(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 807 214**

(51) Int. CI.:

G09C 1/00 (2006.01)
H04L 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.10.2016 E 16196520 (7)**

(97) Fecha y número de publicación de la concesión europea: **03.06.2020 EP 3200173**

(54) Título: **Procedimiento de protección de circuitos electrónicos contra interceptación por análisis de potencia y circuito electrónico que usa el mismo**

(30) Prioridad:

26.01.2016 IL 24378916

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.02.2021

(73) Titular/es:

WINBOND ELECTRONICS CORP. (100.0%)
No. 8 Keya 1st Rd., Daya District, Central Taiwan Science Park
Taichung City, Taiwan. , TW

(72) Inventor/es:

TEPER, VALERY y
TASHER, NIR

(74) Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

DESCRIPCIÓN

Procedimiento de protección de circuitos electrónicos contra interceptación por análisis de potencia y circuito electrónico que usa el mismo

Antecedentes de la invención

1. Campo de la invención

La invención se refiere a contramedidas para prevenir la determinación de claves criptográficas mediante análisis de potencia de un dispositivo criptográfico.

2. Descripción de la técnica relacionada

Cerca del final del siglo XX, ha sido descubierto que la información de un dispositivo criptográfico (por ejemplo, un lector de tarjetas inteligentes) puede ser revelada de manera no intrusiva mediante el análisis del consumo de potencia del dispositivo. Los ejemplos de procedimientos de análisis de potencia son conocidos como Análisis de Potencia Simple (SPA) y Análisis de Potencia Diferencial (DPA). El SPA implica el examen visual de gráficos de la corriente usada por un dispositivo en función del tiempo. Como ejemplo, cuando un circuito lógico de semiconductor complementario de óxido metálico (CMOS) cambia de un estado lógico 0 a un estado lógico 1, una cantidad significativa de corriente eléctrica es extraída de la fuente de alimentación, mientras que en el caso opuesto es extraída una cantidad insignificante. Del mismo modo, un microprocesador tiene diferentes perfiles de consumo de potencia para diferentes comandos. Por lo tanto, en una cantidad mínima de potencia de una tarjeta inteligente que realiza una codificación de estándar de codificación de datos (DES), se pueden ver claramente las diferentes rondas. Además, se pueden distinguir las operaciones de cuadratura y multiplicación de una implementación RSA, lo que permite que un interceptor calcule la clave secreta.

DPA analiza estadísticamente el consumo de potencia de un dispositivo criptográfico. DPA registra el consumo de potencia en muchas rondas y luego puede eliminar el ruido que evitaría el análisis basado en SPA.

Un procedimiento de protección contra el análisis de potencia está basado en ocultar el cálculo. Este procedimiento incluye el diseño del dispositivo criptográfico para que tenga un consumo de potencia uniforme o aleatorio independientemente de las operaciones a ser realizadas, por ejemplo, añadiendo aleatoriedad a la señal de fuga o complementando la señal de cálculo para lograr el consumo de potencia uniforme.

Un procedimiento alternativo de protección del dispositivo criptográfico es el enmascaramiento del cálculo. En este procedimiento, el dispositivo criptográfico está diseñado para añadir aleatoriedad al cálculo (por ejemplo, cálculos innecesarios adicionales que deben ser ejecutados con el cálculo) de modo que el consumo de potencia sea diferente para cada ronda, incluso si son analizados los mismos datos.

Otros procedimientos añaden ruido aleatorio y/o aleatorizan el reloj de señal para dificultar que el cálculo sea identificado por DPA.

Típicamente, cada procedimiento de protección del dispositivo criptográfico está asociado con un nivel de complejidad y puede superarse si se invierte un esfuerzo suficiente. Por lo tanto, es interesante encontrar procedimientos más complejos para evitar que el procedimiento sea violado.

En el documento “A Countermeasure against Differential Power Analysis based on Random Delay Insertion"- Bucci M et al desvelan una contramedida a nivel de puerta que permite la aleatorización del perfil de consumo de corriente instantáneo y la cantidad de carga total transferida desde la fuente de alimentación durante un ciclo de reloj al explotar la inserción de retrasos aleatorios en la trayectoria de datos de un procesador criptográfico. La Solicitud de Patente de los Estados Unidos US 2011/252244 desvela una disposición segura de circuito criptográfico que incluye un bloque de procesamiento criptográfico, un generador de secuencia de expansión y una unidad de control de retardo. La Solicitud de Patente de los Estados Unidos desvela un aparato de procesamiento de datos configurado para ejecutar una operación de procesamiento de datos en al menos un valor de datos en respuesta a una instrucción de procesamiento de datos.

Sumario de la invención

Un aspecto de una realización de la divulgación se refiere a un circuito electrónico y a un procedimiento de protección de un cálculo lógico que es realizado en un conjunto de bits para que no sea descodificado mediante el análisis del consumo de potencia del circuito. El procedimiento incluye dividir el cálculo en dos o más etapas para que el cálculo sea realizado en dos ciclos de reloj en lugar de uno. En el primer ciclo, parte de los bits son proporcionados a una unidad lógica del circuito y parte de los bits son reemplazados por valores aleatorios. La unidad lógica calcula un primer resultado a partir de los datos parciales. Luego, en el siguiente ciclo, son proporcionados los datos correctos de los bits reubicados a la unidad lógica. La unidad lógica calcula resultados adicionales con los datos correctos. Los resultados adicionales se proporcionan a un elemento de almacenamiento para que sirva como un conjunto de bits para el siguiente estado del circuito.

En una realización ilustrativa de la presente divulgación, el circuito selecciona aleatoriamente la mitad de los bits para el primer ciclo o el recíproco del número de ciclos. Alternativamente, el circuito selecciona un número aleatorio de bits para el primer ciclo y los ciclos adicionales. En algunas realizaciones de la presente divulgación, en el siguiente ciclo o ciclos, los bits son proporcionados desde una unidad de almacenamiento intermedia para que el elemento de almacenamiento pueda ser cambiado mediante el cálculo de la unidad lógica en el primer ciclo.

De este modo, es proporcionado, de acuerdo con una realización ilustrativa de la presente divulgación, un circuito electrónico con protección contra interceptación por análisis de potencia. El circuito electrónico incluye un elemento de almacenamiento para almacenar un conjunto de bits correspondiente a los valores correctos, una unidad lógica para procesar el conjunto almacenado de bits y proporcionar un conjunto de siguiente estado de bits luego de dos ciclos, y un generador de bits aleatorios. Además, en un primer ciclo, algunos del conjunto almacenado de bits son proporcionados a la unidad lógica correctamente y algunos son reemplazados por valores aleatorios, y en un último ciclo, todo el conjunto almacenado de bits son proporcionados correctamente a la unidad lógica. El generador de bits aleatorios genera un bit aleatorio para cada bit del conjunto almacenado de bits para determinar qué bits del conjunto almacenado de bits deben ser proporcionados correctamente y qué bits deben ser reemplazados en cada ciclo.

En una realización ilustrativa de la presente divulgación, el circuito electrónico es controlado por dos señales de reloj, y una de las señales de reloj tiene la mitad de frecuencia que la otra. Opcionalmente, el circuito incluye una unidad de almacenamiento intermedia asociada con el elemento de almacenamiento para almacenar los valores correctos del conjunto almacenado de bits para su uso en el último ciclo. En una realización ilustrativa de la presente divulgación, el circuito incluye un selector asociado con el elemento de almacenamiento y el generador de bits aleatorios para cada bit del conjunto almacenado de bits. Además, el selector es controlado por los bits aleatorios para seleccionar entre el valor correcto y el valor aleatorio. Opcionalmente, el conjunto almacenado de bits son almacenados en el elemento de almacenamiento en forma codificada. En una realización ilustrativa de la presente divulgación, el conjunto almacenado de bits son descodificados cuando son proporcionados a la unidad lógica. En un segundo ciclo, los bits reemplazados que corresponden a los valores aleatorios son reemplazados con los valores correspondientes de los valores correctos y son proporcionados a la unidad lógica. En una realización ilustrativa de la presente divulgación, la mitad de los bits son reemplazados por valores aleatorios en el primer ciclo. Opcionalmente, un número aleatorio de bits son reemplazados por valores aleatorios en el primer ciclo. En una realización ilustrativa de la presente divulgación, los bits seleccionados aleatoriamente para ser reemplazados están configurados como valores opuestos de los valores correspondientes de los valores correctos.

