(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 534 403**

(51) Int. CI.:

G06F 7/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.11.2011 E 11785708 (6)**

(97) Fecha y número de publicación de la concesión europea: **07.01.2015 EP 2643750**

(54) Título: **Función física no clonable**

(30) Prioridad:

24.11.2010 EP 10192352

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.04.2015

(73) Titular/es:

INTRINSIC ID B.V. (100.0%)
High Tech Campus 9
5656 AE Eindhoven, NL

(72) Inventor/es:

SIMONS, PETRUS WIJNANDUS y
VAN DER SLUIS, ERIK

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Función física no clonable

Antecedentes de la invención

Las funciones físicas no clonables (PUF) han demostrado ser alternativas ventajosas para muchas formas de identificación segura, incluyendo el almacenamiento de claves, identificadores y similares en las memorias seguras.

Una función física no clonable explota las variaciones de fabricación para derivar un identificador digital. El identificador digital se liga de este modo a un medio físico. Dado que la función física no clonable depende de la variación del proceso aleatorio, es fácil crear una PUF pero es muy difícil, si no totalmente imposible, crear una PUF que diese lugar a un identificador predeterminado específico. Las variaciones de fabricación conducen a diferentes características físicas del elemento de memoria. Por ejemplo, las características físicas pueden incluir: concentraciones de dopaje, espesor de óxido, longitudes de canal, ancho estructural (por ejemplo, de una capa de metal), parasitarias (por ejemplo, resistencia, capacitancia). Cuando un diseño de circuito digital se fabrica múltiples veces, estas características físicas variarán ligeramente y juntas provocarán el comportamiento de un elemento de CI, por ejemplo, un elemento de memoria, se comporta de forma diferente en algunas situaciones. Por ejemplo, el comportamiento de encendido está determinado por las variaciones de fabricación en las características físicas.

Esta propiedad de las PUF las hace adecuadas para una gama de aplicaciones. Por ejemplo, las PUF pueden usarse para combatir la falsificación. Aunque, puede ser posible copiar de manera fraudulenta un dispositivo específico u otro artículo manufacturado, no sería posible duplicar una PUF que pudiese integrarse en el mismo con suficiente precisión de manera que diese lugar al mismo identificador digital como el original. Como un ejemplo adicional, las PUF se usan para crear claves criptográficas. Usando una PUF, se elude la necesidad de una memoria segura para almacenar una clave. Una PUF proporciona además una protección natural contra los intentos ilegales para obtener la clave criptográfica mediante ingeniería inversa, ya que el daño que podría infligirse a la PUF durante el intento cambiaría el identificador digital. Preferentemente, el identificador digital es único para el dispositivo electrónico en el que está integrada la función física no clonable.

Las PUF se han aplicado de manera ventajosa en dispositivos electrónicos. Incluso pequeñas variaciones en la fabricación que son inevitables durante la fabricación de un CI conducen a diferentes propiedades del CI. Estas propiedades diferentes se suprimen normalmente, en un esfuerzo para obtener un lote de CI que funcionen de la misma manera. Sin embargo, para crear una PUF se explotan las diferencias entre los CI individuales en un lote de CI.

Por ejemplo, se ha observado que el comportamiento inicial de algunos elementos de memoria, demuestra un comportamiento similar a una PUF. Cuando se enciende tal memoria, tiende a contener un contenido, es decir, comprender una secuencia de valores de datos, que depende de las características físicas al menos parcialmente aleatorias de los componentes, por ejemplo, puertas o transistores, que componen la memoria, por ejemplo, su disposición física relativa entre sí. Si la memoria se enciende múltiples veces, contendría, hasta un porcentaje grande, el mismo contenido. Desafortunadamente, ya que el comportamiento de la PUF depende de pequeñas fluctuaciones, es inevitable un cierto porcentaje de error. Un procedimiento de corrección de errores, que usan los llamados datos auxiliares, puede usarse para corregir estas fluctuaciones, y asegurarse de que se deriva un identificador digital idéntico cada vez que se usa la PUF.

Por lo tanto, es deseable que el contenido de una memoria, cuando se compara después de múltiples secuencias de encendido y apagado, sea idéntico en una gran parte. Al mismo tiempo es deseable, que cuando el contenido de la memoria se compara con otras memorias del mismo tipo sea diferente en un gran porcentaje.

Se hace referencia al documento "Extended abstract: The butterfly PUF protecting IP on every FPGA" por Kumar, SS; Guajardo, J.; Maes, R.; Schrijen, G.-J.; Tuyls, P, que divulga una PUF de mariposa que comprende unos biestables de acoplamiento cruzado.

Sumario de la invención

Se proporciona una función física no clonable, que comprende una pluralidad de bus keepers, estando cada bus keeper de la pluralidad de bus keepers configurado para asentarse en uno de al menos dos estados estables diferentes tras el encendido, siendo el estado estable específico en el que se asienta un bus keeper específico de la pluralidad de bus keepers dependiente al menos en parte de las características físicas al menos parcialmente aleatorias del bus keeper específico, y un circuito de lectura para leer la pluralidad de estados estables en los que se asienta la pluralidad de bus keepers después de un encendido, siendo la pluralidad bus keepers de solo lectura.

Teniendo el bus keeper de solo lectura, es decir, solo se puede leer un valor de los mismos, no un nuevo valor, puede omitirse escribir la lógica de escritura. Esto hace más pequeño el número de puertas, y el diseño más barato. Una ventaja importante es que puede usarse un dominio de alimentación.

En una realización, el circuito de lectura comprende una pluralidad de multiplexores para seleccionar los bus keepers de la pluralidad de bus keepers.

Usar multiplexores para seleccionar los bus keepers de la pluralidad de bus keepers tiene la ventaja de que no es necesario ningún decodificador de dirección para seleccionar los bus keepers. Esto tiene la ventaja de que la pluralidad de bus keepers es más pequeña en tamaño en un circuito integrado y en requisitos de energía que lo que sería una memoria comparable.

Un multiplexor o MUX es un componente electrónico que realiza la multiplexación; éste selecciona una de una pluralidad de señales digitales de entrada y remite la entrada seleccionada a una sola línea. Un multiplexor de n entradas puede tener log_2 (n) líneas de selección, que se usan para seleccionar qué línea de entrada enviar a la salida. En una realización de la invención se usan los multiplexores que tienen dos entradas y una línea de selección.

En una realización, la función física no clonable comprende una fuente de alimentación y un dominio de alimentación, estando la pluralidad de bus keepers comprendida en el dominio de alimentación y estando al menos una parte de la función física no clonable fuera del dominio de alimentación, estando el dominio de alimentación configurado para conectar y desconectar de manera selectiva la pluralidad de bus keepers de la fuente de alimentación mientras que al menos una parte de la función física no clonable está conectada a la fuente de alimentación.

A pesar de que son muy pequeños los requisitos de alimentación de un bus keeper, todavía hay varias ventajas conectadas para tener un dominio de alimentación.

