(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 386 061**

(51) Int. CI.:
G06F 21/02 (2006.01)
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09806408 .2**
(96) Fecha de presentación: **30.07.2009**
(97) Número de publicación de la solicitud: **2324442**
(97) Fecha de publicación de la solicitud: **25.05.2011**

(54) Título: **Procedimiento de detección de anomalias en un circuito criptográfico protegido por lógica diferencial y circuito para implementar a dicho procedimiento**

(30) Prioridad:
12.08.2008 FR 0855537

(45) Fecha de publicación de la mención BOPI:
08.08.2012

(45) Fecha de la publicación del folleto de la patente:
08.08.2012

(73) Titular/es:
Institut Telecom - Telecom Paristech
46 Rue Barrault
75013 Paris, FR

(72) Inventor/es:
DANGER, Jean-Luc;
GUILLEY, Sylvain y
FLAMENT, Florent

(74) Agente/Representante:
Carpintero López, Mario

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

Procedimiento de detección de anomalías en un circuito criptográfico protegido por lógica diferencial y circuito implementa a dicho procedimiento

La invención se refiere a un procedimiento y un circuito de detección de anomalías en un circuito criptográfico protegido por lógica diferencial.

La invención se aplica particularmente al campo de la protección de los circuitos criptográficos contra los ataques por inyección de fallos.

La criptografía tiene particularmente como objetivo proteger:

- el secreto de información por medio del cifrado y de su operación dual: el descifrado;
- solamente su integridad, mediante operaciones de firma y de verificación de firma.

La criptografía utiliza métodos matemáticos seguros, en el sentido de que no existen en el estado actual de los conocimientos publicados métodos de ataque más rápido que el ataque exhaustivo correspondiente al ensayo de todas las claves posibles.

En general, los métodos de cifrado implican cálculos complejos necesarios para la seguridad de los sistemas. Esta complejidad no plantea problemas particulares a los ordenadores pero constituye un inconveniente en el caso de dispositivos para el gran público que no cuentan con una gran potencia de cálculo, en general controlados por microprocesadores de coste reducido. Las consecuencias pueden ser entonces de varios órdenes, de este modo por ejemplo una tarjeta bancaria emplearía varios minutos en firmar una transacción o un decodificador digital de televisión de pago no podría seguir el caudal de información en juego.

Para paliar este tipo de problema sin aumentar el precio de los sistemas, es habitual añadir una ayuda a la unidad central que controla el dispositivo, en general en forma de un coprocesador dedicado a la criptografía.

Sin embargo, ya sea implementado por la unidad central o por un coprocesador especializado, el algoritmo criptográfico es implementado en todos los casos por un dispositivo físico, electrónico. Los dispositivos electrónicos presentan imperfecciones inevitables vinculadas a las propiedades inherentes de las leyes de la electricidad.

Es así que sistemas criptográficos seguros desde el punto de vista matemático pueden ser atacados explotando las imperfecciones de los sistemas físicos que implementan el algoritmo. La duración de los cálculos puede depender de los valores de los datos, en particular en sistemas informáticos optimizados en tiempo, lo que puede dar lugar a los ataques de tipo “*timing attack*” que permiten en algunos casos recuperar la totalidad de las claves secretas a partir de simples mediciones de tiempos de ejecución. El consumo eléctrico instantáneo también puede depender de los datos, lo que puede dar lugar a series de ataques tales como:

- SPA (*Simple Power Analysis*) que intenta diferenciar las operaciones ejecutadas por una unidad central a partir de una medición de su consumo eléctrico medido durante una operación criptográfica;
- análisis diferencial de consumo DPA (*Differential Power Analysis*) que utiliza operaciones estadísticas en numerosas mediciones de consumo eléctrico, realizadas durante operaciones de criptografía en mensajes aleatorios y con una clave constante para validar o invalidar una hipótesis planteada en una parte limitada de la clave;
- ataques de tipo “*template*” (plantilla) que en una primera fase utilizan un dispositivo idéntico al dispositivo atacado, excepto que este dispositivo idéntico no contiene ningún secreto, para construir modelos de consumo indexados por el valor de una parte limitada de la clave y en una segunda fase utilizan varias mediciones de consumo del dispositivo atacado para determinar el modelo cuyos consumos medidos son los más próximos y, de este modo, determinar el valor de esta sub-clave;

Por otro lado, cualquier corriente eléctrica que circula por un conductor genera un campo electromagnético cuya medición puede dar lugar a ataques idénticos en su principio a los ataques relacionados con el consumo eléctrico, particularmente por DPA.

Finalmente, ataques llamados activos, o por inyección de fallos, perturban el funcionamiento de los sistemas para explotar los falsos resultados para recuperar los secretos del sistema.

Se denomina “canal oculto” a cualquier imperfección de un dispositivo físico que emplea un algoritmo criptográfico y susceptible de dejar escapar información vinculada a los secretos conservados en la memoria del dispositivo.

Los ataques en fallos son ataques activos que pueden se de naturalezas muy diferentes, como se explica particularmente en el artículo de David Naccache “Finding faults”, IEEE Security and Privacy, 3(5), páginas 61-65, 2005: variación de temperatura o tensión, señal parásita fuerte en la alimentación o mediante campo electromagnético, disparos láser, etc. Los fallos generados tienen como consecuencia la modificación del valor de un nodo del circuito atacado. Estos pueden ser sencillos o múltiples, permanentes o transitorios en función del impacto sobre el silicio. La flexibilidad de las inyecciones de fallos transitorios da lugar a ataques más potentes realizando

ensayos múltiples y aumenta, de este modo, las probabilidades de éxito. Los ataques con fallos sencillos simplifican el procedimiento de ataque. Los ataques en fallos se basan en el análisis diferencial entre la salida cifrada no errónea y la salida con fallo. Por ejemplo, el ataque presentado en el artículo de Gilles Piret y Jean-Jacques Quisquater “A Differential Fault Attack Technique against SPN Structures, with Application to the AES and KHAZAD”, en CHES, volumen 2779 de LNCS, páginas 77-88, Springer, 2003 sobre el cifrado AES ha demostrado ser extremadamente eficaz si el fallo llega en la penúltima o antepenúltima ronda.

Los ataques por inyección de fallos han sido, hasta el presente, y esto de forma muy paradójica, considerados como costosos y, por lo tanto, accesibles en la práctica únicamente por organizaciones dudosas sostenidas económicamente. Actualmente es posible controlar a través de Internet una estación de descapsulación y un banco láser conciliable clave en mano. De ello resulta que la verosimilitud de un ataque por inyección de fallos ha aumentado considerablemente. De este modo, un criptoprocesador implantado en un circuito integrado, por ejemplo un FPGA, no obstante solamente puede considerarse seguro si implementa simultáneamente contramedidas para los ataques en observación, particularmente de tipos DPA o EMA, y en inyección de fallos. Además, ataques que combinan observación y fallos se han propuesto, como el descrito por Bruno Robisson y Pascal Manet en su artículo “Differential Behavioral Analysis”, en CHES, volumen 4727 de LNCS, páginas 413-426, Springer, 2007.