Además, es proporcionado, de acuerdo con una realización ilustrativa de la presente divulgación, un procedimiento de protección de un circuito electrónico contra interceptación por análisis de potencia. El procedimiento incluye: almacenar un conjunto inicial de bits correspondientes a valores correctos en un elemento de almacenamiento; generar un bit aleatorio para cada bit del conjunto almacenado de bits; en un primer ciclo, proporcionar correctamente algunos de los bits del elemento de almacenamiento a una unidad lógica y reemplazar el resto de los bits por valores aleatorios; en un último ciclo, proporcionar todo el conjunto almacenado de bits correctamente a la unidad lógica; y procesar todo el conjunto almacenado de bits en el último ciclo para proporcionar un conjunto de siguiente estado de bits.

En una realización ilustrativa de la presente divulgación, el circuito es controlado por dos señales de reloj, y una de las señales de reloj tiene la mitad de frecuencia que la otra. Opcionalmente, el procedimiento incluye además almacenar los valores correctos del conjunto almacenado de bits para su uso en el último ciclo en una unidad de almacenamiento intermedia asociada con el elemento de almacenamiento. El procedimiento incluye además seleccionar entre el valor correcto y el valor aleatorio de acuerdo con el bit aleatorio mediante un selector para cada bit del conjunto almacenado de bits. Opcionalmente, la etapa de almacenar un conjunto inicial de bits incluye además codificar el conjunto almacenado de bits, y la etapa de proporcionar todo el conjunto almacenado de bits a la unidad lógica en el último ciclo incluye además descodificar el conjunto almacenado de bits. Opcionalmente, la etapa de proporcionar todo el conjunto almacenado de bits a la unidad lógica en el último ciclo incluye además obtener algunos de los bits del elemento de almacenamiento en el primer ciclo y reemplazar el resto de los bits que han sido reemplazados por los valores aleatorios en el primer ciclo con los valores correspondientes de los valores correctos. En una realización ilustrativa de la presente divulgación, la mitad de los bits son reemplazados por los valores aleatorios en el primer ciclo. Opcionalmente, un número aleatorio de bits son reemplazados por los valores aleatorios en el primer ciclo. En una realización ilustrativa de la presente divulgación, los bits seleccionados aleatoriamente para ser reemplazados están configurados como valores opuestos de los valores correspondientes de los valores correctos.

Breve descripción de los dibujos

Los dibujos adjuntos están incluidos para proporcionar una comprensión adicional de la invención, y están incorporados en y constituyen una parte de la presente especificación. Los dibujos ilustran realizaciones de la invención y, junto con la descripción, sirven para explicar los principios de la invención.

La Fig. 1 es una ilustración esquemática de un sistema para ejecutar un ataque de potencia en un dispositivo criptográfico de acuerdo con una realización ilustrativa de la presente divulgación.

La Fig. 2 es una ilustración esquemática de un circuito lógico de un dispositivo criptográfico de acuerdo con una realización ilustrativa de la presente divulgación.

La Fig. 3 es una ilustración esquemática de un circuito lógico de dos bits de un dispositivo criptográfico de

acuerdo con una realización ilustrativa de la presente divulgación.

La Fig. 4 es una ilustración esquemática de un circuito lógico mejorado de un dispositivo criptográfico de acuerdo con una realización ilustrativa de la presente divulgación.

La Fig. 5 es una ilustración esquemática de señales lógicas y consumo de potencia en función del tiempo de acuerdo con una realización ilustrativa de la presente divulgación.

La Fig. 6 es un diagrama de flujo de un procedimiento para ejecutar cálculos lógicos en dos ciclos de acuerdo con una realización ilustrativa de la presente divulgación.

La Fig. 7 es una ilustración esquemática de un circuito lógico mejorado de un dispositivo criptográfico que también enmascara el siguiente estado de acuerdo con una realización ilustrativa de la presente divulgación.

La Fig. 8 es una ilustración esquemática de un circuito lógico mejorado alternativo de un dispositivo criptográfico que también enmascara el siguiente estado de acuerdo con una realización ilustrativa de la presente divulgación.

Descripción de las realizaciones

A continuación, se hará referencia en detalle a las realizaciones preferentes de la presente invención, cuyos ejemplos son ilustrados en los dibujos adjuntos. Siempre que sea posible, son usados los mismos números de referencia en los dibujos y la descripción para referirse a las mismas partes o partes similares.

La Fig. 1 es una ilustración esquemática de un sistema 100 para realizar un ataque de potencia en un dispositivo criptográfico 110 de acuerdo con una realización ilustrativa de la presente divulgación. En una realización ilustrativa de la presente divulgación, puede ser usado un osciloscopio 140 u otro dispositivo de medición de potencia para monitorizar una entrada de potencia 150 del dispositivo criptográfico 110. Opcionalmente, el dispositivo criptográfico 110 puede ser un lector de tarjetas (por ejemplo, para leer una tarjeta inteligente 120), un chip en un circuito u otras implementaciones.

En una realización ilustrativa de la presente divulgación, un ordenador de propósito general 130 está programado para comunicar con el dispositivo criptográfico 110, por ejemplo para proporcionar instrucciones al dispositivo criptográfico 110 y recibir información de la transacción no codificada. Opcionalmente, durante el uso, el dispositivo criptográfico 110 lee información sin codificar, por ejemplo desde una tarjeta inteligente 120 y proporciona información sin codificar al ordenador 130 para realizar una transacción. En una realización ilustrativa de la descripción, el osciloscopio 140 controla el consumo de potencia del dispositivo criptográfico 110 y proporciona una señal grabada 160 al ordenador 130 para su análisis. Opcionalmente, en base a la información del dispositivo criptográfico 110 y/o el osciloscopio 140, el ordenador 130 puede determinar las claves criptográficas u otra información confidencial utilizada para codificar la información.

La Fig. 2 es una ilustración esquemática de un circuito lógico 200 del dispositivo criptográfico 110 de acuerdo con una realización ilustrativa de la presente divulgación. En una realización ilustrativa de la presente divulgación, el circuito lógico 200 incluye elementos de almacenamiento 220 (flip-flops S0 ... Sn) para almacenar un valor/estado actual y una unidad lógica combinacional 210 que acepta datos de los elementos de almacenamiento 220 y calcula el siguiente valor/estado, y el siguiente valor/estado es almacenado nuevamente en los elementos de almacenamiento. En una realización ilustrativa de la presente divulgación, el circuito lógico 200 está provisto inicialmente con un valor de entrada externo 230, por ejemplo, valores leídos desde una tarjeta inteligente. Opcionalmente, el circuito lógico 200 ejecuta uno o más ciclos de procesamiento produciendo unas pocas generaciones de los siguientes valores a partir del valor de entrada externo 230 y luego enviando el valor procesado/descodificado, por ejemplo al ordenador 130.

La Fig. 3 es una ilustración esquemática de un circuito lógico de dos bits 300 del dispositivo criptográfico 110 de acuerdo con una realización ilustrativa de la presente divulgación. En una realización ilustrativa de la descripción, el circuito lógico 300 incluye un elemento de almacenamiento 320 con dos flip flops (S0 y S1) para almacenar el estado actual y una unidad lógica combinada 310 que en este caso incrementa el valor de almacenamiento en 1 y almacena los valores incrementados como el siguiente estado nuevamente en el elemento de almacenamiento 320. Una línea de tiempo 360 muestra los valores de reloj de una señal de reloj CLK que controla el circuito lógico 300 y las líneas de tiempo 370 y 380 muestran los valores almacenados en el elemento de almacenamiento 320 para el siguiente estado y estado actual respectivamente. En este caso, el circuito lógico 300 implementa un contador simple que cuenta de 0 a 3.

En una realización ilustrativa de la presente divulgación, hay dos ubicaciones que son vulnerables con respecto a un ataque de potencia y pueden servir como posibles fugas para el contenido del circuito lógico (por ejemplo, 200 y 300). La primera ubicación es de la unidad lógica (por ejemplo, 210, 310) durante el cálculo del siguiente valor/estado, y la segunda ubicación es cuando se actualiza el almacenamiento, por ejemplo al almacenar el siguiente valor/estado nuevamente en el elemento de almacenamiento (por ejemplo, 220, 320). En una realización ilustrativa de la presente divulgación, para evitar que un interceptor use el análisis de potencia para determinar el contenido actual del circuito lógico, el cálculo está dividido en dos o más ciclos.