Debido a que los bus keepers se seleccionan usando multiplexores, puede separarse el circuito de lectura de los bus keepers. Esto permite que el dominio de alimentación sea más pequeño. Como resultado puede usarse un pequeño conmutador para el dominio de alimentación.

Debido al dominio de alimentación, la pluralidad de bus keepers solo necesita alimentarse durante la lectura de los bus keepers. Se ha descubierto que esto reduce el efecto de envejecimiento problemático que puede ocurrir en las PUF basado en la lógica CMOS.

Por otra parte, el tener un dominio de alimentación permite al circuito de lectura leer los bus keepers más de una vez realizando múltiples ciclos de encendido, lectura, apagado de la pluralidad de bus keepers. En una realización, el circuito de lectura está configurado para múltiples ciclos de encendido, lectura, apagado de la pluralidad de bus keepers. Procesando la múltiple pluralidad de lecturas de estados estables puede reducirse el ruido. Por ejemplo, puede promediarse y redondearse la múltiple pluralidad de lecturas de estados estables.

Por ejemplo, después de cada lectura de la pluralidad de bus keepers, la pluralidad de estados estables puede convertirse en una matriz de valores de bits. Leyendo múltiples veces se obtienen múltiples matrices de valores de bits. Las múltiples matrices se suman, añadiendo los componentes correspondientes juntos, para obtener una matriz sumada. Cada componente de la matriz sumada se divide por el número de lecturas. Finalmente, cada uno de los componentes se redondea a 0 o 1. Si se obtiene un valor de 0,5 puede redondearse a 1, o puede reemplazarse por una elección aleatoria de 0 o 1. La matriz promediada ha reducido el ruido, y pueden usarse para derivar un identificador. La matriz promediada es menos adecuada para derivar un número aleatorio.

Por ejemplo, la al menos una parte de la función física no clonable que está fuera del dominio de alimentación puede comprender el circuito de lectura o parte del mismo, o la lógica de control de la PUF, etc.

En una realización, la pluralidad de bus keepers, el dominio de alimentación, el conmutador de encendido, y la al menos una parte de la función física no clonable se implementan en un único circuito integrado.

Tener el conmutador de alimentación en el chip es posible debido a que el conmutador de alimentación puede ser más pequeño debido a los pequeños requerimientos de energía de los bus keepers.

La función física no clonable puede proporcionarse en un dispositivo electrónico, en particular en un dispositivo electrónico móvil tal como un teléfono móvil, un decodificador, un ordenador, una tarjeta inteligente, una etiqueta RFID.

La función física no clonable puede usarse para derivar un identificador. El identificador puede usarse como una clave criptográfica, o como un valor inicial para derivar una clave criptográfica.

En una realización, al menos un bus keeper en la pluralidad de bus keepers 110 no está configurado con medios para escribir de forma selectiva un valor en el bus keeper. Preferentemente, ninguno de los bus keepers en la pluralidad de bus keepers está provisto de medios para escribir de forma selectiva un valor en el bus keeper.

En una realización, la función física no clonable comprende la lógica de control PUF para derivar un identificador de la pluralidad de estados estables.

En una realización, la lógica de control PUF está configurada para aplicar un algoritmo de corrección de errores a la pluralidad de estados estables y a los datos auxiliares para derivar el identificador.

Existen muchos métodos para aplicar un código de corrección de errores a los datos PUF. Por ejemplo, durante una fase de inscripción, una matriz de valores que representa la pluralidad de estados estables puede hacer una operación lógica XOR con una palabra de código de un código de corrección de errores. El resultado, la diferencia XOR, se puede almacenar en una memoria. Durante una fase de uso, se obtiene una nueva lectura de la pluralidad de estados estables, se hace una operación lógica XOR a una matriz de valores que representa la nueva pluralidad de estados estables con la diferencia XOR almacenada. El resultado se somete a un algoritmo de corrección de errores asociado con el código de corrección de errores. El resultado es la palabra de código original. Si se desea se puede hacer una operación lógica XOR a la palabra de código original con la diferencia XOR almacenada para obtener la respuesta de inscripción.

En una realización, la lógica de control PUF está configurada para derivar un número aleatorio de la pluralidad de estados estables.

El número aleatorio puede obtenerse aplicando una función hash, por ejemplo, la sha-256, a la pluralidad de estados estables, o a una matriz de valores que representan la pluralidad de estados estables.

El número aleatorio puede usarse como un valor inicial en un pseudo generador de números aleatorios. En una realización, la pluralidad de valores estables se usa de dos maneras: se usa la pluralidad de valores estables para derivar un identificador para obtener un identificador. Para este fin, no es deseable el ruido en los bus keepers; Puede usarse la misma pluralidad de valores estables sin corrección de errores para obtener un número aleatorio, en este caso el ruido es deseable.

Derivar un número aleatorio de la pluralidad de estados estables es especialmente ventajoso si la PUF tiene un dominio de alimentación conmutable. El dominio de alimentación conmutable permite a la pluralidad de bus keepers iniciarse de nuevo, por ejemplo, apagarse y encenderse, sin interrumpir la alimentación a la lógica de control PUF. De esta forma, puede derivarse un número aleatorio múltiple de alta calidad. Esa es una secuencia de un número aleatorio que puede derivarse sin la necesidad de usar un pseudo generador de números aleatorios. Los verdaderos números aleatorios son especialmente útiles cuando se usan en un protocolo criptográfico, ya que le dan una mayor seguridad. Por ejemplo, cuando se usa en un protocolo de desafío-respuesta. El desafío o la pluralidad de desafíos puede comprender, respectivamente, un número aleatorio generado a partir de datos PUF o una pluralidad de números aleatorios generados a partir de datos PUF.

En una realización, la lógica de control PUF está configurada para un ciclo de lectura que comprende: apagar la pluralidad de bus keepers, encender la pluralidad de bus keepers, y leer la pluralidad de bus keepers.

El apagado y el encendido usan el conmutador de encendido. El ciclo de lectura puede realizarse una vez. Sin embargo, el ciclo de lectura también puede realizarse múltiples veces, dichas 2 veces, 3 veces, o más.

En una realización, al menos un bus keeper comprende exactamente una conexión de datos, y en el que la exactamente una conexión de datos está configurada solamente para leer el estado estable en el que el al menos un bus keeper se asienta tras el encendido.

Preferentemente, todos los bus keepers de la pluralidad de bus keepers comprenden exactamente una conexión de datos, y en el que la exactamente una conexión de datos está configurada solamente para leer el estado estable en el que el al menos un bus keeper se asienta tras el encendido. Puede implementarse un método de acuerdo con la invención en un ordenador como un método implementado por ordenador, o en un hardware dedicado, o en una combinación de ambos. El código ejecutable por un método de acuerdo con la invención puede almacenarse en un producto de programa informático. Ejemplos de productos de programas de ordenador incluyen dispositivos de memoria, dispositivos de almacenamiento ópticos, circuitos integrados, servidores, software en línea, etc.