Una contramedida eficaz para luchar contra este tipo de ataque se basa en el empleo de la redundancia. Por ejemplo, puede reproducirse un bloque de cálculo tres veces y una función mayoría permite a continuación eliminar el bloque en el que se ha inyectado un fallo. Uno de los inconvenientes de esta solución es que implica un sobrecoste debido a la reproducción del o de los bloques de cálculo o bien a la inserción de un módulo de control de coherencia basado en una verificación de invariantes.

Otra contramedida consiste en detectar la inyección de fallos. En este caso el usuario es alertado y puede actuar para protegerse, reinicializando el sistema, por ejemplo.

Un objetivo de la invención es, particularmente, paliar los inconvenientes mencionados anteriormente.

A tal efecto, la invención tiene por objeto un procedimiento de detección de anomalías en un circuito protegido por lógica diferencial y que procesa variables lógicas representadas por un par de componentes, una primera red de células que realizan funciones lógicas sobre la primera componente de dichos pares, una segunda red de células duales que funcionan en lógica complementaria sobre la segunda componente, estando las funciones lógicas realizadas por cada par de células en una fase de precarga que pone a las variables en un estado conocido en la entrada de las células, seguida por una fase de evaluación en la que un cálculo es realizado por las células. Una anomalía es detectada por al menos un estado no coherente que se produce durante la fase de precarga o durante la fase de evaluación.

El circuito protegido por lógica diferencial es, por ejemplo, un circuito criptográfico.

De acuerdo con un aspecto de la invención, se utiliza una puerta lógica para la detección de estados no coherentes que se producen durante la fase de precarga, siendo esta puerta lógica una puerta “O” si el estado coherente es (0,0) o una puerta “Y” si el estado coherente es (1,1).

La puerta lógica utilizada para la detección de estados no coherentes que se producen durante la fase de evaluación puede ser una puerta “XNOR”.

Un multiplexor permite, por ejemplo, seleccionar la señal resultante de la detección de estados no coherentes, estando la salida de la puerta de detección de estados no coherentes en fase de precarga seleccionada durante la fase de precarga y la salida de la puerta de detección de estados no coherentes en fase de evaluación durante la fase de evaluación, estando la selección controlada por una señal de configuración.

La invención también tiene, por objeto, un circuito protegido por lógica diferencial que procesa variables lógicas representadas por un par de componentes, una primera red de células que realizan funciones lógicas sobre la primera componente de dichos pares, una segunda red de células duales que funcionan en lógica complementaria sobre la segunda componente, estando las funciones lógicas realizadas por cada par de células en una fase de precarga que pone a las variables en un estado conocido en la entrada de las células seguida de una fase de evaluación en la que un cálculo es realizado por las células, estando dicho circuito caracterizado por que comprende al menos un módulo de detección que implementa el procedimiento de acuerdo con una de las reivindicaciones anteriores y que comprende medios para testar la coherencia entre las dos componentes de las variables lógicas durante las fases de precarga o de evaluación en los nodos controlados del circuito.

El circuito es, por ejemplo, un circuito programable de tipo FPGA o bien un circuito de tipo ASIC.

Al menos uno de los módulos de detección comprende, por ejemplo, medios para detectar los estados no coherentes durante la fase de precarga en la salida de las células a vigilar.

Al menos uno de los módulos de detección comprende, por ejemplo, medios para detectar los estados no coherentes durante la fase de evaluación en la salida de las células a vigilar.

Las salidas de los módulos de detección pueden recogerse mediante encadenamiento, estando los resultados centralizados en al menos una equipotencial por medio de puertas “O”.

La salida de cada cadena de detección puede estar conectada a una conexión oscilante activada por la señal de reloj y que genera una salida global que toma el valor de 1 cuando al menos un estado no coherente es detectado por uno de los módulos de detección de la cadena.

Como ejemplo, al menos una parte de los módulos de detección del circuito pueden estar organizados en árbol, generando el último módulo de detección una señal global que indica si al menos un estado no coherente ha sido detectado en uno de los nodos del circuito vigilados por dichos módulos.

Los pares de componentes a vigilar pueden, por ejemplo, agruparse por vectores, estando los módulos de detección compuestos por dos multiplicadores-acumuladores que realizan operaciones de multiplicación-acumulación entre los vectores después de que un bit de orden bajo de valor 1 haya sido añadido a cada uno de dichos vectores, siendo la diferencia entre los resultados de las dos operaciones calculada y a continuación procesada por un comparador con cero cuya salida toma el valor cero cuando un estado no coherente es detectado en las fases de precarga o de evaluación.

La salida del comparador con cero de los módulos de detección está, por ejemplo, conectada a un basculador para generar una salida estable, resultado de la detección de estados no coherentes.

La invención tiene, particularmente, la ventaja de basarse en las características de los circuitos protegidos gracias a una contramedida por lógica diferencial, inicialmente prevista para combatir los ataques por observación de los canales ocultos para detectar otros tipos de ataques o de perturbaciones.

Otras características y ventajas de la invención serán evidentes con ayuda de la siguiente descripción, que se da a título ilustrativo y no limitante, realizada respecto a los dibujos adjuntos, entre los cuales:

- la figura 1 representa una puerta “Y” en lógica diferencial;
- la figura 2 ilustra las fases de una etapa de cálculo en lógica diferencial;
- la figura 3 ilustra el principio de funcionamiento de la detección de anomalías que se basa en una arquitectura protegida por lógica diferencial;
- la figura 4 presenta un ejemplo de circuito que utiliza el procedimiento de detección de anomalías;
- la figura 5 presenta un primer ejemplo de cadena de detección de anomalías;
- la figura 6 presenta un segundo ejemplo de cadena de detección de anomalías;
- la figura 7 presenta un ejemplo de estructura en árbol para la detección de anomalías;
- la figura 8 presenta un ejemplo de utilización del procedimiento en un circuito utilizando bloques de multiplicación acumulación;

La figura 1 presenta una puerta “Y” 1, 2 en lógica WDDL (*Wave Dynamic Differential Logic*) como ejemplo de ilustración del principio de la lógica diferencial. Ésta está compuesta por dos redes lógicas duales 1, 2, que funcionan en lógicas complementarias. El ejemplo de la lógica WDDL se utiliza en lo sucesivo en la descripción, pero el principio de la invención se aplica a los otros tipos de lógica diferencial, como por ejemplo la lógica MDPL (*Masked Dual-rail Pre-charge Logic*). Además de la dualidad de las redes de cálculo, se realiza un cálculo en lógica diferencial siguiendo dos fases distintas: una fase de precarga y una fase de evaluación.