La Fig. 4 es una ilustración esquemática de un circuito lógico 400 mejorado del dispositivo criptográfico 110 de acuerdo

a una realización ilustrativa de la presente divulgación. En una realización ilustrativa de la presente divulgación, el circuito lógico 400 mejorado incluye un elemento de almacenamiento 420 con dos o más flip flops (S0, S1 ... Si ... Sm, solo se muestran S0 y S1 por simplicidad). El circuito lógico 400 también incluye una unidad lógica combinacional 410 que proporciona los siguientes bits de estado N0, N1 ... Ni ... Nm en respuesta a su entrada (por simplicidad, sólo son mostrados N0 y N1).

El circuito lógico 400 incluye un generador de bits aleatorios 440 que proporciona m bits aleatorios (R0, R1 ... Ri ... Rm) como el elemento de almacenamiento 420. Opcionalmente, un bit aleatorio Ri que tiene un valor de cero significa que el bit almacenado en el flip flop Si debe ser transferido a la unidad lógica 410 en un primer ciclo, mientras que un bit aleatorio Ri que tiene un valor de uno significa que el bit almacenado en el flip flop Si debe ser transferido a la lógica unidad 410 solo en un segundo ciclo. Los bits aleatorios Ri seleccionan aleatoriamente 1 o más o de los bits almacenados en los flip flops SO a Sm para ser procesados por la unidad lógica combinacional 410 en el primer ciclo y seleccionan los bits restantes para ser procesados por la unidad lógica combinacional 410 solo en el segundo ciclo. Opcionalmente, el generador de bits aleatorios 440 puede proporcionar una secuencia de bits aleatoria en la que la mitad de los bits son cero, de modo que la mitad de los bits se procesan en el primer ciclo y luego todos los bits se procesan en el segundo ciclo. Esto divide el cálculo procesado por la unidad lógica combinacional 410 en dos ciclos y evita que el cálculo sea descodificado por análisis de potencia.

Es proporcionado un selector Li (L0 y L1 son mostrados en la Fig. 4) para cada bit almacenado en el flip flop Si. Opcionalmente, cuando el bit aleatorio Ri es cero, el selector transfiere el valor correcto del bit almacenado en el flip flop Si a la unidad lógica combinacional 410. Sin embargo, cuando Ri es 1, entonces en el primer ciclo, un valor aleatorio (Ri, por ejemplo, R0 y R1 mostrado en la Fig. 4) es proporcionado a la unidad lógica combinacional 410 desde un flujo aleatorio 460 por una puerta XOR 480 y en el segundo ciclo, el bit almacenado en el flip flop Si se transfiere a la unidad lógica combinacional 410. Opcionalmente, los valores aleatorios son los mismos (Ri) según lo proporcionado por el generador de bits aleatorios 440 o pueden provenir de un generador de bits aleatorios distinto. Del mismo modo, los bits que se seleccionan en forma aleatoria para ser reemplazados pueden establecerse en el valor opuesto del valor correcto (por ejemplo, uno en lugar de cero y cero en lugar de uno). El circuito lógico 400 mejorado incluye un indicador 450 que proporciona un valor de 1 para el primer ciclo y un valor de cero para el segundo ciclo. Opcionalmente, en el primer ciclo, el valor de 1 permite proporcionar un valor aleatorio al selector Li y luego proporcionar a la unidad lógica combinacional 410 si Ri tiene un valor de 1. En una realización ilustrativa de la presente divulgación, las unidades de almacenamiento intermedio 470 se proporcionan para preservar el valor del bit almacenado en el flip flop Si para el segundo ciclo en el caso de que Ri sea 1.

La Fig. 5 es una ilustración esquemática 500 de señales lógicas y consumo de potencia en función del tiempo del circuito lógico 400 mejorado y la Fig. 6 es un diagrama de flujo de un procedimiento 600 para ejecutar cálculos lógicos en dos ciclos de acuerdo con un realización ilustrativa de la presente divulgación. El circuito lógico 400 mejorado usa 2 señales de reloj, una que tiene una frecuencia de reloj clk 510 y una que tiene la mitad de la frecuencia clk/2 520. Opcionalmente, algunos de los elementos del circuito funcionan en la frecuencia clk 510 y algunos funcionan a la mitad de la frecuencia clk/2 520 (en dos ciclos). En una realización ilustrativa de la presente divulgación, el circuito lógico 400 acepta valores de un conjunto inicial almacenado de bits en los flip flops Si en el elemento de almacenamiento 420 (etapa 610). Una señal 550 muestra un conjunto ilustrativo de bits almacenados en los flip flops Si en el circuito lógico 400 mejorado. Opcionalmente, el generador de bits aleatorios 440 genera un conjunto aleatorio de los bits Ri como es mostrado mediante una señal 530 para determinar cuál de los bits almacenados en los flip flops Si son usados en el primer ciclo y qué bits sólo son usados en el segundo ciclo (etapa 620).

En el primer ciclo, algunos de los bits almacenados en los flip flops Si son transferidos desde el elemento de almacenamiento 420 a la unidad lógica combinacional 410 y algunos bits son reemplazados por valores aleatorios (etapa 630). Los bits aleatorios Ri determinan qué bits son transferidos y qué bits son reemplazados en el primer ciclo. En el segundo ciclo, todos los bits son transferidos desde el elemento de almacenamiento 420 a la unidad lógica combinacional 410 (los bits aleatorios son reemplazados por los bits reales) (etapa 640). Opcionalmente, en el segundo ciclo, menos bits cambian de 0 a 1 consumiendo una gran cantidad de potencia en la unidad lógica combinacional 410, ya que casi la mitad ya ha cambiado en el ciclo anterior. El resultado del procesamiento por la unidad combinacional lógica 410 sirve como los siguientes bits de estado Ni (540) que se almacenarán nuevamente en el elemento de almacenamiento 420 (etapa 650).

En una realización ilustrativa de la presente divulgación, una línea de tiempo 560 muestra un uso de potencia estándar por un circuito lógico en relación con una línea de tiempo 570 que muestra el consumo de potencia dividido aleatoriamente en dos partes durante los dos ciclos. Algunos de los bits están configurados correctamente en el primer ciclo y otros sólo son corregidos en el segundo ciclo.

La Fig. 7 es una ilustración esquemática de un circuito lógico 700 mejorado del dispositivo criptográfico 110 que también enmascara los siguientes bits de estado Ni (540) de acuerdo con una realización ilustrativa de la presente divulgación. El circuito lógico 700 mejorado es similar al circuito lógico 400 mejorado, excepto que, como fue explicado con anterioridad, el circuito lógico 400 mejorado solo impide el análisis de potencia de la unidad lógica combinacional 410 y no del elemento de almacenamiento 420. En el circuito lógico 700, son usadas un par de puertas XOR interconectadas (710, 720) para codificar y descodificar los bits de datos almacenados en el elemento de almacenamiento 420. U opcionalmente, la puerta XOR 710 aplica una máscara aleatoria a los siguientes bits de estado Ni para que los siguientes bits de estado Ni sean codificados aleatoriamente cuando se almacenan en el elemento de

almacenamiento 420 para evitar interceptación con análisis de potencia. Igualmente, la puerta XOR 720 aplica la máscara aleatoria para descodificar los bits almacenados en los flip flops Si cuando llegan a la unidad lógica combinacional 410, para que se procesen los datos correctos.

La Fig. 8 es una ilustración esquemática de un circuito lógico mejorado alternativo 800 de un dispositivo criptográfico que también enmascara el siguiente estado de acuerdo con una realización ilustrativa de la presente divulgación. El circuito lógico mejorado 800 es similar al circuito lógico mejorado 700, excepto que se implementa sin unidades de almacenamiento intermedio 470.

Debe apreciarse además que los procedimientos y aparatos descritos con anterioridad pueden variar de muchas maneras, incluyendo la misión y agregado de pasos, cambiando el orden de los pasos y el tipo de dispositivos utilizados. Debe apreciarse que diferentes características pueden combinarse de diferentes maneras. En particular, no todas las características mostradas con anterioridad en una realización particular son necesarias en cada realización de la divulgación. Otras combinaciones de las características anteriores también se consideran dentro del alcance de las reivindicaciones adjuntas. Los expertos en la materia también apreciarán que la presente descripción no se limita a lo que se ha mostrado y descrito particularmente con anterioridad.