En una realización preferida, el programa informático comprende medios de código de programa informático adaptados para realizar todas las etapas de un método de acuerdo con la invención cuando el programa informático se ejecuta en un ordenador. Preferentemente, el programa informático se incorpora en un medio legible por ordenador.

Breve descripción de los dibujos

La invención se explica con más detalle a modo de ejemplo y con referencia a los dibujos adjuntos, en los que:

La figura 1 es un diagrama de bloques que ilustra una realización de un sistema PUF,
La figura 2 es un diagrama de bloques que ilustra una variación opcional en el sistema PUF de la figura 1,
La figura 3a es un diagrama de bloques que ilustra un primer tipo de bus keeper,
La figura 3b es un diagrama de bloques que ilustra un segundo tipo de bus keeper,
La figura 4 es un diagrama de bloques que ilustra una realización de un sistema PUF,
La figura 5 es un diagrama de bloques que ilustra un circuito de lectura para su uso en un sistema PUF,
La figura 6 es un diagrama de bloques que ilustra un dominio de alimentación para su uso en un sistema PUF,
La figura 7 es un diagrama de bloques que ilustra un dominio de alimentación para su uso en un sistema PUF,
La figura 8 es un diagrama de bloques que ilustra un circuito de lectura para su uso en un sistema PUF,
La figura 9 es una figura de la técnica anterior que ilustra el uso convencional de un bus keeper.

En todas las figuras, las características similares o correspondientes están indicadas por los mismos números de referencia.

Lista de números de referencia:

100	un sistema PUF
110	una pluralidad de bus keepers
112, 114, 116, 118	un bus keeper
120	un circuito de lectura
130	una lógica de control PUF
140	una memoria no volátil
150	un circuito usando los datos PUF procesados
160	un comparador
165	una memoria no volátil
300	un bus keeper
310	un primer inversor
320	un segundo inversor
330	una salida
340	una resistencia
350	un bus keeper
400	un sistema de lectura PUF
410	un dominio de alimentación conmutable
420	un circuito de aislamiento
430	un circuito de lectura
500	un sistema de lectura PUF
510, 520, 530	un MUX
612, 614, 616, 618	una puerta AND
700	un sistema de lectura PUF
710, 720	una puerta AND
812, 814, 816, 818	un flip-flop
822, 824, 826	un MUX

Realizaciones detalladas

Aunque esta invención es susceptible de realizarse de muchas formas diferentes, se muestra en los dibujos y se describirá en detalle en el presente documento una o más realizaciones específicas, con el conocimiento de que la presente descripción ha de considerarse como un ejemplo de los principios de la invención y no pretende limitar la invención a las realizaciones específicas mostradas y descritas.

Bus keepers

Los inventores han tenido la idea de que puede usarse un bucle de acoplamiento cruzado de dos inversores como una fuente de datos PUF. Un bucle de acoplamiento cruzado de dos inversores también se conoce en la técnica como un bus keeper.

La figura 3a muestra un primer tipo de bus keeper 300, que puede usarse en la invención.

La figura 3a muestra un bucle de acoplamiento cruzado de un primer inversor 310 y un segundo inversor 320. Una salida del primer inversor 310 está conectada a una entrada del segundo inversor 320, y una entrada del primer inversor 310 está conectada a una salida de segundo inversor 320. El bus keeper tiene una sola conexión de datos a partir de la que puede leerse el contenido del bus keeper: salida 330.

La figura 3b muestra un segundo tipo de bus keeper 350. La figura 3b es la misma que la figura 3a excepto por la incorporación de una resistencia entre la salida del inversor 310 y la entrada del inversor 320.

Convencionalmente, un bus keeper (también conocido como un bus holder) es un circuito biestable débil, usado para mantener el último valor en un bus de tres estados. A continuación, el circuito se usa básicamente como un elemento de retardo con la salida conectada de vuelta a la entrada a través de una impedancia relativamente alta. Esto se logra normalmente con dos inversores conectados espalda contra espalda. Los bus holders se usan para evitar que las entradas de la puerta CMOS consigan valores flotantes cuando están conectadas a redes de tres estados. De lo contrario, tanto los transistores P como los N en la puerta podrían excitarse, cortocircuitando de este modo la fuente de alimentación y la tierra, lo que destruiría la puerta CMOS o provocaría una alta corriente de fuga. Esto se evita mediante el bus holder que arrastra la entrada al último nivel lógico válido (0 o 1) en la red. El circuito se coloca normalmente en paralelo con la red de tres estados.

Opcionalmente, un bus keeper comprende una resistencia, excitando la resistencia el bus débilmente; por lo tanto, otros circuitos pueden ignorar el valor del bus cuando no están en modo de tres estados. Se puede prescindir de la resistencia, aunque algunos diseños de bus keeper pueden incluir una, por ejemplo, para reducir los flujos máximos.

Si la resistencia, por ejemplo, la resistencia 340, en el diseño es del orden de unos pocos kilo-ohmios, el bus keeper puede mostrar una polarización para un valor de inicio específico; siendo un inversor más débil que el otro debido a la resistencia. Incluso unos pocos ohmios pueden dar lugar a una polarización medible pero su influencia será mucho menor. Un bus keeper también puede comprender un inversor que excita más débil que el otro; esta opción no necesita una resistencia. Tener un inversor débil también puede proporcionar alguna polarización, pero también trabajará bien.

Puede fabricarse un bus keeper sin resistencia usando inversores de celdas convencionales. Para la PUF, esto tiene las mismas ventajas sin el riesgo de que la resistencia en serie provoque una polarización.

Idealmente, un bus keeper usado en una PUF tendrá un valor de inicio que es 1 o 0 con un 50 % de probabilidad dado su diseño, pero que repetirá su valor de inicio específico cada vez que se encienda. Si los bus keepers tienen una probabilidad mayor o menor de 50 % de ser 1 o 0, tienen una polarización o de 0 o de 1.

Se prefiere que ambos inversores estén diseñados para ser de igual fuerza en la excitación de la salida. Esto proporciona las mejores posibilidades de obtener un bus keeper con baja polarización, y por lo tanto de alta entropía.

Sin embargo, se observa que un bus keeper que tiene un diseño en polarización, por ejemplo, teniendo una baja polarización debido a un inversor más débil o una resistencia pequeña, o teniendo una polarización más grande debido a una resistencia más grande, también es útil como datos PUF. Sin embargo, si la polarización es alta, es decir, la entropía es baja, entonces se usan preferentemente las medidas que mejoran la entropía.

La polarización específica del bus keeper de un estado de inicio depende del diseño del bus keeper y cómo se ha fabricado. El valor de inicio de un bus keeper es susceptible al ruido y a las perturbaciones.

Es ventajoso ser capaz de usar bus keepers a pesar de que puedan tener una ligera polarización o incluso una polarización fuerte, ya que esto permite crear el sistema PUF a partir de componentes convencionales, es decir, usando bus keepers a partir de un estudio de celdas convencional.