Los datos se representan en rail doble, estando cada variable lógica a formada por un par de señales (a_t, a_f) codificadas de la siguiente manera:

- (0, 0) para el estado de reposo durante la fase de precarga: el valor de a no se ha definido, se indica como Ω;
- (1, 0) es un estado activo durante la fase de evaluación en el que a = 1 ;
- (0, 1) es el otro estado activo durante la fase de evaluación en el que a = 0.

Una puerta lógica H con dos entradas a y b y una salida s se representa físicamente mediante dos puertas 1, 2 que tienen respectivamente las funciones lógicas T (a_t, b_t) y F(a_f, b_f) tales que:

$$s_t = T(a_t, b_t) \qquad (1)$$

$$s_f = F(a_f, b_f) \qquad (2)$$

La red lógica “verdadera” corresponde a la función T que suministra la señal s_t. La red lógica dual “falsa” corresponde a la función F que suministra la señal dual s_f. La figura 1 ilustra la puerta “Y” en la que la red “verdadera” que realiza la función T recibe las dos entradas no complementadas a_t y b_t. La función dual “O” realiza la

función F. Para un vector de variables x se verifican las siguientes relaciones:

$$T(x) = H(x) \qquad (3)$$

$$F(\bar{x}) = \overline{H(x)} \qquad (4)$$

La figura 2 presenta las fases de una etapa de cálculo en lógica diferencial, por ejemplo del tipo WDDL. Esta etapa comprende fases sucesivas de precarga 21 y de evaluación 22. Los ejemplos de estados de las variables de entradas a_t ,b_t ,a_f ,b_f y de las variables de salidas correspondientes s_t, s_f se presentan respecto a fases de precarga y de evaluación. Los cronogramas de la figura 2 muestran que el número de transiciones es el mismo, tres en este caso, durante el paso de la fase de precarga a la fase de evaluación y viceversa. Como el consumo está directamente vinculado al número de transiciones en las tecnologías electrónicas de tipo CMOS particularmente, el consumo se equilibra de este modo.

La figura 3 ilustra el principio de funcionamiento de la detección de anomalías que se basa en una arquitectura protegida por lógica diferencial.

La lógica diferencial cualificada de rail doble es redundante por naturaleza. En efecto, una variable en el estado lógico implica una señal “Verdadera” cuyo valor es complementario de la señal “Falsa” durante la evaluación e idéntica durante la precarga. Por consiguiente, puede detectarse una anomalía cuando se producen estados no coherentes, es decir estados que se supone que no existen. Por ejemplo en lógica WDDL, una anomalía se detecta si se detecta un estado no coherente, es decir:

- durante la fase de precarga el par de señales duales es diferente del estado (Q_t, Q_f) = (0, 0);
- durante la fase de evaluación el par de señales es diferente de los estados (Q_t, Q_f) = (0, 1) o (Q_t, Q_f) = (1, 0).

Por otro lado, un fallo único en lógica diferencial tienen una probabilidad de 1/2 de tener un impacto, ya que el paso de la lógica de rail doble a rail simple se realiza considerando solamente una única señal en las dos componentes de una variable.

En caso de fallos múltiples, el mecanismo de detección propone poder no detectar cambios de estado conjugados, como por ejemplo (0, 1) que puede transformarse en (1, 0) durante la fase de evaluación. Este caso concreto es, sin embargo, muy poco probable, ya que:

- el estado de precarga tiene una gran probabilidad de resultar afectado,
- en caso de múltiples fallos, otras variables pueden resultar afectadas y ser detectadas,
- la mayor parte de los ataques no permiten realizar una inversión de bit de forma concomitante en las dos señales. Por ejemplo, los ataques por violación de tiempo de posicionamiento previo utilizando la temperatura, la tensión o la frecuencia.

El ejemplo de la figura 3 ilustra el principio de una puerta diferencial WDDL que tiene un mecanismo de detección de anomalías.

Para realiza esta función de detección, una puerta “O” 34 que realiza la operación de adición lógica permite detectar los estados no coherentes en la salida de las redes T 31 y F 32 durante la fase de precarga. De este modo, cuando los estados (0,1), (1,0) o (1,1) aparecen, la salida de la puerta “O” 34 vale 1.

De la misma manera, una puerta “XNOR” 33 que realiza la operación de o exclusivo inverso permite detectar los estados no coherentes en la salida de las redes T 31 y F 32 durante la fase de de evaluación. De este modo, cuando los estados (0,0) o (1,1) aparecen, la salida de la puerta “XNOR” 33 vale 1.

Un multiplexor 35 permite, a continuación, seleccionar la salida de la puerta “O” 34 o de la puerta “XNOR” 33. Dicho multiplexor está configurado con una señal de entrada PRE/EVAL. Por ejemplo, puede utilizarse la siguiente convención:

- durante la fase de precarga, PRE/EVAL toma el valor 0 y la salida de la puerta “O” 34 es transmitida en la salida del multiplexor 35;
- durante la fase de evaluación, PRE/EVAL toma el valor 1 y la salida de la bascule “XNOR” 33 es transmitida en la salida del multiplexor 35;

Por consiguiente, la señal FALLO disponible en la salida del multiplexor 35 toma el valor 1 cuando se detecta un estado no coherente y sigue siendo 0 en caso contrario.

Para simplificar la implementación del procedimiento, la detección puede realizarse solamente durante la fase de evaluación, permitiendo de este modo reducir la complejidad y necesitando solamente una puerta “XNOR”. La

detección también puede realizarse solamente durante la fase de precarga, permitiendo de este modo reducir la complejidad necesitando solamente una puerta “O”. En los dos casos, no se requiere la utilización del multiplexor 35. El inconveniente de esta reducción de complejidad es que las probabilidades de detectar una intrusión se reducen.

La figura 4 presenta un ejemplo de utilización del procedimiento de detección de fallos. La detección de fallos puede llevarse a cabo en módulos de detección colocados por ejemplo en la salida de cada puerta dual compuesta por una red T 41 y por una red F 42 de un circuito criptográfico. El circuito criptográfico que comprende dichos módulos se implementa, por ejemplo, en un circuito ASIC o bien en un circuito programable de tipo FPGA.