REIVINDICACIONES

1. Un circuito electrónico (110, 400, 700, 800) con protección contra interceptación por análisis de potencia, que comprende:

un elemento de almacenamiento (420) configurado para almacenar un conjunto de bits correspondientes a valores correctos, en el que el elemento de almacenamiento (420) es accionado por una primera señal de reloj (clk/2 520) que tiene una primera frecuencia;

un generador de bits aleatorios (440), configurado para generar un bit aleatorio (R0, R1, Ri) para cada uno del conjunto de bits almacenado correspondiente a los valores correctos respectivamente, siendo dicho generador de bits aleatorios accionado por la primera señal de reloj;

un indicador (450), accionado por una segunda señal de reloj en una segunda frecuencia que es de dos veces la primera frecuencia, configurado para proporcionar un primer valor para un primer ciclo de la segunda señal de reloj y un segundo valor para un segundo ciclo de la segunda señal de reloj;

una pluralidad de selectores (L0, L1), acoplados al elemento de almacenamiento (420) y al generador de bits aleatorios (440), siendo cada selector accionado por uno de los bits aleatorios y estando configurado ya sea para el bit correspondiente del conjunto de bits almacenado correspondiente a los valores correctos, o para un bit reemplazado,

en el que el primer valor permite que un valor aleatorio sea proporcionado como el bit reemplazado, y el segundo valor permite que el valor correcto sea establecido como el bit reemplazado; y

una unidad lógica combinacional (410), acoplada a la pluralidad de selectores (L0, L1), configurada para proporcionar un siguiente conjunto de bits de estado (N0, N1, 540) luego de dos ciclos de la segunda señal de reloj al elemento de almacenamiento (420), en el que la unidad lógica combinacional (410) está configurada para realizar un primer cálculo lógico en la salida de la pluralidad de selectores (L0, L1) incluyendo cada uno de los bits reemplazados en el primer ciclo, y está configurada para realizar un último cálculo lógico sobre todo el conjunto de bits almacenado correspondiente a los valores correctos en el segundo ciclo.

2. Un circuito electrónico (110, 400, 700, 800) con protección contra interceptación por análisis de potencia, que comprende:

un elemento de almacenamiento (420) configurado para almacenar un conjunto de bits correspondientes a valores correctos, en el que el elemento de almacenamiento (420) es accionado por una primera señal de reloj (clk/2 520) que tiene una primera frecuencia;

un generador de bits aleatorios (440), configurado para generar un bit aleatorio (R0, R1, Ri) para cada uno del conjunto de bits almacenado correspondiente a valores correctos respectivamente, siendo dicho generador de bits aleatorios accionado por la primera señal de reloj;

un indicador (450), accionado por una segunda señal de reloj a una segunda frecuencia que es de dos veces la primera frecuencia, configurado para proporcionar un primer valor para un primer ciclo de la segunda señal de reloj y un segundo valor para un segundo ciclo de la segunda señal de reloj;

una pluralidad de selectores (L0, L1), acoplados al elemento de almacenamiento (420) y al generador de bits aleatorios (440), siendo cada selector accionado por uno de los bits aleatorios y estando configurado ya sea para el bit correspondiente del conjunto de bits almacenado correspondiente a los valores correctos, o un bit reemplazado,

en el que el primer valor permite que el valor opuesto del valor correcto sea proporcionado como el bit reemplazado, y el segundo valor permite que el valor correcto sea establecido como el bit reemplazado; y una unidad lógica combinacional (410), acoplada a la pluralidad de selectores (L0, L1), configurada para proporcionar un siguiente conjunto de bits de estado (N0, N1, 540) luego de dos ciclos de la segunda señal de reloj al elemento de almacenamiento (420), en el que la unidad lógica combinacional (410) está configurada para realizar un primer cálculo lógico en la salida de la pluralidad de selectores (L0, L1) incluyendo cada uno de los bits reemplazados en el primer ciclo, y está configurada para realizar un último cálculo lógico en todo el conjunto de bits almacenado correspondiente a los valores correctos en el segundo ciclo.

3. El circuito electrónico (110, 400) de acuerdo con la reivindicación 1 o la reivindicación 2, que comprende además una unidad de almacenamiento intermedio (470) asociada con el elemento de almacenamiento (420) para almacenar el conjunto de bits almacenado para uso en el segundo ciclo.

4. El circuito electrónico (110, 400, 700, 800) de acuerdo con la reivindicación 1 o la reivindicación 2, en el que el conjunto de bits almacenado está codificado por las primeras puertas XOR (710) y almacenado en el elemento de almacenamiento (420), y el conjunto de bits almacenado está descodificado por las segundas puertas XOR

(720) cuando son proporcionados a la unidad lógica combinacional (410), en el que las primeras puertas XOR y las segundas puertas XOR están interconectadas.

5. Un procedimiento (600) de protección de un circuito electrónico (110, 200, 300, 400, 700, 800) contra interceptación por análisis de potencia, que comprende:

almacenar (610) un conjunto inicial de bits correspondientes a valores correctos en un elemento de almacenamiento (420) accionado por una primera señal de reloj (clk/2 520) que tiene una primera frecuencia;

generar (620), mediante un generador de bits aleatorios (440) accionado por la primera señal de reloj, un bit aleatorio (R0, R1, Ri) para cada uno del conjunto inicial de bits almacenado correspondiente a los valores correctos respectivamente;

proporcionar, mediante un indicador (450) accionado por una segunda señal de reloj a una segunda frecuencia que es de dos veces la primera frecuencia, un primer valor para un primer ciclo de la segunda señal de reloj y un segundo valor para un segundo ciclo de la segunda señal de reloj;

emitir, mediante un selector accionado por un bit aleatorio respectivo, ya sea el bit correspondiente del conjunto de bits almacenado correspondiente a los valores correctos, o un bit reemplazado,

en el que el primer valor permite que un valor aleatorio sea proporcionado como el bit reemplazado, y el segundo valor permite que el valor correcto sea establecido como el bit reemplazado;

proporcionar, mediante una unidad lógica combinacional (410), un siguiente estado de bits luego de dos ciclos de la segunda señal de reloj al elemento de almacenamiento (420), en el que la realización de cálculos lógicos en un ciclo de la segunda señal de reloj comprende:

en el primer ciclo, realizar un primer cálculo lógico en la salida de la pluralidad de selectores incluyendo cada uno de los bits reemplazados; y

en el segundo ciclo, realizar un último cálculo lógico en todo el conjunto inicial de bits almacenado correspondiente a los valores correctos; y

almacenar el siguiente conjunto de bits de estado (N0, N1, 540) en el elemento de almacenamiento (420).

6. Un procedimiento (600) de protección de un circuito electrónico (110, 200, 300, 400, 700, 800) contra interceptación por análisis de potencia, que comprende:

almacenar (610) un conjunto inicial de bits correspondientes a valores correctos en un elemento de almacenamiento (420) accionado por una primera señal de reloj (clk/2 520) que tiene una primera frecuencia

generar (620), mediante un generador de bits aleatorios (440) accionado por la primera señal de reloj, un bit aleatorio (R0, R1, Ri) para cada uno del conjunto inicial de bits almacenado correspondiente a los valores correctos respectivamente;

proporcionar, mediante un indicador (450) accionado por una segunda señal de reloj a una segunda frecuencia que es de dos veces la primera frecuencia, un primer valor para un primer ciclo de la segunda señal de reloj y un segundo valor para un segundo ciclo de la segunda señal de reloj;

emitir, mediante un selector accionado por un bit aleatorio respectivo, ya sea el bit correspondiente del conjunto de bits almacenado correspondiente a los valores correctos, o un bit reemplazado,

en el que el primer valor permite que el valor opuesto al valor correcto sea proporcionado como el bit reemplazado, y el segundo valor permite que el valor correcto sea establecido como el bit reemplazado;

proporcionar, mediante una unidad lógica combinacional (410), un siguiente estado de bits luego de dos ciclos de la segunda señal de reloj al elemento de almacenamiento (420), en el que la realización de cálculos lógicos en un ciclo de la segunda señal de reloj comprende:

en el primer ciclo, realizar un primer cálculo lógico en la salida de la pluralidad de selectores incluyendo cada uno de los bits reemplazados; y

en el segundo ciclo, realizar un último cálculo lógico sobre todos el conjunto inicial de bits almacenado correspondiente a los valores correctos; y

almacenar el siguiente conjunto de bits de estado (N0, N1, 540) en el elemento de almacenamiento (420).

7. El procedimiento (600) de acuerdo con la reivindicación 5 o la reivindicación 6, que comprende además almacenar el conjunto inicial de bits almacenado para uso en el segundo ciclo en una unidad de almacenamiento intermedio

(470) asociada con el elemento de almacenamiento (420).