La figura 9 muestra un uso convencional de un bus keeper. La figura 9 muestra dos registros: el registro A y B, siendo cada uno n+1 bits de ancho. Los registros están conectados ambos a un bus paralelo, que es n+1 bits de ancho. Cada bit de un registro está conectado a una línea asociada del bus paralelo a través de una memoria intermedia de tres estados. La figura 9 muestra cómo 2 bits de cada registro están conectados a dos líneas correspondientes del bus, a través de elementos de memoria intermedia. Cada línea del bus está conectada a un bus keeper. La figura 9 muestra dos bus keepers 910 y 920 cada uno conectado a una línea de bus. El efecto de los bus keepers es que evitan que el bus flote. El último valor puesto en el bus se mantiene por el bus keeper.

En lugar de los registros, otros bloques funcionales pueden ser la fuente de datos (por ejemplo las ALU, los núcleos de CPU, etc.). En este ejemplo, la señal de habilitación para el excitador de bus se activa baja (nEN_A), ésta podría activarse alta.

Se sabe que una celda SRAM también comprende un bucle de acoplamiento cruzado de dos inversores. Sin embargo, una celda SRAM también comprende dos transistores de acceso adicionales que sirven para controlar el acceso a una celda de almacenamiento durante las operaciones de lectura y escritura, respectivamente. Estos transistores de acceso no son necesarios en un bus keeper cuando se usa en la invención. Especialmente, se prescinde totalmente del control de las operaciones de escritura. La SRAM tiene múltiples bits de datos cada uno conectado a través de su propio transistor de lectura en un hilo; esto es similar a la figura 9, en la que las memorias intermedias de tres estados se sustituyen por un transistor de lectura, y en la que se elimina el bus keeper.

El bus keeper está configurado para asentarse en uno de al menos dos estados estables diferentes tras el encendido, siendo el estado estable específico en el que se asienta el bus keeper dependiente, al menos en parte, de las características físicas al menos parcialmente aleatorias del bus keeper. El valor de inicio de un bus keeper se

usa como datos PUF.

Una ventaja de usar bus keepers es que extraen poca corriente. Cuando los bus keepers se colocan en un dominio de alimentación conmutable separado, el conmutador de alimentación de este dominio puede ser más pequeño de lo que sería necesario para, por ejemplo, un memoria o un flip-flop basado en PUF. Esto abre la posibilidad de implementar el conmutador de alimentación en el chip, al tiempo que se limita el coste adicional en la superficie. Cuando se usa una memoria el consumo de energía es significativamente mayor durante la lectura, ya que toda la lógica de decodificación de memoria estaría incluida también en el dominio de alimentación. Los flip-flop tienen más lógica por sí mismos y por lo tanto también consumen más energía; esto necesitaría de conmutadores más grandes para mantener la tensión de alimentación dentro del intervalo de funcionamiento. El conmutador tiene una resistencia interna, lo que significa que a más corriente más caída de tensión; para compensar esto la resistencia debe disminuirse lo que puede hacerse aumentando el tamaño del conmutador.

Figura 1

La figura 1 ilustra de manera esquemática un sistema PUF 100 a modo de ejemplo.

El sistema PUF 100 comprende una pluralidad de bus keepers 110. La pluralidad de bus keepers puede disponerse de manera adecuada en un circuito integrado, por ejemplo, dispuesta como una matriz.

La figura 1 muestra dos bus keepers en la pluralidad de bus keepers 110: un primer bus keeper 112 y un segundo bus keeper 114. Sin embargo, esto es solo un ejemplo, normalmente el número de bus keepers usados será considerablemente más alto. Por ejemplo, el número de bus keepers puede ser 1024 o 4096. El número de bus keepers puede ser más bajo que 1024. El número de bus keepers puede ser más alto que 1024. El número de bus keepers a usar depende de un número de factores, que incluyen los siguientes: El número deseado de bits en un identificador que depende de la pluralidad de bus keepers 110; cuanto mayor sea el número deseado de bits se necesitan más bus keepers. La tasa de error de un bus keeper en la tecnología elegida, es decir, cuán probable es que un bus keeper cambie su valor de inicio específico, es decir, un bit de inicio, en un inicio posterior; cuanto mayor sea la tasa de error más corrección de errores se necesita y más bus keepers se necesitan.

La entropía en los bus keepers, es decir, cuán probable es el valor de inicio de un bus keeper diferente del valor de inicio de un bus keeper diferente; cuanto menor es la entropía más bus keepers se necesitan.

Un bus keeper solo tiene una conexión de datos. La conexión de datos se usa en la invención para leer el valor de inicio. Aparte de la conexión de datos, el bus keeper estará conectado a una fuente de alimentación, usando una conexión Vss y Vdd. Un tipo de bus keeper que puede usarse para la invención tiene exactamente tres conexiones externas: una conexión de datos y dos conexiones de alimentación (Vss y Vdd).

Un sistema PUF 100 comprende además un circuito de lectura 120 para leer el contenido de la pluralidad de bus keepers 110. El contenido de cada uno de los bus keepers en la pluralidad de bus keepers 110 se determina únicamente por su comportamiento de inicio. El sistema PUF 100 y, en particular, ni el circuito de lectura 120 ni la pluralidad de bus keepers 110 ni ningún bus keeper de los mismos tienen capacidad de escritura que permitiría a uno escribir los datos seleccionados a un bus keeper en la pluralidad de bus keepers 110. Omitir la escritura lógica hace que las celdas en la pluralidad de bus keepers 110 sean más pequeñas. La pluralidad de bus keepers no puede usarse como una memoria escribible sin la incorporación de lógica adicional, pero esto no es necesario para una PUF, de hecho puede considerarse como una ventaja de seguridad; es imposible escribir una cadena predeterminada en la memoria con el objetivo de engañar a la lógica posterior.

Como consecuencia no se pueden escribir datos anti-envejecimiento en un bus keeper, sin embargo, el uso de un dominio de alimentación que comprende la pluralidad de bus keepers mitiga este problema.

El circuito de lectura 120 comprende preferentemente una pluralidad de MUX, estando la pluralidad de MUX dispuesta para recibir una pluralidad de señales de selección para seleccionar uno específico de la pluralidad de bus keepers.

El sistema PUF 100 comprende una lógica de control 130. La lógica de control 130 PUF puede implementarse en hardware en el circuito integrado. La lógica de control 130 PUF puede comprender un procesador de datos, por ejemplo, una CPU, para ejecutar un programa de software para obtener la funcionalidad de la lógica de control 130 PUF.

El sistema PUF 100 comprende además una memoria 140. La memoria 140 es no volátil, la memoria se puede escribir tal como una memoria flash, una memoria EPROM, una EEPROM, etc. La memoria 140 almacena datos auxiliares obtenidos anteriormente para esta instanciación específica de la pluralidad de bus keepers 110.

La lógica de control 130 PUF está configurada para recibir los datos PUF leídos por el circuito de lectura 120 de la pluralidad de bus keepers 110 y para recibir datos auxiliares desde la memoria 140. Usando un algoritmo de datos

auxiliares, también conocido como un extractor difuso, por ejemplo, ejecutado en la lógica de control 130 PUF, los datos obtenidos, por ejemplo, de la pluralidad de bus keepers 110 se procesan usando los datos auxiliares. Como resultado de este procesamiento, se elimina la variación que puede presentarse en los datos PUF.