En lugar de colocar los módulos de detección en la salida de cada puerta dual, también es posible, y esto para reducir la complejidad del circuito, implementar dichos módulos únicamente en los nodos importantes del circuito. Un nodo llamado “importante” del circuito es un nodo que se sitúa en la salida de los registros, de tipo basculadores D 43, 45 por ejemplo, para asegurar la estabilidad de las señales vigiladas por el módulo de detección. De este modo, en el ejemplo de la figura 4, la detección se realiza en la salida de una red de células T 41 y de una red de células F 42. El módulo de detección 47 está situado entre dos pares de registros 43, 45 y 44, 46 compuestos por basculadores D. Cada fase de cálculo corresponde entonces a un periodo de reloj. Un circuito de cifrado que utiliza la lógica diferencial comprende un gran número de nodos. La señal PRE/EVAL permite configurar cada módulo del circuito para la detección de fallos durante la fase de precarga o la fase de evaluación. Una señal FALLO en la salida de cada módulo 47 permite saber si una anomalía, es decir un estado no coherente, ha sido detectada a nivel de cada nodo vigilado.

La figura 5 presenta un ejemplo de cadena de detección de anomalías. Como se ha descrito anteriormente, módulos de detección pueden estar colocados en un circuito de cifrado que utiliza una arquitectura de lógica diferencial, y esto a nivel de cada uno de los nodos a vigilar. Una manera de recoger las anomalías y de encadenar los detectores. Esta técnica presenta el interés de tener solamente una equipotencial 56 entre las puertas donde se realiza la detección y facilita, de este modo, el enrutamiento en ASIC o FPGA. De este modo, las señales FALLO de los módulos de detección 51, 52 se encadenan unas a otras utilizando puertas “O” 53, 54.

Las señales de salida de los módulos de detección se encadenan hasta un basculador 55 que recoge el estado global del sistema para fiabilizar la señal global de salida FALLO_GLOBAL. Dicha señal toma el valor 1 si se ha detectado al menos un fallo por uno de los módulos de detección presentes en la cadena.

Si se demuestra que la cadena presenta una trayectoria crítica que limita la velocidad global de funcionamiento del procesador protegido, puede insertarse un registro de *pipeline*. Es preciso, sin embargo, asegurarse de que la latencia de la detección no permita al atacante recuperar el resultado del cálculo antes de la detección de anomalía.

La figura 6 presenta un segundo ejemplo de cadena de detección de fallos. Para reducir la complejidad, puede utilizarse una sola cadena. Por ejemplo, los módulos de detección pueden estar simplificados con respecto a los de la figura 5 y reducirse a una puerta “XNOR” 61, 62. En este caso, la detección de estados no coherentes solamente es válida durante la fase de evaluación. Para ignorar el resultado de los módulos de detección durante la fase de precarga, una puerta “Y” 66 permite tener en cuenta el resultado de la detección de fallos de cada uno de los módulos de detección de la cadena solamente cuando la señal PRE/EVAL está en 1. Las señales FALLO de los módulos de detección 61, 62 se encadenan unas a otras utilizando puertas “O” 63, 64. Las anomalías detectadas por los módulos de detección encadenados son transmitidas en una equipotencial 67 hasta un basculador 65 que recoge el estado global del sistema para fiabilizar la señal global de salida FALLO_GLOBAL. Dicha señal toma el valor 1 si al menos un fallo ha sido detectado en uno de los nodos de la cadena.

De acuerdo con el mismo principio, los módulos de detección pueden simplificarse para detectar los estados no coherentes únicamente durante la fase de evaluación. En este caso, se utilizan puertas “O” en lugar de las puertas “XNOR” 61, 62 de la figura 6 y la señal PRE/EVAL utilizada en la entrada de la puerta “Y” 66 es sustituida por la señal PRE/EVAL para tener en cuenta el resultado de la detección global solamente durante la fase de evaluación, o sea cuando la señal PRE/EVAL toma el valor 1.

También es posible utilizar dos cadenas independientes, una para la detección de estados no coherentes en fase de precarga y la otra para la detección de los estados no coherentes en fase de evaluación, permitiendo esto librarse de la utilización de multiplexores.

La figura 7 presenta un ejemplo de estructura en árbol para la detección de fallos. En efecto, para acelerar la trayectoria de detección, los módulos de detección pueden estar estructurados en árbol. El ejemplo de la figura 7 da un ejemplo en el que la detección de estados no coherentes se realiza en ocho nodos de un circuito protegido por lógica diferencial. Los estados de los pares (Q_{1t}, Q_{1f}), (Q_{2t}, Q_{2f}),...,(Q_{8t}, Q_{8f}) son vigilados gracias a módulos de detección 71 tales como los descritos con ayuda de las figuras 3 y 4 y están situados a nivel de cada uno de dichos nodos. El resultado de la detección mediante cada uno de los módulos es transmitido, a continuación, a un segundo banco de módulos de detección 72 cuyas salidas son, a su vez, transmitidas a un tercer banco de módulos de detección 73. Finalmente, un último detector 74 genera una señal resultado de la detección global de los estados no coherentes en los ocho nodos vigilados. Un basculador 75 recoge el estado global del sistema para fiabilizar la señal de salida FALLO_GLOBAL.

La figura 8 presenta un ejemplo de utilización del procedimiento en un circuito que utiliza bloques de multiplicación acumulación. En efecto, la detección puede simplificarse utilizando bloques de multiplicación-acumulación, denominados generalmente bloques MAC, acrónimo de la terminología anglo-sajona "*multiplication and accumulation*". Estos bloques están, por ejemplo, disponibles en algunos circuitos FPGA. Las señales de entradas están, en este caso, compuestas por dos pares de palabras de N bits $A = (A_t, A_f)$ y $B = (B_t, B_f)$. A_f y B_f son los dobles de A_t y B_t y se expresan, por lo tanto, de la siguiente manera de acuerdo con la representación de los números enteros firmados en complemento a dos:

$$A_f = -A_t - 1 \qquad (5)$$

$$B_f = -B_t - 1 \qquad (6)$$

El producto $A_t \times B_t$, se calcula en el conjunto de los números enteros relativos y debe corresponder al producto $(A_f + 1) \times (B_f + 1)$. De este modo, puede detectarse un fallo único si no hay correspondencia entre los dos productos.

En el caso de fallos múltiples, pueden existir casos en los que los fallos en A y B se compensan y dan los mismos productos pero estos casos tienen probabilidades de ocurrir muy reducidas. Sin embargo, este cálculo de multiplicación entera basado en una invariante algebraica asegura una cobertura importante y constituye, por lo tanto, una contramedida eficaz contra la inyección de fallos.

Para utilizar este principio, es preciso no solamente considerar $A_f + 1$ y $B_f + 1$ y no A_f y B_f, sino que es preciso además que estas variables no sean nunca nulas para realizar la detección durante las dos fases de precarga y de evaluación. Una manera sencilla de cumplir estas condiciones es añadir un bit de orden bajo de valor 1 a las cuatro palabras A_t, B_t, A_f y B_f.