8. El procedimiento (600) de acuerdo con la reivindicación 5 o la reivindicación 6, en el que la etapa de almacenamiento del conjunto inicial de bits comprende además codificar el conjunto inicial de bits almacenado usando las primeras puertas XOR (710), y la etapa del segundo ciclo, realizar el último cálculo lógico en todos los conjuntos iniciales de bits almacenados, comprende además descodificar el conjunto inicial de bits almacenado mediante el uso de las segundas puertas XOR (720) antes de realizar el último cálculo lógico.

9. El procedimiento (600) de acuerdo con la reivindicación 5, en el que la mitad del conjunto inicial de bits almacenado es reemplazado por los valores aleatorios proporcionados por el generador de bits aleatorios (440) en el primer ciclo.

10. El procedimiento (600) de acuerdo con la reivindicación 5, en el que un número aleatorio del conjunto inicial de bits almacenado es reemplazado por los valores aleatorios proporcionados por el generador de bits aleatorios (440) en el primer ciclo.

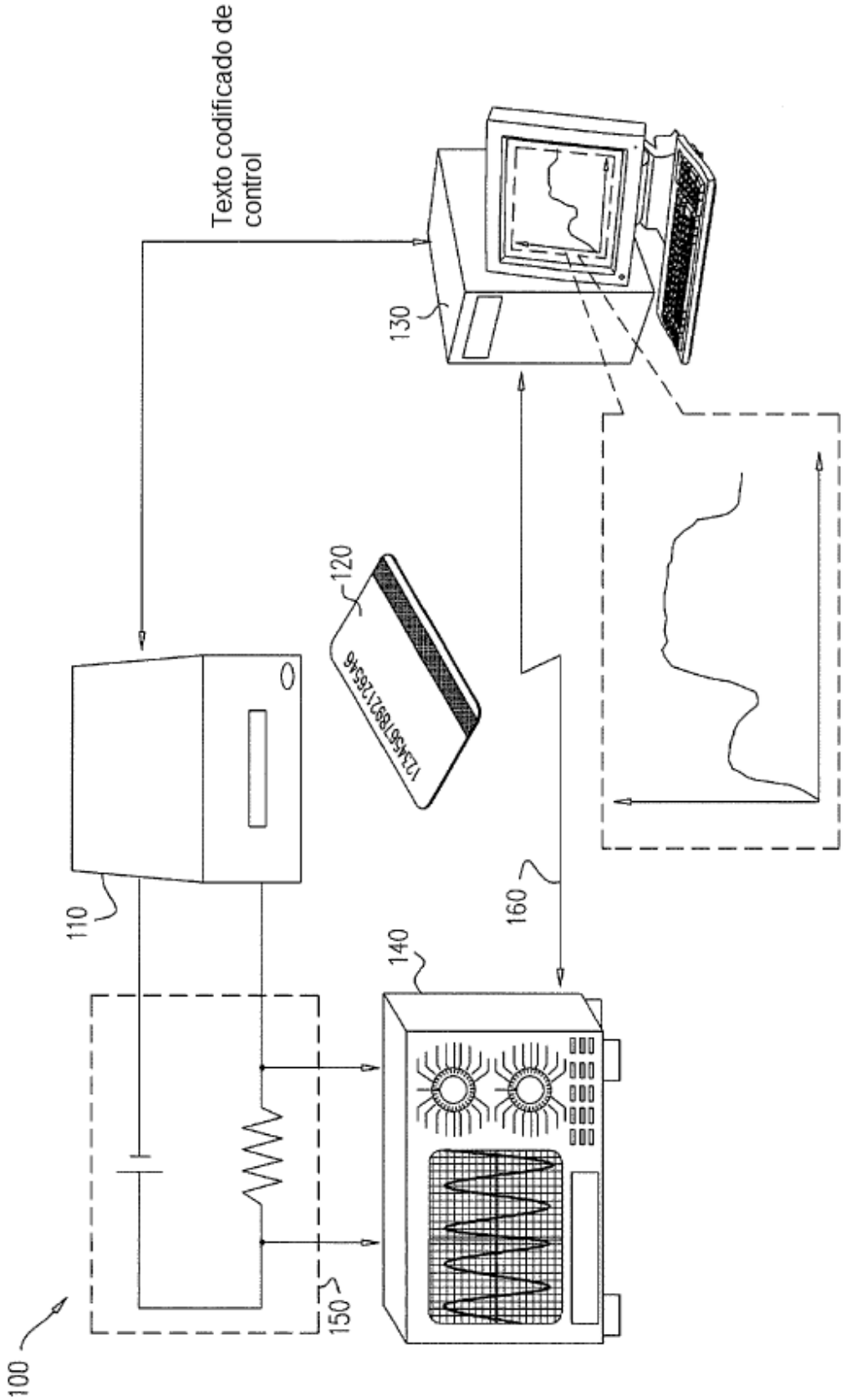

FIG.1

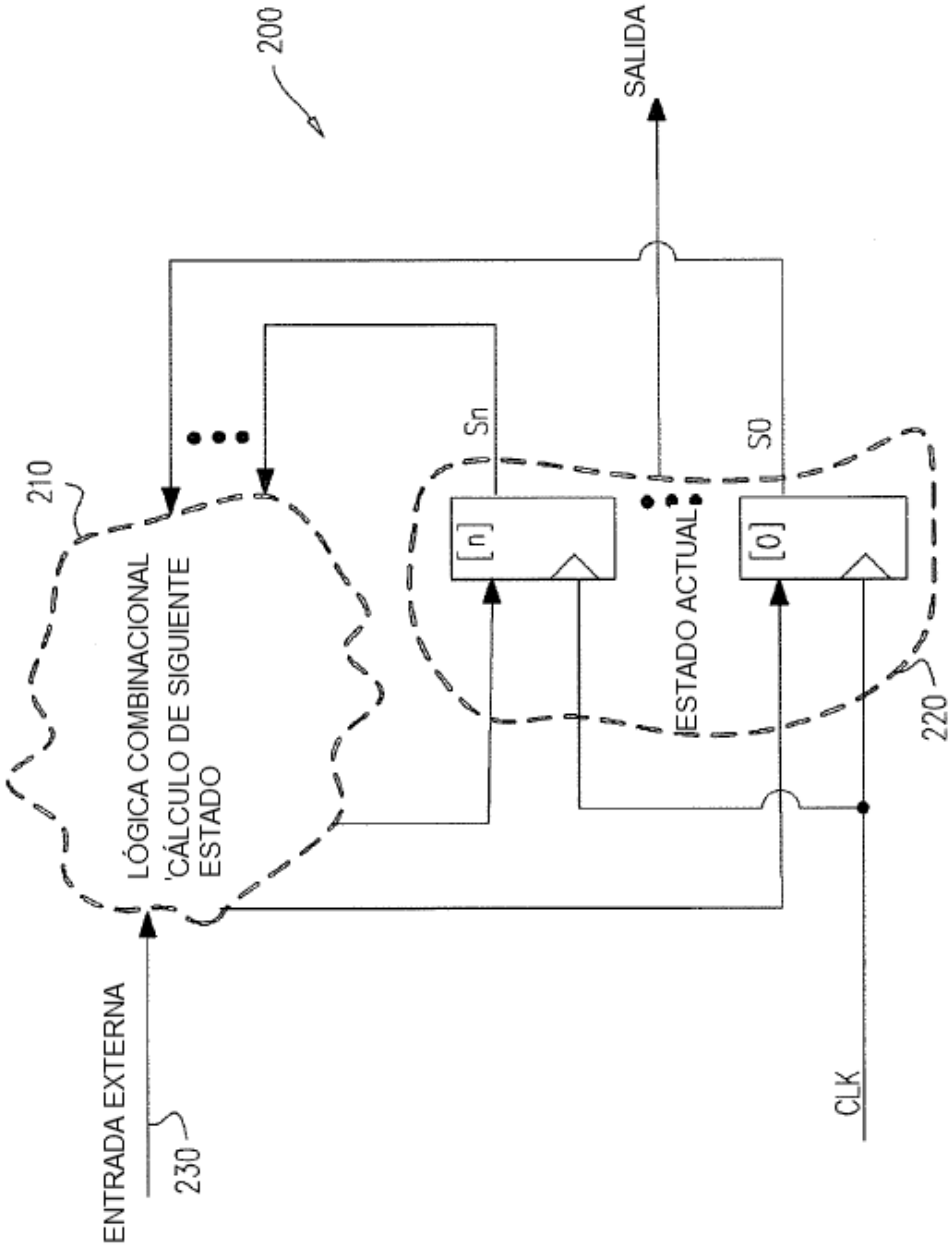
200
SALIDA
210
LÓGICA COMBINACIONAL
'CÁLCULO DE SIGUIENTE
ESTADO
Sn
S0
[n]
[0]
ESTADO ACTUAL
220
ENTRADA EXTERNA
230
CLK