Una forma de usar una PUF para crear una clave criptográfica es de la siguiente manera. En primer lugar, durante una fase de inscripción, se leen los valores de inicio de la pluralidad de bus keepers 110, por ejemplo usando el circuito de lectura 120. A continuación, usando el extractor difuso, también conocido como una función de protección, se crean los datos auxiliares, véase, por ejemplo, el documento WO/2004/066296. En el dispositivo, los datos auxiliares se almacenan en la memoria 140. Durante una fase de uso, se obtiene una nueva respuesta evaluando la PUF de nuevo. La nueva respuesta puede diferir de la respuesta obtenida durante la fase de inscripción. Preferentemente, la nueva respuesta difiere un poco de la respuesta, de modo que se necesita poca corrección de errores. Se necesita que la nueva respuesta coincida con la respuesta al menos por un porcentaje de los valores de inicio, el valor que depende de, por ejemplo la corrección de errores. El porcentaje es más de un 50 %.

Combinando la nueva respuesta con los datos auxiliares almacenados, de acuerdo con un algoritmo de datos auxiliares, se obtiene una respuesta corregida. Los datos auxiliares garantizan que la respuesta corregida sea la misma, cada vez que se derive.

No se necesita la memoria 140; los datos auxiliares pueden almacenarse fuera de línea, recibiendo la lógica de control 130 PUF los datos auxiliares desde una fuente externa a la lógica de control 130 PUF cuando se necesiten.

Después de la corrección de la perturbación en la respuesta, la respuesta puede usarse para diversos fines. Como ejemplo, el sistema PUF 100 comprende un circuito de cifrado 150 para usar la respuesta con fines criptográficos.

Un ejemplo de aplicación de la respuesta corregida incluye aplicar un algoritmo de derivación (KDF) a la respuesta corregida para obtener una clave criptográfica. Ejemplos de tales funciones de derivación de claves incluyen el KDF1, definido en la norma IEEE Std 1363-2000, y las funciones similares en la norma ANSI X9.42.

Un ejemplo de aplicación de la respuesta corregida incluye usar la respuesta o clave corregida en un algoritmo de autenticación.

La invención también puede usarse sin corrección de errores, es decir, sin la lógica de control 130 PUF, la memoria 140 y el circuito 150. Se muestra un ejemplo en la figura 2. La figura 2 es la misma que la figura 1 pero sin la lógica de control 130 PUF, la memoria 140 y el circuito 150. Una respuesta obtenida durante la inscripción se almacena en la memoria 165 no volátil. Durante su uso, el comparador 160 recibe una respuesta del circuito de lectura 120 y la compara con la respuesta almacenada, almacenada en la memoria 165. Si el número de diferencias entre las dos respuestas (es decir, representadas como cadenas de valores de bit) es menor que un límite predeterminado, la PUF se considera como auténtica.

En lugar de la respuesta corregida, el proceso de corrección de errores puede producir otros identificadores que dependen de la variación en las características físicas pero que son correctos por ser idénticos tras cada inicio. En particular, puede establecerse una palabra de código corregido. Las realizaciones proporcionadas en el presente documento pueden usar una variante con el mismo efecto.

Durante el uso, un sistema PUF 100 puede funcionar de la siguiente manera.

En primer lugar el dispositivo comprende una pluralidad de bus keepers 110 que están encendidos. Como resultado, cada uno de la pluralidad de bus keepers 110 se asienta en un estado estable. Un bus keeper es un elemento biestable. El bus keeper permanecerá en uno de dos estados. Los estados estables en los que se inicia un bus keeper tras el encendido están determinados por las variaciones en las características físicas provocadas durante la fabricación de la pluralidad de bus keepers 110.

A continuación, se lee la pluralidad de bus keepers 110 por el circuito 120. El valor de inicio de un bus keeper puede representarse con un 0 lógico o un 1 lógico. La pluralidad de bus keepers 110 da lugar, de esta manera, a una pluralidad de valores de inicio. El circuito de lectura 120 puede representar la pluralidad de los valores de inicio como una matriz de bits, cada bit diferente en la matriz correspondiente a uno diferente de la pluralidad de bus keepers 110. La pluralidad de valores de inicio se llama la respuesta de la pluralidad de bus keepers 110.

La pluralidad de valores de inicio se procesa por el circuito 150. En una realización, la lógica de control 130 PUF ejecuta un algoritmo de corrección de errores. Por lo tanto, se obtiene una respuesta corregida.

Debido a la polarización en el bus keeper de uno de sus dos posibles estados iniciales estables puede haber una polarización en la respuesta. Por ejemplo, la mayoría de los valores pueden ser un 1 lógico. La cantidad de entropía por bit puede aumentarse verificando la respuesta corregida para una respuesta más corta, aplicando una función hash a la respuesta corregida. Por ejemplo, aplicando el algoritmo sha-256 a una respuesta corregida que sea

mayor que 256 bits, se obtiene una secuencia de 256 bits de la misma entropía, y por lo tanto una mayor entropía por bit.

Aumentando la entropía, se aumenta la dependencia de las variaciones en las características físicas provocadas durante la fabricación de la pluralidad de bus keepers 110 reduciendo la dependencia de la polarización de los bus keepers individuales.

Tener un árbol de MUX, permite tener un menor número de componentes en el dominio de alimentación. Como resultado, el dominio de alimentación es más pequeño y se atraerá una corriente menor. En particular, cuando conmuta el dominio de alimentación la corriente máxima será más baja. Por lo tanto, un conmutador para encender y apagar el dominio de alimentación que comprende una pluralidad de bus keepers 110, puede ser más pequeño. Un conmutador más pequeño es una ventaja. En particular, puede implementarse un conmutador más pequeño en un circuito integrado.

En una realización, la pluralidad de bus keepers 110 y el circuito de lectura 120 están integrados en un único circuito integrado. En una realización, la pluralidad de bus keepers 110, el circuito de lectura 120 y la lógica de control 130 PUF están integrados en un único circuito integrado. En una realización, la pluralidad de bus keepers 110, el circuito de lectura 120, la lógica de control 130 PUF, y la memoria 140 están integrados en un único circuito integrado. En una realización, la pluralidad de bus keepers 110, el circuito de lectura 120, la lógica de control 130 PUF, la memoria 140 y el circuito 150 están integrados en un único circuito integrado.

La figura 4 ilustra un refinamiento del mecanismo de lectura de la pluralidad de bus keepers 110, que pueden aplicarse en un sistema tal como el sistema PUF 100.