Se utilizan dos bloques MAC 81, 82. El primer 81 toma en la entrada una palabra binaria de N bits A_t a la que se le añade un bit de orden bajo que vale 1 y una palabra binaria de N bits B_t a la que también se le añade un bit de orden bajo que vale 1. El segundo bloque MAC 82 toma en la entrada una palabra binaria de N bits A_f a la que se le añade un bit de orden bajo que vale 1 y una palabra binaria de n bits B_f a la que también se le añade un bit de orden bajo que vale 1. Los resultados en la salida de cada uno de los bloques 81, 82 se comparan realizando la diferencia entre dichos resultados 83. Esta diferencia es nula cuando no se ha detectado ninguna anomalía. Un comparador con cero 84 se añade, por consiguiente, para comparar si hay o no fallos. El resultado del comparador 84 es transmitido a continuación en la entrada de un basculador 85 para fiabilizar la señal de salida. La señal FALLO en la salida del basculador sigue siendo 1 cuando no se ha detectado ninguna anomalía y toma el valor 0 en el caso contrario.

REIVINDICACIONES

1. Circuito protegido por lógica diferencial que procesa variables lógicas representadas por pares de componentes (a_t, a_f) (b_t, b_f), una primera red de células (T) que realizan funciones lógicas sobre la primera componente de dichos pares, una segunda red de células duales (F) que funciona en lógica complementaria sobre la segunda componente, **caracterizado porque** las componentes de los pares son agrupadas por vectores (A_t, A_f, B_t, B_f), comprendiendo dicho circuito módulos de detección compuestos por dos multiplicadores-acumuladores (81, 82) que realizan operaciones de multiplicación-acumulación entre los vectores (A_t, B_t) que agrupan a las primeras componentes de los pares por un lado y los vectores (A_f, B_f) que agrupan a las segundas componentes de los pares por otro lado, esto después de que un bit de orden bajo de valor 1 se haya añadido a cada uno de dichos vectores, siendo la diferencia calculada entre los resultados de las dos operaciones (83) y a continuación procesada por un comparador con cero (84) cuya salida toma el valor cero cuando se detecta un estado no coherente en las fases de precarga o de evaluación.

2. Circuito de acuerdo con la reivindicación 1, **caracterizado porque** la salida del comparador con cero (84) de los módulos de detección está conectada a una conexión oscilante (85) para generar una salida estable (FALLO), resultado de la detección de estados no coherentes.

3. Circuito protegido por lógica diferencial, preferiblemente definido por una cualquiera de las reivindicaciones 1 ó 2, que procesa variables lógicas representadas por pares de componentes (a_t, a_f) (b_t, b_f), una primera red de células (T) que realizan funciones lógicas sobre la primera componente de dichos pares, una segunda red de células duales (F) que funcionan en lógica complementaria sobre la segunda componente, estando las funciones lógicas realizadas por cada par de células en una fase de precarga que pone a las variables en un estado conocido en la entrada de las células seguida por una fase de evaluación en la que un cálculo es realizado por las células, comprendiendo dicho circuito una pluralidad de módulos de detección (47) de anomalías colocados en diferentes nodos del circuito, correspondiendo una anomalía a un estado no coherente que se produce durante la fase de precarga o durante la fase de evaluación, produciendo un módulo de detección una señal de salida (FALLO) que indica que se detecta una anomalía a nivel del nodo al que está asociado, **caracterizado porque** el circuito comprende medios para combinar dichas señales de salidas para generar una señal global de salida (FALLO_GLOBAL) cuyo estado indica que un fallo es detectado por al menos un módulo de detección.

4. Circuito de acuerdo con la reivindicación 3, **caracterizado porque** las salidas de los módulos de detección (FALLO) se recogen mediante encadenamiento, estando los resultados centralizados en al menos una equipotencial (56, 67) por medio de puertas “O” (53, 54, 63, 64).

5. Circuito de acuerdo con la reivindicación 4, **caracterizado porque** la salida de cada cadena de detección está conectada a un una conexión oscilante activada por la señal de reloj del circuito (CLK) y que genera la señal global de salida (FALLO_GLOBAL) que toma el valor 1 cuando al menos un estado no coherente es detectado por uno de los módulos de detección (51, 52, 61, 62) de la cadena.

6. Circuito de acuerdo con la reivindicación 3, **caracterizado porque** al menos una parte de los módulos de detección del circuito están organizados en árbol (71, 72, 73, 74), generando el último módulo de detección (74) una señal global que indica si al menos un estado no coherente ha sido detectado en uno de los nodos del circuito controlados por dichos módulos.

7. Circuito de acuerdo con una cualquiera de las reivindicaciones 3 a 6, **caracterizado porque** un módulo de detección comprende una puerta lógica utilizada para la detección de estados no coherentes que se producen durante la fase de precarga, siendo esta puerta lógica una puerta “O” si el estado coherente es (0,0) o una puerta “Y” si el estado coherente es (1,1).

8. Circuito de acuerdo con una cualquiera de las reivindicaciones 3 a 7, **caracterizado porque** un módulo de detección comprende una puerta lógica “XNOR” para la detección de estados no coherentes que se producen durante la fase de evaluación.

9. Circuito de acuerdo con una cualquiera de las reivindicaciones 3 a 8, **caracterizado porque** un módulo de detección comprende un multiplexor (35) que permite seleccionar la señal (FALLO) resultante de la detección de estados no coherentes, seleccionándose la salida de la puerta de detección de estados no coherentes en fase de precarga (34) durante la fase de precarga y seleccionándose la salida de la puerta de detección de estados no coherentes en fase de evaluación (33) durante la fase de evaluación, estando la selección controlada por una señal de configuración (PRE/EVAL).

10. Circuito de acuerdo con una cualquiera de las reivindicaciones anteriores, **caracterizado porque** el circuito protegido por lógica diferencial es un circuito criptográfico.

11. Circuito de acuerdo con una cualquiera de las reivindicaciones anteriores, **caracterizado porque** el circuito es un circuito programable de tipo FPGA.

12. Circuito de acuerdo con una cualquiera de las reivindicaciones anteriores, **caracterizado por ue** el circuito es un circuito de tipo ASIC.