FIG. 2

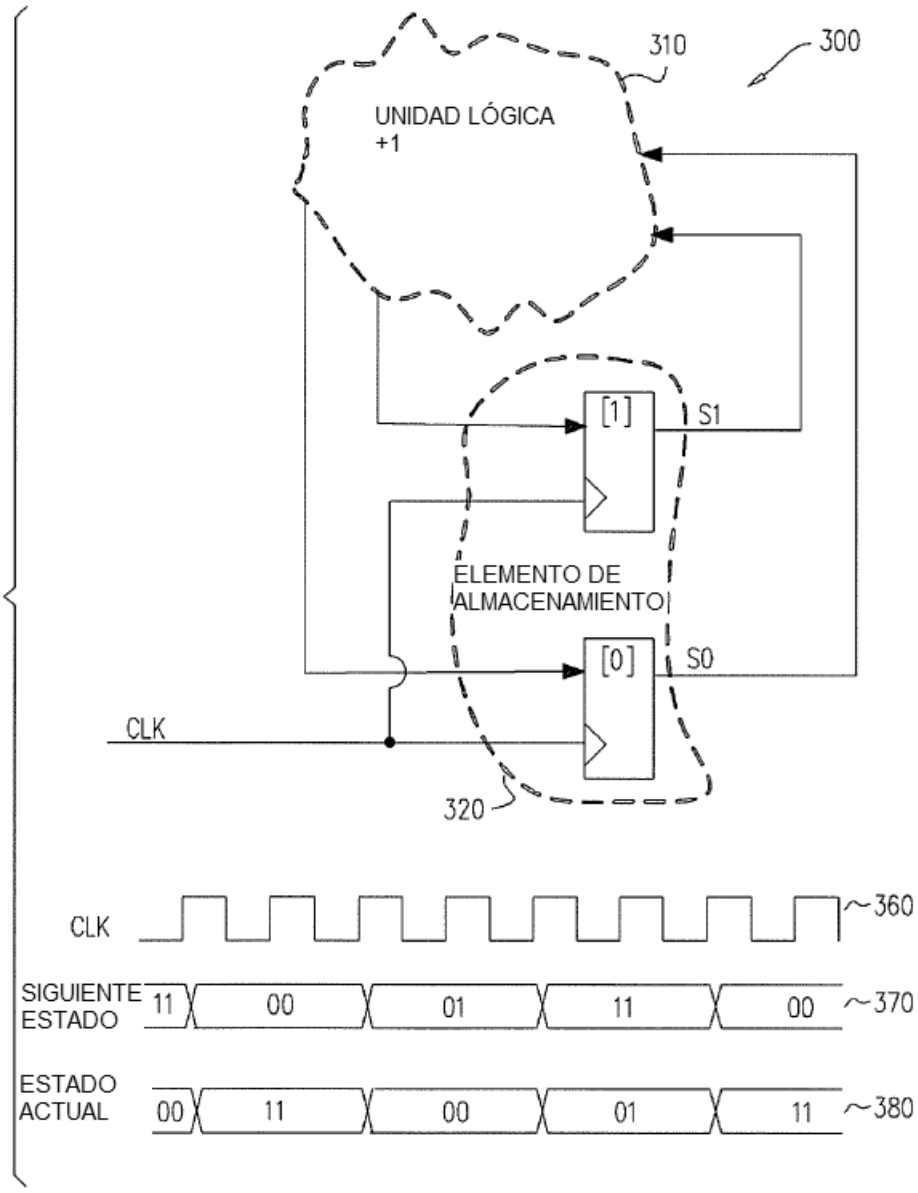
310
300
UNIDAD LÓGICA
+1
[1]
S1
ELEMENTO DE
ALMACENAMIENTO
[0]
S0
CLK
320
CLK
360
SIGUIENTE
ESTADO
11
00
01
11
00
370
ESTADO
ACTUAL
00
11
00
01
11
380

FIG. 3

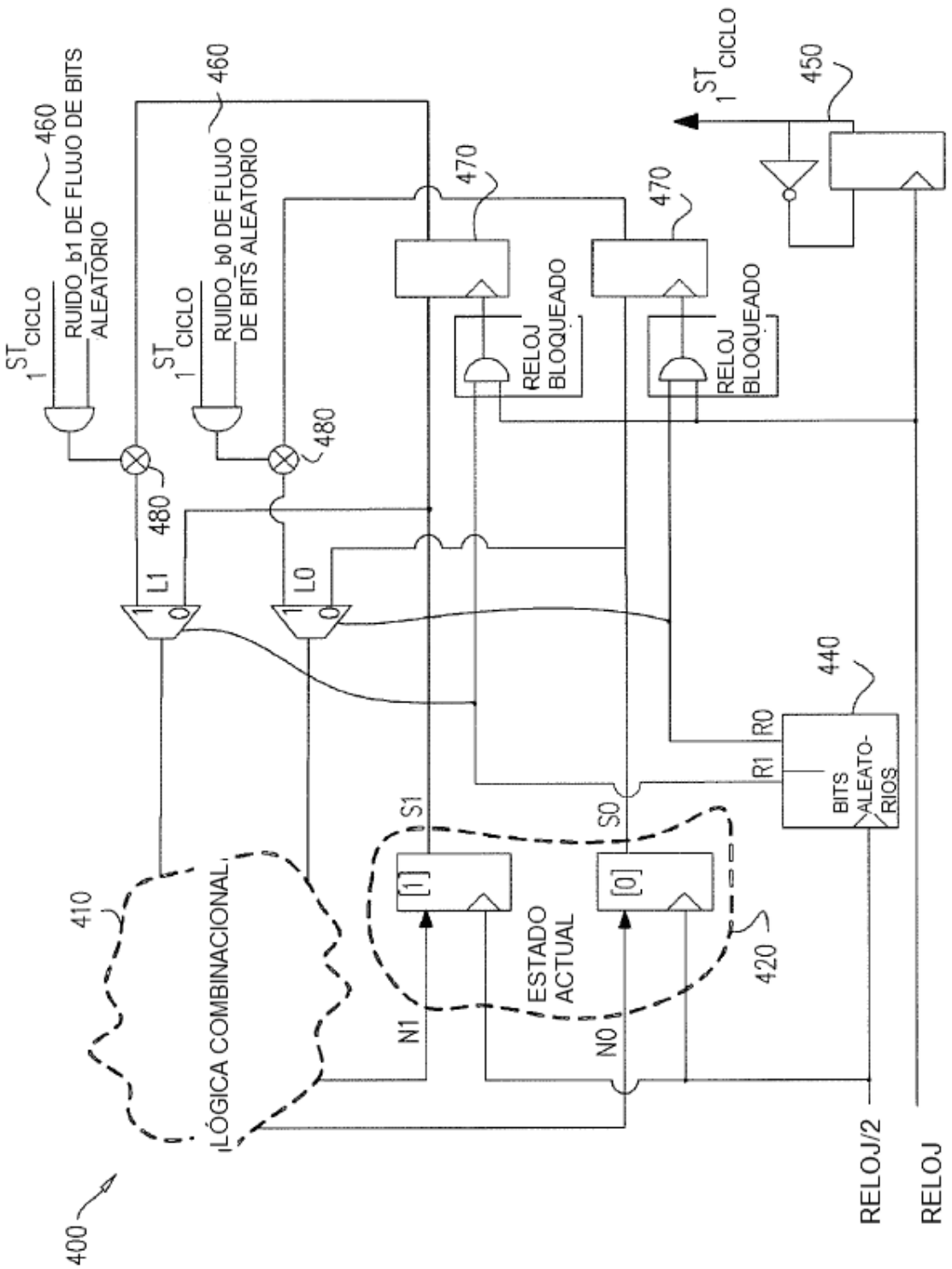
400
410
LÓGICA COMBINACIONAL
420
ESTADO ACTUAL
N1
N0
S1
S0
[1]
[0]
440
BITS ALEATO-RIOS
R0
R1
L1
L0
480
460
RUIDO_b1 DE FLUJO DE BITS ALEATORIO
RUIDO_b0 DE FLUJO DE BITS ALEATORIO
ST 1 CICLO
470
RELOJ BLOQUEADO
450
RELOJ/2
RELOJ