La figura 4 muestra un dominio de alimentación 410 conmutable. El dominio de alimentación 410 comprende una pluralidad de bus keepers 110. Los componentes en el dominio de alimentación 410 pueden estar desconectados de la fuente de alimentación, independientemente de otros componentes del circuito integrado de los que está compuesto el dominio de alimentación 410, tal como el circuito de lectura 120 o la lógica de control 130 PUF. La figura 4 comprende además un circuito de aislamiento 420. El circuito de aislamiento evita que el dominio de alimentación 410 esté conectado a los componentes CMOS mientras el dominio de alimentación está apagado. El circuito de aislamiento 420 evita redes flotantes dentro del circuito. La figura 4 comprende además un circuito de lectura, tal como el circuito de lectura 120, para leer la pluralidad de bus keepers 110 en el dominio de alimentación 410.

Durante el funcionamiento, el dominio de alimentación 410 está encendido. A continuación, el circuito de aislamiento 420 permite el acceso al dominio de alimentación 410 por el circuito 430 de lectura. A continuación, el circuito 430 de lectura lee el contenido de la pluralidad de bus keepers 110. La respuesta de la pluralidad de bus keepers 110, es decir, la pluralidad de valores de inicio, podrá remitirse a la lógica de control 130 PUF o al comparador 160 para su uso, o pueden exportarse del circuito integrado, etc.

Después de que se lean los contenidos de la pluralidad de bus keepers 110, el dominio de alimentación 410 se apaga. Por ejemplo, la lógica de control 130 PUF o el circuito de lectura 120 puede dar la orden para apagar el dominio de alimentación 410. Después de que se haya apagado el dominio de alimentación 410, el circuito de aislamiento 420 redirige el acceso al dominio de alimentación 410 repetidamente. Por ejemplo, el circuito de aislamiento 420 proporciona una respuesta fija predeterminada para leer los intentos, por ejemplo, un 0 lógico.

Son posibles diferentes implementaciones del circuito de aislamiento; por ejemplo, el circuito de aislamiento 420 puede estar configurado para mantener las salidas en el último valor de la señal y/o incluir una función de desplazamiento de nivel. Una función de desplazamiento de nivel puede usarse en el caso de que diferentes dominios de alimentación usen diferentes tensiones de alimentación.

El dominio de alimentación 410 proporciona varias ventajas.

Si se han usado los datos PUF obtenidos de la pluralidad de bus keepers 110, los datos pueden borrarse de una memoria de trabajo, por ejemplo, de la lógica 130. Por ejemplo, se deriva una clave, que se usa para un fin criptográfico, por ejemplo, cifrar o descifrar un mensaje, autenticación, etc. Esa clave puede eliminarse cuando se termine. Cuando se necesite la clave de nuevo, el dominio de alimentación 410 puede reiniciarse y la clave puede derivarse de nuevo. No es necesario el apagado del circuito integrado en el que está incluido el dominio de alimentación 410. Por lo tanto, se aumenta la seguridad ya que se disminuye el tiempo en el que el material sensible, por ejemplo, una llave, está presente en una memoria de trabajo.

Una PUF basada en CMOS está sujeta a una condición conocida como el envejecimiento. A medida que el PUF se hace más viejo, la calidad de sus respuestas se degrada; el número de diferencias entre una respuesta original obtenida durante la inscripción y una nueva respuesta obtenida después de encender la pluralidad de bus keepers 110 durante una fase de uso se incrementa. En algún momento los datos auxiliares pueden necesitar corregir muchos errores. En ese momento, no puede recuperarse la respuesta de inscripción.

Los inventores han tenido la idea de que el envejecimiento se ve agravado por mantener alimentados los bus keepers. Introduciendo el dominio de alimentación 410, puede reducirse el tiempo durante el que se alimenta la pluralidad de bus keepers 110, y se reduce el envejecimiento. Anteriormente, se creía que el envejecimiento era provocado principalmente por el número de secuencias de apagado y encendido a las que estaba sometido un elemento CMOS.

Aunque en un circuito de aislamiento, para aislar una pluralidad de bus keepers 110 cuando está separada de la fuente de alimentación, se prefiere en gran medida evitar las puertas flotantes, esto no es estrictamente necesario, por ejemplo, si la flotación se puede tolerar.

La figura 5 muestra con más detalle una fuente de datos PUF que incluye una pluralidad de bus keepers 110 y un circuito de lectura. La figura 5 muestra 4 bus keepers 112, 114, 116 y 118. Un circuito de lectura 120 comprende un así llamado árbol MUX a través del que puede leerse la pluralidad de bus keepers. Del árbol MUX, se muestran tres MUX, el MUX 510, el MUX 520 y el MUX 530.

En general, una forma de organizar la lectura de datos de la pluralidad de bus keepers 110, es tener la lógica de control 130 PUF que envía una señal de selección de bus keeper al circuito de lectura 120; estando el circuito de lectura 120 configurado para seleccionar un bus keeper de la pluralidad de bus keepers 110 asociados con la señal de selección de bus keeper y para leer el bus keeper seleccionado.

Una realización del circuito de lectura 120 comprende una pluralidad de elementos de MUX. En una realización, cada bus keeper de la pluralidad de bus keepers está conectado a unos elementos de MUX de la pluralidad de elementos de MUX. En una realización, cada bus keeper diferente de la pluralidad de bus keepers está conectado a un MUX diferente de la pluralidad de elementos de MUX. En una realización, al menos dos bus keepers de la pluralidad de bus keepers están conectados al mismo MUX de la pluralidad de MUX.

En la figura 5, la señal de selección de bus keepers comprende una pluralidad de señales. Un MUX en el árbol de MUX está configurado para recibir una señal de la pluralidad de señales de selección y para seleccionar en respuesta una de sus entradas. Por ejemplo, un MUX seleccionará una entrada si recibe un 1 lógico y selecciona la otra entrada si recibe un 0 lógico.

En la figura 5, el árbol de MUX está organizado en un número de capas (también llamados niveles); recibiendo cada MUX en una misma capa la misma señal de la pluralidad de señales. Cada MUX en la capa 0 está conectado a dos bus keepers diferentes, estando cada uno de los bus keepers de la pluralidad de bus keepers 110 conectado a un MUX en la capa 0. Cada MUX en la capa 0 recibe una señal sel_0. Cada MUX en una capa posterior, es decir, las capas 1 a x, están conectados con unos MUX en capas anteriores. Junto con el árbol de MUX, es decir, el circuito de lectura permite una lectura individual de los bus keepers en la pluralidad de bus keepers 110.

El número de MUX depende del número de bus keepers. Cuando se usan n bus keepers, un árbol de MUX es posible que tenga n-1 MUX.

Si el número de bus keepers es una potencia de 2, y el número es mayor que 1, los MUX pueden estar dispuestos de tal manera que cada MUX en la capa 1 a x solo está conectado a unos MUX en la capa anterior más cercana a la pluralidad de bus keepers 110; además, todos los bus keepers están conectados a un MUX en la capa 0. Si el número de MUX no es una potencia de 2, puede ser necesario para algunos MUX conectarse a más de una capa anterior.

