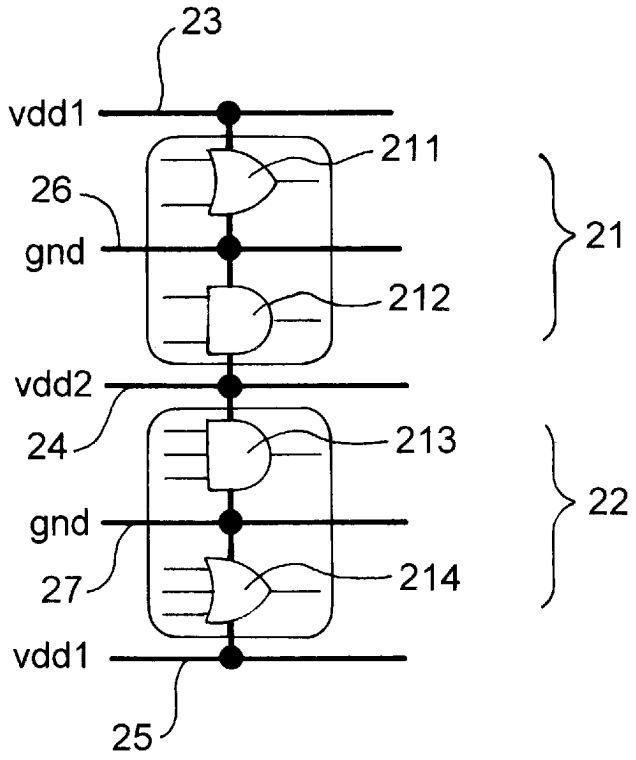
23
vdd1
211
26
gnd
212
21
vdd2
24
213
gnd
22
27
214
vdd1
25

FIG.3

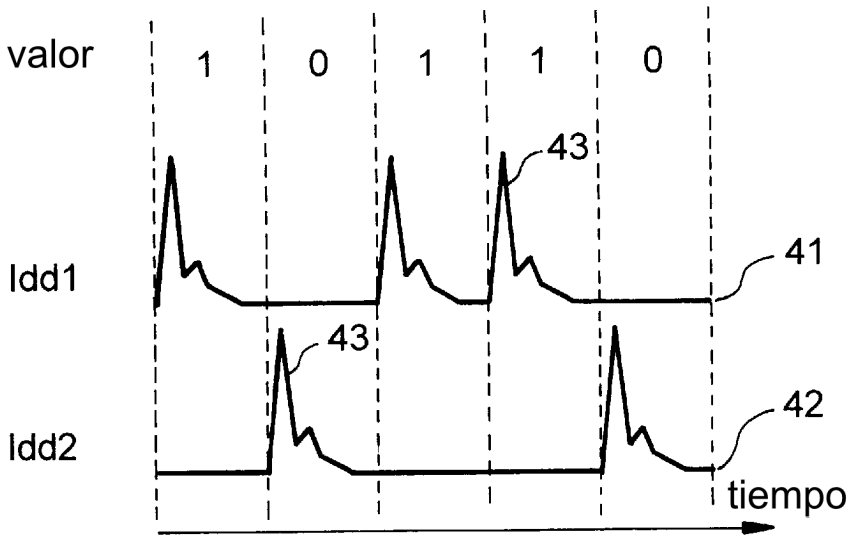
valor
1
0
1
1
0
43
Idd1
41
43
Idd2
42
tiempo

FIG.4

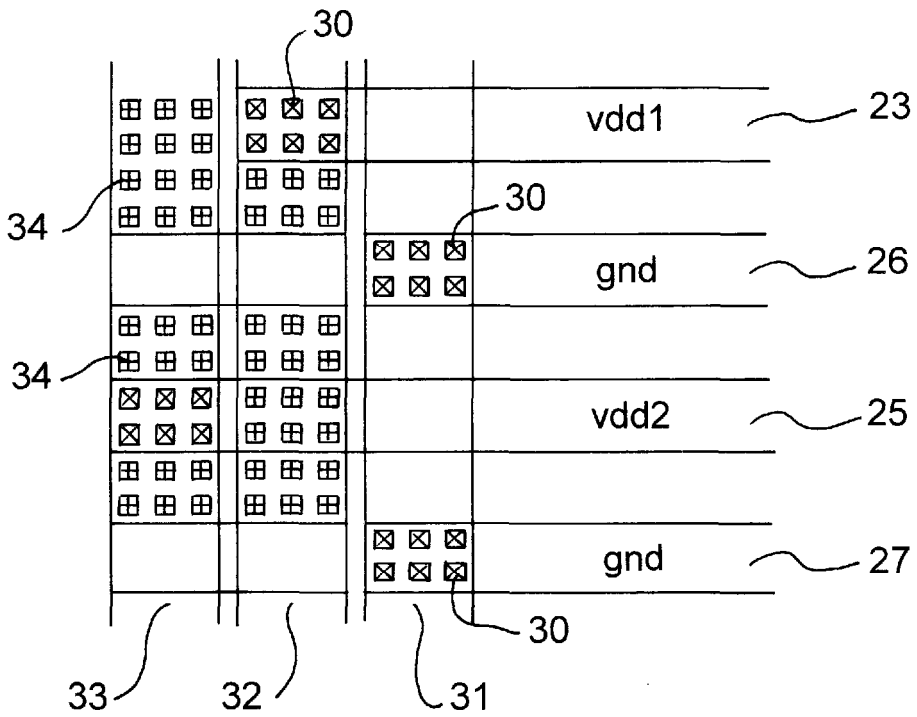

FIG.5