FIG. 4

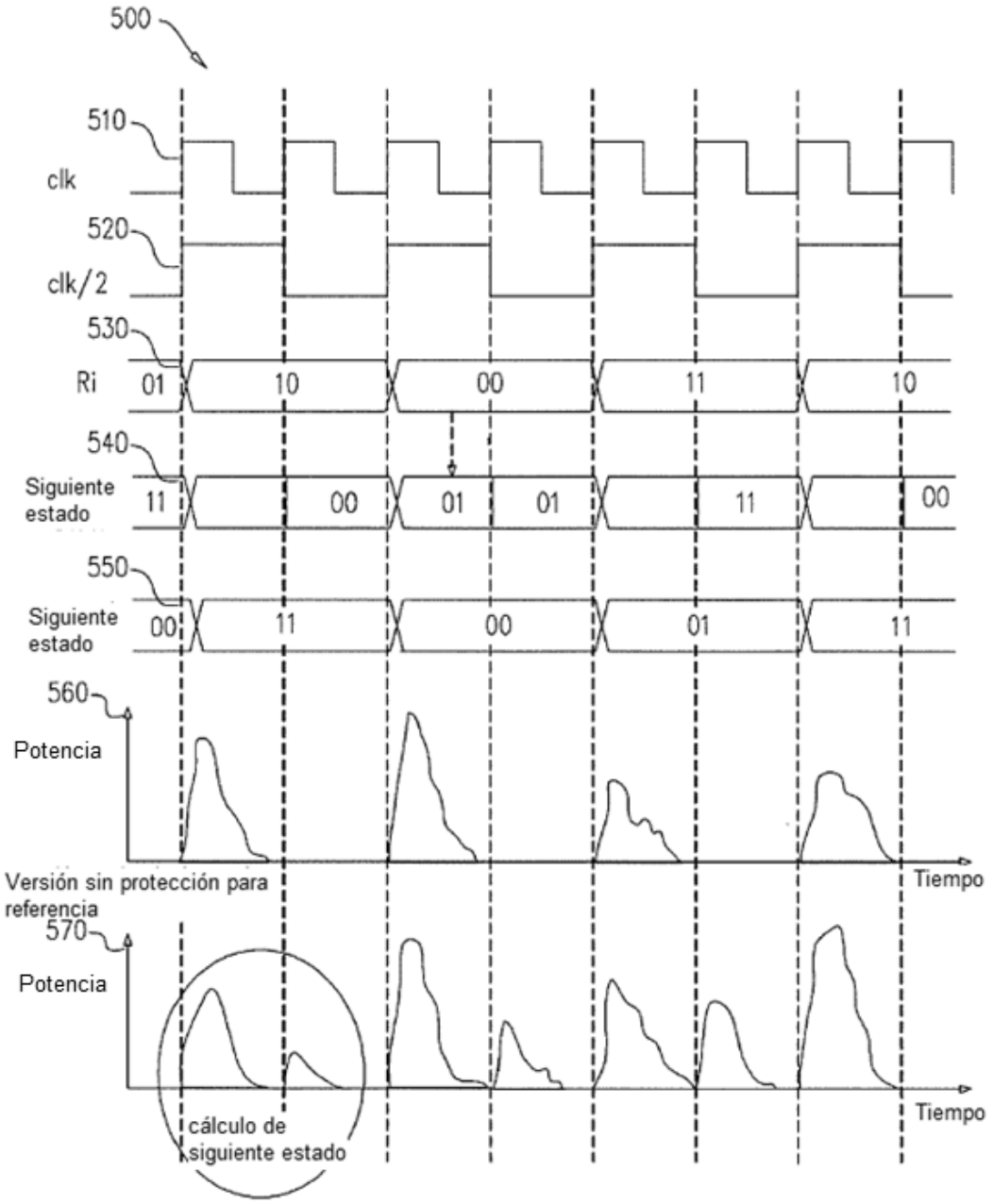
500
510
clk
520
clk/2
530
Ri
01
10
00
11
10
540
Siguiente estado
11
00
01
01
11
00
550
Siguiente estado
00
11
00
01
11
560
Potencia
Tiempo
Versión sin protección para referencia
570
Potencia
Tiempo
cálculo de siguiente estado

FIG. 5

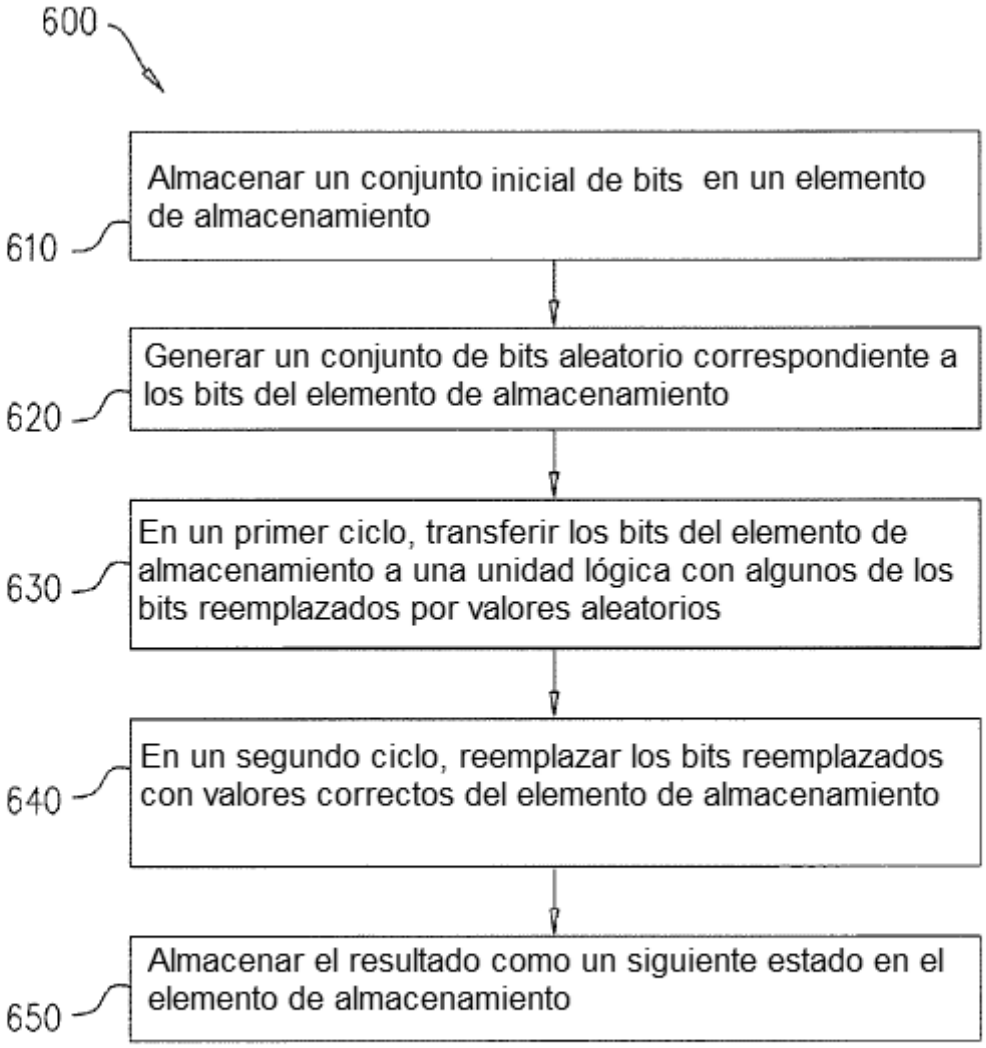
600
Almacenar un conjunto inicial de bits en un elemento de almacenamiento
610
Generar un conjunto de bits aleatorio correspondiente a los bits del elemento de almacenamiento
620
En un primer ciclo, transferir los bits del elemento de almacenamiento a una unidad lógica con algunos de los bits reemplazados por valores aleatorios
630
En un segundo ciclo, reemplazar los bits reemplazados con valores correctos del elemento de almacenamiento
640
Almacenar el resultado como un siguiente estado en el elemento de almacenamiento
650