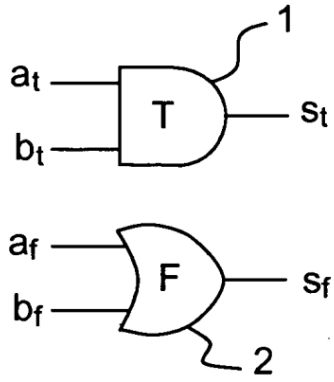
1
a_t
T
s_t
b_t
a_f
F
s_f
b_f
2

FIG.1

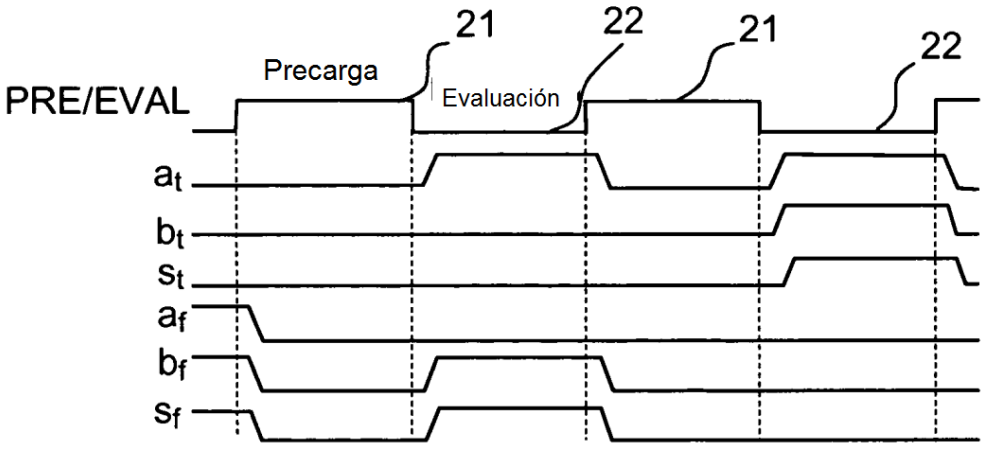
21
22
21
22
Precarga
Evaluación
PRE/EVAL
a_t
b_t
s_t
a_f
b_f
s_f

FIG.2

F2

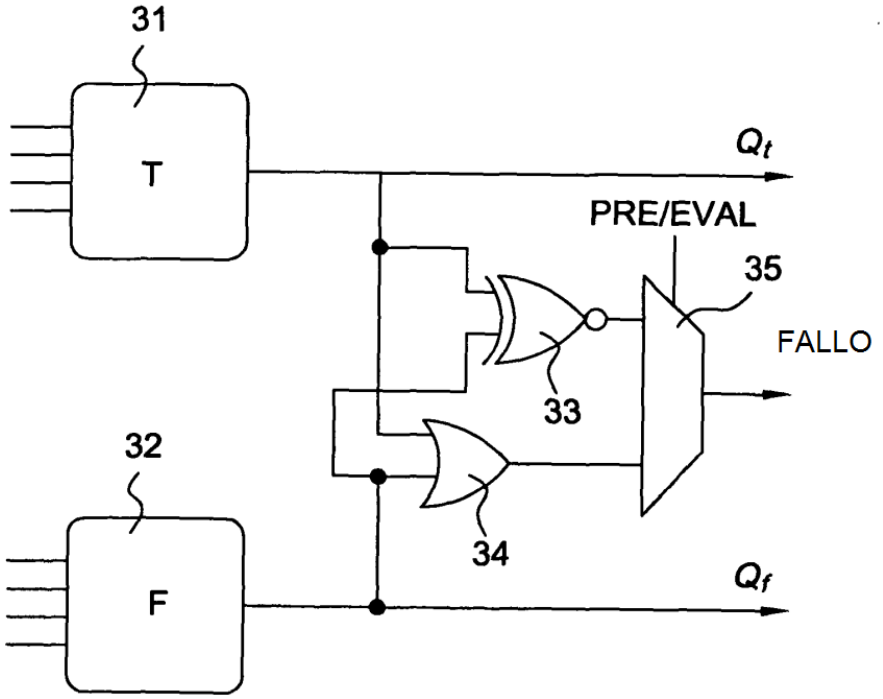
31
T
Q_t
PRE/EVAL
35
FALLO
33
32
34
F
Q_f

FIG.3

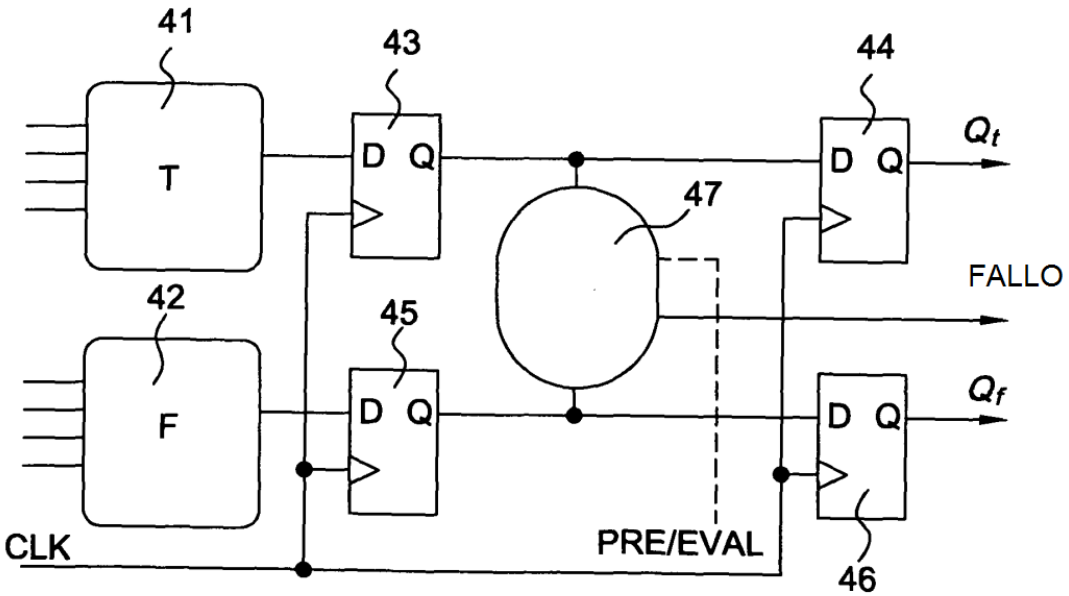
41
43
44
T
D Q
D Q
Q_t
47
FALLO
42
45
F
D Q
D Q
Q_f
CLK
PRE/EVAL
46