Una ventaja de usar los MUX para seleccionar un bus keeper en lugar de un decodificador de dirección , por ejemplo, un decodificador de dirección como el usado en la SRAM, es que la pluralidad de bus keepers 110 puede separarse del circuito de lectura en un dominio de alimentación. Como resultado, el dominio de alimentación es más pequeño. Un dominio de alimentación más pequeño tiene la ventaja de que puede usarse un conmutador más pequeño. Tener una pluralidad de bus keepers 110 en un dominio de alimentación retrasa el proceso de envejecimiento.

El sistema PUF 100, en particular, el circuito de lectura 120 y la pluralidad de bus keepers 110 no tienen medios de escritura para escribir en la pluralidad de bus keepers 110. Esto permite que el circuito de lectura 120 y la pluralidad de bus keepers 110 sean más pequeños y consuman menos energía. El circuito de lectura 120 está configurado para leer la pluralidad de bus keepers 110 en la ausencia de medios de escritura para escribir datos de forma selectiva en la pluralidad de bus keepers 110 de lectura.

La figura 6 muestra una realización en la que la pluralidad de bus keepers 110 está en un dominio de alimentación.

La figura 6 es la misma que la figura 5 excepto por la incorporación de un dominio de alimentación conmutable y un circuito de aislamiento.

La pluralidad de bus keepers 110 se compone de un dominio de alimentación conmutable para conectar o desconectar de manera selectiva la pluralidad de bus keepers 110 a una fuente de alimentación. La conexión puede ser bajo demanda. Por ejemplo, la conmutación puede iniciarse por el circuito de lectura 120, por ejemplo, conectándose a una fuente de alimentación antes de una lectura de salida de un bus keeper. El circuito de lectura 120 puede desconectar la pluralidad de bus keepers 110 de la fuente de alimentación después de que se complete la lectura. Por ejemplo, la conmutación puede iniciarse por la lógica de control 130 PUF.

La figura 6 comprende un circuito de aislamiento 420 para aislar el dominio de alimentación, es decir, la pluralidad de bus keepers 110, del resto del circuito cuando la pluralidad de bus keepers 110 no está conectada a una fuente de alimentación. En esta realización, el circuito de aislamiento 420 comprende una pluralidad de puertas AND, en este caso dispuestas en una capa. La capa de las puertas AND se dispone entre la pluralidad de bus keepers 110 y la capa 0 del circuito de lectura. Se muestran las puertas AND 612, 614, 616 y 618 en el circuito de aislamiento 420. En esta realización, el número de puertas AND es igual al número de bus keepers en la pluralidad de bus keepers 110. Cada una de las puertas AND en la pluralidad de puertas AND tiene dos entradas; estando una entrada conectada a una señal de control de alimentación, estando la otra conectada a un bus keeper de la pluralidad de bus keepers 110.

Durante el funcionamiento, cuando el dominio de alimentación está encendido, una puerta AND permitirá que pasen señales a través de la pluralidad de bus keepers 110. Sin embargo, cuando el dominio de alimentación está apagado, la puerta AND bloquea eficazmente a la pluralidad de bus keepers 110 del circuito de lectura 120.

La figura 7 muestra una manera diferente en que un circuito de aislamiento puede combinarse con el circuito de lectura 120. La capa 0 del circuito de lectura 120 (como se muestra en la figura 5) está incluida en el dominio de alimentación. Es decir, los MUX 510 y 520 también pueden desconectarse de manera selectiva de la fuente de alimentación. Un circuito de aislamiento está dispuesto entre un lado de salida del dominio de alimentación y un lado de entrada de una parte del circuito de lectura 120 fuera del dominio de alimentación. En la figura 7, el circuito de aislamiento está dispuesto entre dos capas del circuito de lectura 120; por ejemplo, entre las capas 0 y 1. Una ventaja es que el circuito de aislamiento es más pequeño, por ejemplo, necesita menos puertas AND.

Las celdas de aislamiento, por ejemplo, las puertas AND, son puertas adicionales, y solo incluidas para evitar que las señales flotantes entren en la parte del circuito que permanece alimentada. Las señales flotantes pueden producirse cuando el dominio de alimentación conmutable está desconectado. Debido a que estas son celdas adicionales que no son necesarias para la funcionalidad (sólo para suprimir efectos físicos), es deseable mantener su número lo más bajo posible.

Incluyendo algunos niveles de MUX en el dominio de alimentación conmutable se reduce el número de señales que cruzan el dominio de alimentación (dos factores para cada nivel de MUX) y con ello también el número de celdas de aislamiento. Esto reduce la superficie general del chip. Esto puede ser significativo dependiendo del número de bus keepers y del tamaño total del chip.

Por otro lado, manteniendo el circuito de lectura 120 completamente separado del dominio de alimentación, el dominio de alimentación es más pequeño y, correspondientemente, los conmutadores de alimentación pueden ser más pequeños, porque durante la lectura de los datos PUF estarán alternando menos señales por lo que se reduce el consumo de energía. De qué manera se realiza la compensación, por ejemplo, la compensación entre el tamaño del conmutador de alimentación y el tamaño de las celdas de aislamiento, depende de las limitaciones del diseño. Un conmutador de alimentación puede ser un transistor, por ejemplo, un transistor FET adecuado para el tamaño del dominio de alimentación.

La figura 8 muestra todavía una forma diferente de lectura de la pluralidad de bus keepers 110 por el circuito de lectura 120. La figura 8 muestra una implementación del circuito de lectura 120 con un registro de desplazamiento como el circuito de lectura. En este caso, el circuito de lectura 120 comprende una pluralidad de MUX y de flip-flops.

El circuito de lectura con registros de desplazamiento no necesita decodificación de direcciones. Está construido con flip-flops que están conectados en serie con los MUX. En el encendido los bus keepers se estabilizan a sus valores de datos PUF.

Después de esto, la señal de lectura se hace 1 y se proporciona un reloj en los registros. Esto copia los datos PUF en los flip-flops. Después de esto, la señal de lectura se hace 0 y en cada siguiente reloj los datos se desplazan un bit a la vez a través de los flip-flops hacia la salida.

Todavía son posibles otros circuitos de lectura. Pueden crearse múltiples circuitos de lectura en paralelo para obtener un bus como salida en lugar de un solo bit. Por ejemplo, puede obtenerse un circuito de lectura sin multiplexores a partir de la figura 9 de la siguiente manera.

Se reemplazan en la figura 9, los registros A y B por dos archivos de bus keepers. Por ejemplo, cada registro puede comprender 32 bus keepers. Los bus keepers pueden leerse de manera selectiva a través de las memorias

intermedias de tres estados y el bus paralelo de 32 bits de ancho. Obsérvese que esta realización no comprende lógica de escritura para escribir en el bus keeper.