FIG. 6

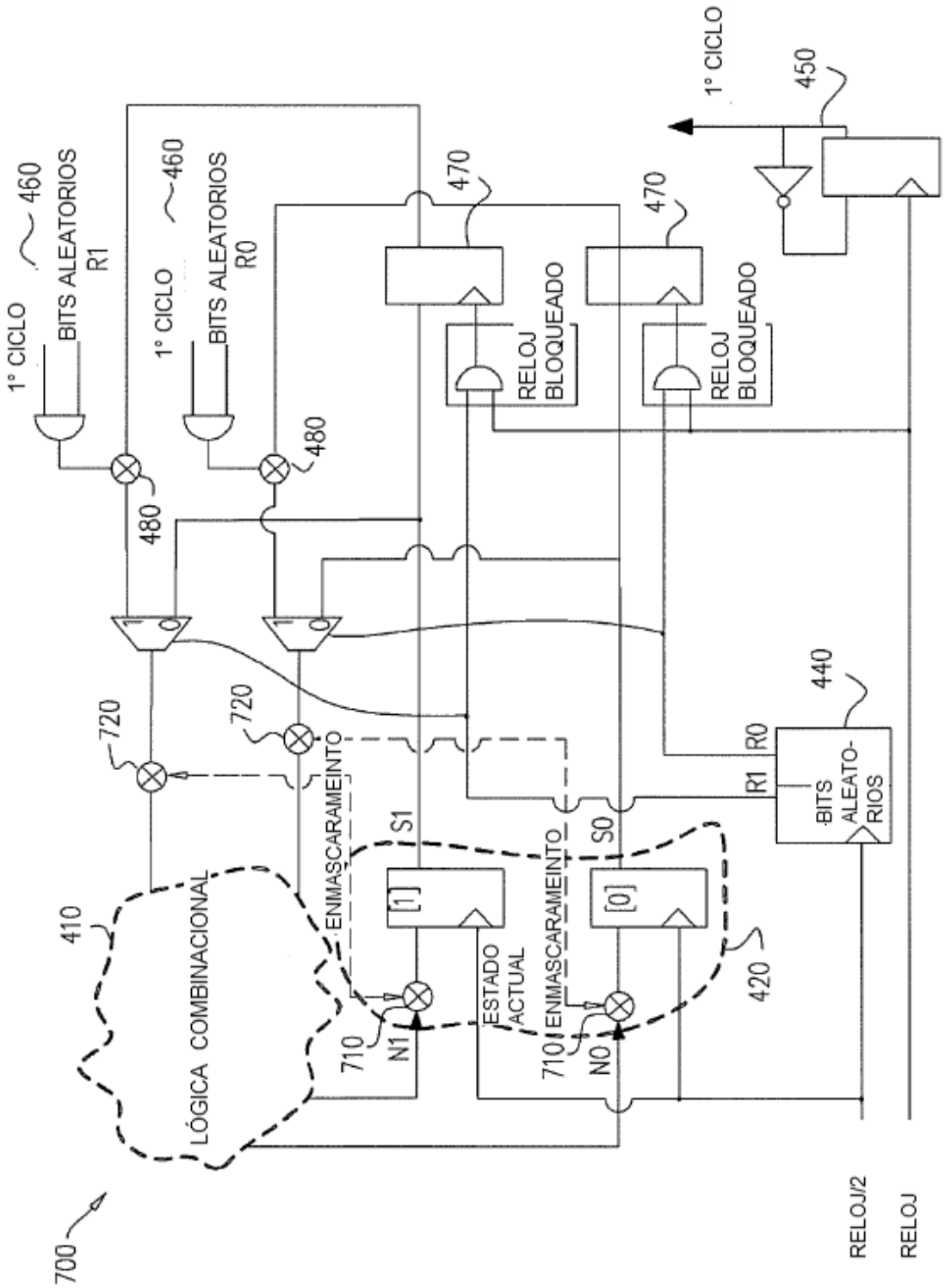
700
410
LÓGICA COMBINACIONAL
720
720
ENMASCARAMEINTO
S1
S0
ENMASCARAMEINTO
[1]
[0]
ESTADO ACTUAL
710
N1
710
N0
420
480
480
1° CICLO
BITS ALEATORIOS R1
460
1° CICLO
BITS ALEATORIOS R0
460
470
470
RELOJ BLOQUEADO
RELOJ BLOQUEADO
1° CICLO
450
440
R0
R1
BITS ALEATO-RIOS
RELOJ/2
RELOJ

FIG. 7

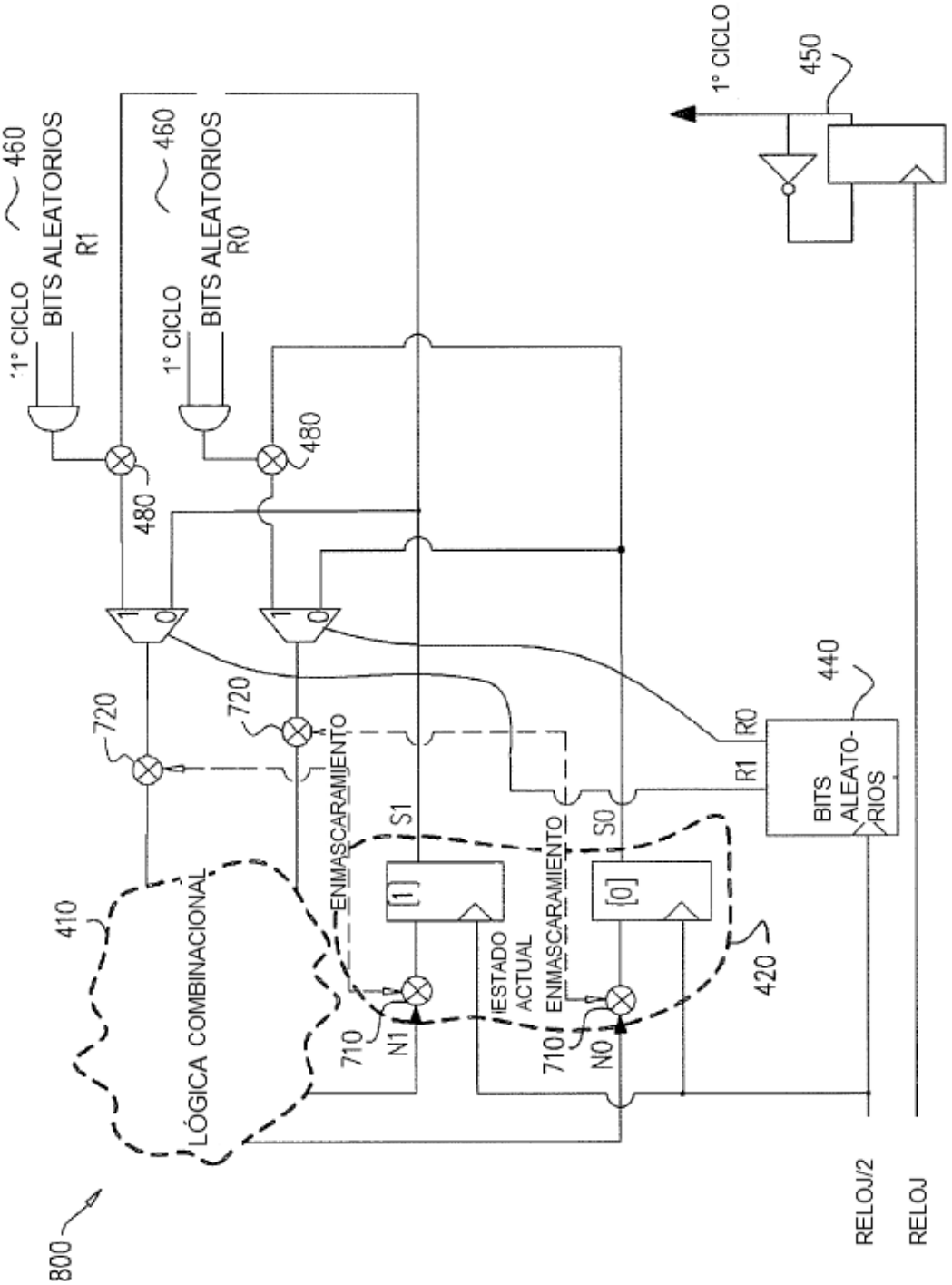
800
410
LÓGICA COMBINACIONAL
460
BITS ALEATORIOS
R1
1° CICLO
460
BITS ALEATORIOS
R0
1° CICLO
480
480
720
720
ENMASCARAMIENTO
S1
S0
ENMASCARAMIENTO
[1]
[0]
ESTADO ACTUAL
710
N1
710
N0
420
1° CICLO
450
440
R0
R1
BITS ALEATO-RIOS
RELOJ/2
RELOJ

FIG. 8