FIG.4

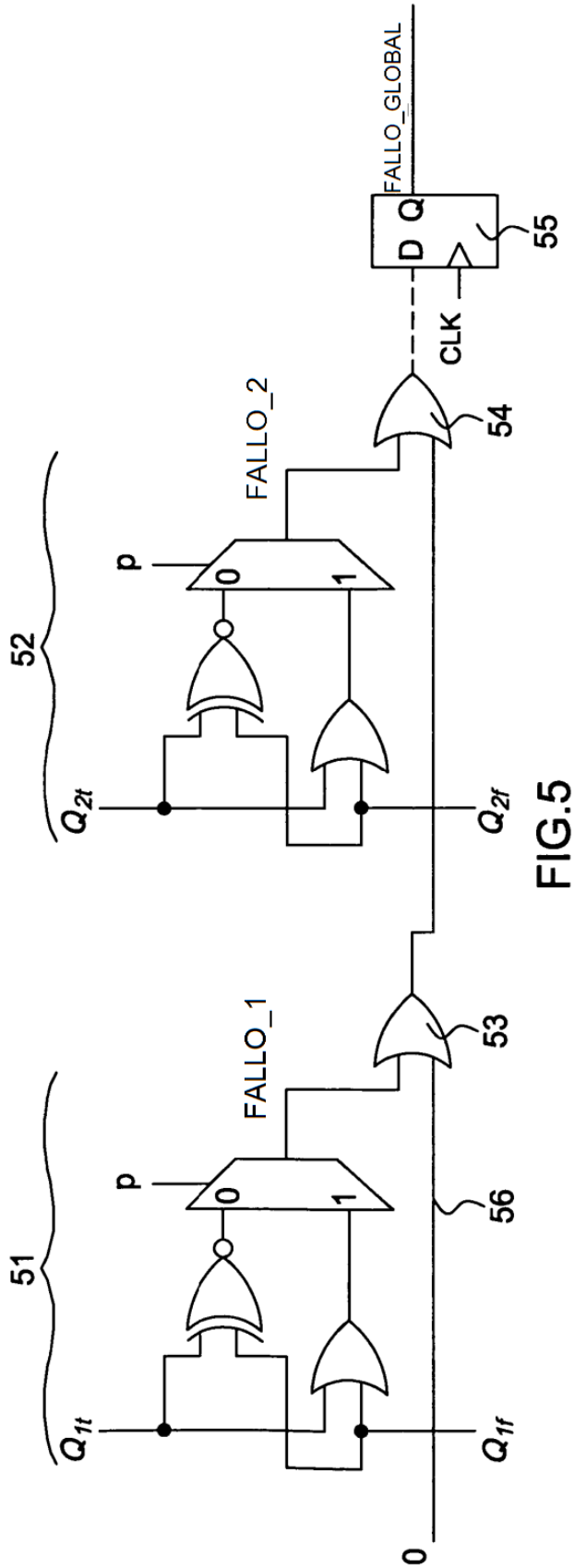
FALLO_GLOBAL
D Q
55
CLK
54
FALLO_2
p
0
1
52
Q_{2t}
Q_{2f}
53
FALLO_1
p
0
1
51
Q_{1t}
Q_{1f}
56
0

FIG.5

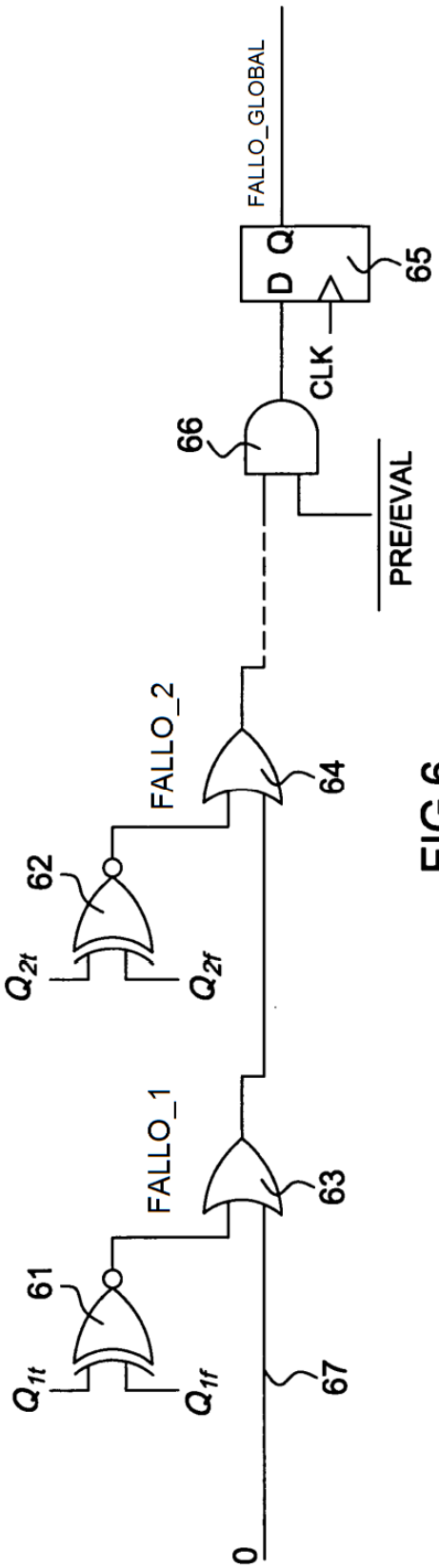
FALLO_GLOBAL
D Q
65
CLK
66
PRE/EVAL
FALLO_2
64
62
Q_{2t}
Q_{2f}
FALLO_1
63
61
Q_{1t}
Q_{1f}
67
0

FIG.6

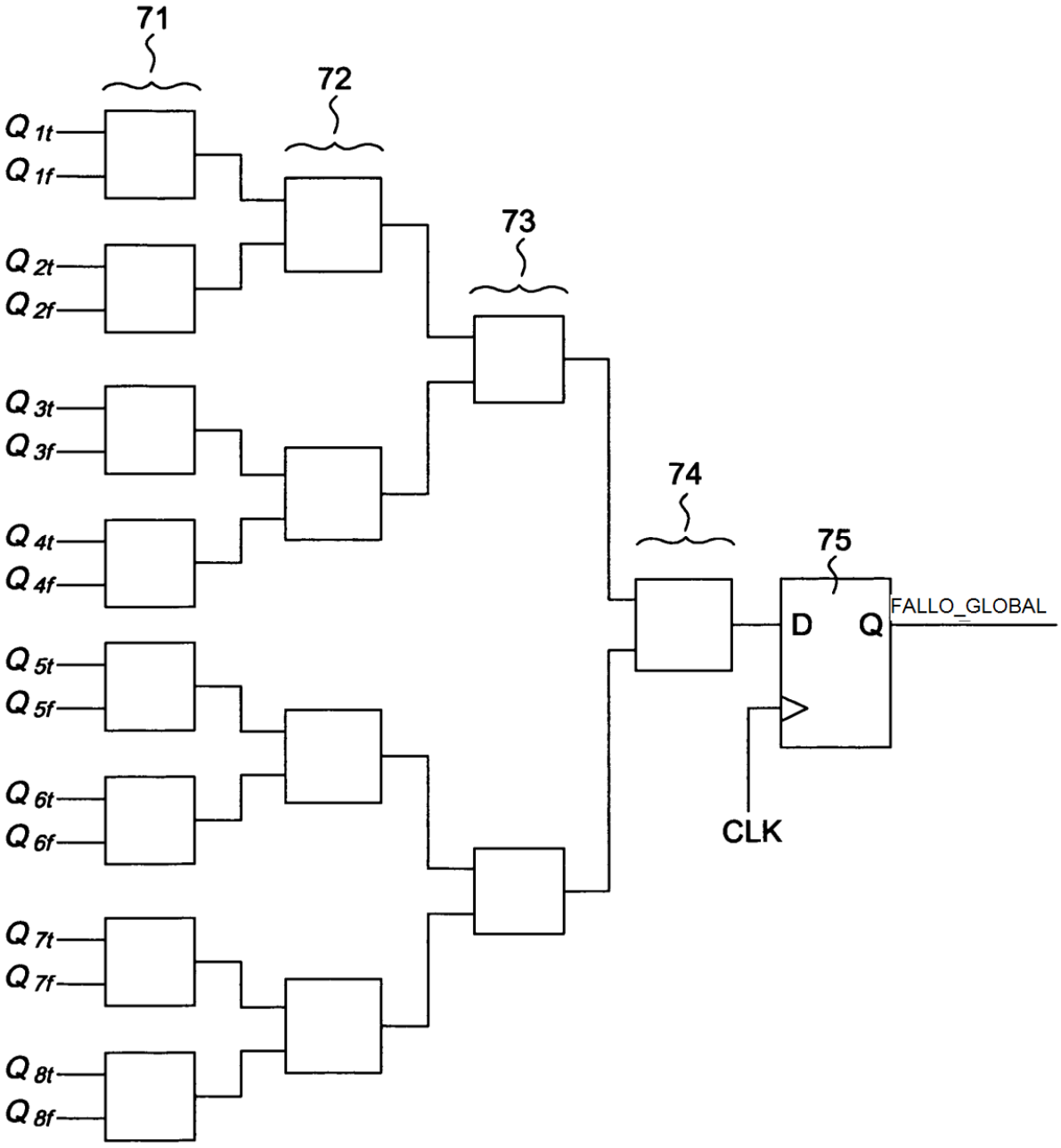
71
72
73
74
75
Q 1t
Q 1f
Q 2t
Q 2f
Q 3t
Q 3f
Q 4t
Q 4f
Q 5t
Q 5f
Q 6t
Q 6f
Q 7t
Q 7f
Q 8t
Q 8f
D
Q
FALLO_GLOBAL
CLK

FIG.7

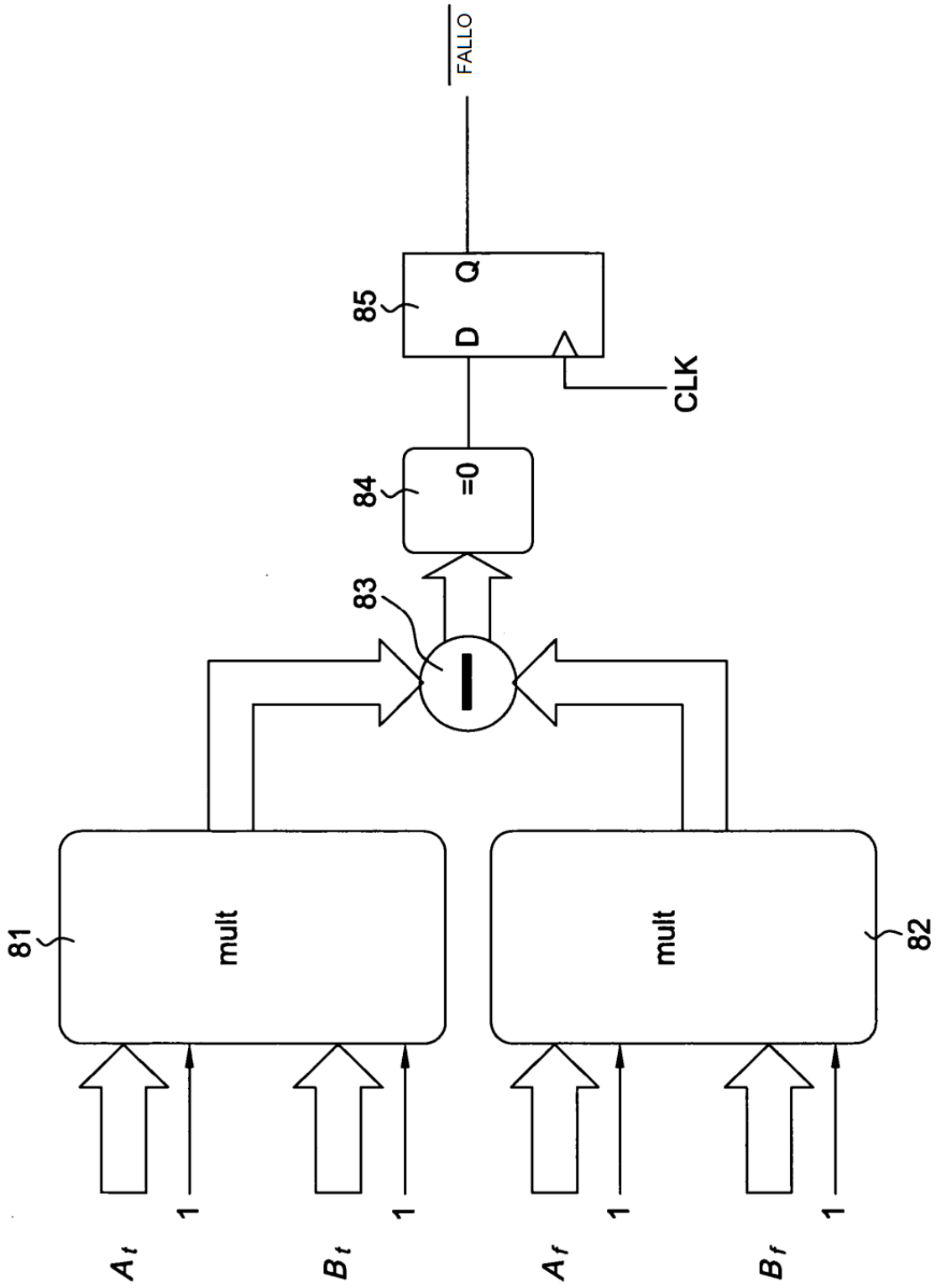

FIG.8