Debería tenerse en cuenta que las realizaciones mencionadas anteriormente ilustran más que limitan la invención, y que los expertos en la materia serán capaces de diseñar muchas realizaciones alternativas sin alejarse del alcance de las reivindicaciones adjuntas. En las reivindicaciones, cualquier signo de referencia colocado entre paréntesis no se interpretará como que limita la reivindicación. El uso del verbo "comprende" y sus conjugaciones no excluyen la presencia de elementos o etapas distintos de los indicados en una reivindicación. El artículo "un" o "una" precediendo a un elemento no excluye la presencia de una pluralidad de tales elementos. La invención puede implementarse por medio de hardware que comprende varios elementos distintos, y por medio de un ordenador programado adecuadamente. En la reivindicación de dispositivo que enumera varios medios, varios de estos medios pueden realizarse por uno y el mismo elemento de hardware. El mero hecho de que ciertas medidas se enumeren en las reivindicaciones dependientes mutuamente diferentes no indica que una combinación de estas medidas no pueda usarse como una ventaja.

REIVINDICACIONES

1. Una función física no clonable (100) que comprende:

- una pluralidad de bucles de acoplamiento cruzado de dos inversores (110), estando cada bucle de acoplamiento cruzado de la pluralidad de bucles de acoplamiento cruzado configurado para asentarse en uno de al menos dos estados estables diferentes tras el encendido, siendo el estado estable específico en el que se asienta un bucle de acoplamiento cruzado específico de la pluralidad de bucles de acoplamiento cruzado dependiente al menos en parte de las características físicas al menos parcialmente aleatorias del bucle de acoplamiento cruzado específico, y
- un circuito de lectura (120) para leer la pluralidad de estados estables en los que se asienta la pluralidad de bucles de acoplamiento cruzado (110) después de un encendido, estando la función física no clonable para la pluralidad de bucles de acoplamiento cruzado configurada para ser de solo lectura, **caracterizada por**
- un dominio de alimentación conmutable, estando la pluralidad de bucles de acoplamiento cruzado (110) comprendida en el dominio de alimentación y estando al menos una parte de la función física no clonable fuera del dominio de alimentación, estando el dominio de alimentación configurado para conectar y desconectar de manera selectiva la pluralidad de bucles de acoplamiento cruzado (110) de la fuente de alimentación mientras que la al menos una parte de la función física no clonable está conectada a la fuente de alimentación.

2. Una función física no clonable (100) como en la reivindicación 1, en la que la pluralidad de bucles de acoplamiento cruzado de dos inversores (110) son una pluralidad de bus keepers.

3. Una función física no clonable (100) como en las reivindicaciones 1 o 2, en la que al menos una parte del circuito de lectura está fuera del dominio de alimentación.

4. Una función física no clonable (100) como en una cualquiera de las reivindicaciones anteriores, en la que el dominio de alimentación se alimenta solo durante la lectura de los bucles de acoplamiento cruzado.

5. Una función física no clonable (100) como en las reivindicaciones 1, 2, 3 o 4, en la que la pluralidad de bucles de acoplamiento cruzado (110), el dominio de alimentación, el conmutador de alimentación y la al menos una parte de la función física no clonable están implementados en un único circuito integrado.

6. Una función física no clonable (100) como en las reivindicaciones 1, 2, 3, 4 o 5 que comprende un circuito de aislamiento para aislar la pluralidad de bucles de acoplamiento cruzado (110) de la al menos una parte de la función física no clonable, mientras que la pluralidad de bucles de acoplamiento cruzado (110) está desconectada de la fuente de alimentación.

7. Una función física no clonable (100) como en una cualquiera de las reivindicaciones anteriores, en la que al menos un bucle de acoplamiento cruzado comprende exactamente una conexión de datos, y en la que la exactamente una conexión de datos está configurada solo para leer el estado estable en el que el al menos un bucle de acoplamiento cruzado se ha asentado tras el encendido.

8. Una función física no clonable (100) como en una cualquiera de las reivindicaciones anteriores, en la que el circuito de lectura (120) comprende una pluralidad de multiplexores para seleccionar los bucles de acoplamiento cruzado de la pluralidad de bucles de acoplamiento cruzado.

9. Una función física no clonable (100) como en la reivindicación 8, en la que cada bucle de acoplamiento cruzado de la pluralidad de bucles de acoplamiento cruzado está conectado a un multiplexor de la pluralidad de multiplexores.

10. Una función física no clonable (100) como en una cualquiera de las reivindicaciones 8 y 9, en la que al menos dos bucles de acoplamiento cruzado de la pluralidad de bucles de acoplamiento cruzado están conectados al mismo multiplexor de la pluralidad de multiplexores.

11. Una función física no clonable (100) como en una cualquiera de las reivindicaciones 8, 9, y 10, en la que la pluralidad de multiplexores está dispuesta como un árbol de multiplexores, estando el circuito de lectura dispuesto para leer la pluralidad de estados estables a través del árbol de multiplexores.

12. Una función física no clonable (100) como en una cualquiera de las reivindicaciones 8 y 9, en la que cada bucle de acoplamiento cruzado diferente de la pluralidad de bucles de acoplamiento cruzado está conectado a un multiplexor diferente de la pluralidad de multiplexores.

13. Una función física no clonable (100) como en una cualquiera de las reivindicaciones anteriores, que comprende una lógica de control PUF para derivar un identificador de la pluralidad de estados estables.

14. Una función física no clonable (100) como en la reivindicación 13, en la que la lógica de control PUF está configurada para aplicar un algoritmo de corrección de errores a la pluralidad de estados estables y a los datos auxiliares para derivar el identificador.

15. Una función física no clonable (100) como en la reivindicación 13, en la que la lógica de control PUF está configurada para derivar un número aleatorio de la pluralidad de estados estables.

16. Una función física no clonable (100) como en la reivindicación 13, en la que la lógica de control PUF está configurada para un ciclo de lectura que comprende:

- apagar la pluralidad de bucles de acoplamiento cruzado,
- encender la pluralidad de bucles de acoplamiento cruzado, y
- leer la pluralidad de bucles de acoplamiento cruzado.

17. Un método para obtener datos PUF que comprende

- encender una pluralidad de bucles de acoplamiento cruzado de dos inversores (110) comprendidos en un dominio de alimentación conmutable configurado para conectar y desconectar de manera selectiva la pluralidad de bucles de acoplamiento cruzado de dos inversores (110) de la fuente de alimentación,
- permitir que cada uno de la pluralidad de bucles de acoplamiento cruzado de dos inversores (110) se asiente en uno de al menos dos estados estables diferentes, siendo el estado estable específico en el que se asienta un bucle de acoplamiento cruzado específico de la pluralidad de bucles de acoplamiento cruzado dependiente al menos en parte de las características físicas al menos parcialmente aleatorias del bucle de acoplamiento cruzado específico,
- leer la pluralidad de estados estables en los que se asienta la pluralidad de bucles de acoplamiento cruzado de dos inversores (110) después de un encendido a través de un circuito de lectura, siendo la pluralidad de bucles de acoplamiento cruzado de dos inversores de solo lectura.

18. Un ordenador que comprende una función física no clonable como en la reivindicación 1, programado con un programa informático que comprende unos medios de código de programa informático adaptados para realizar todas las etapas de la reivindicación 17 cuando el programa informático se ejecuta en un ordenador.

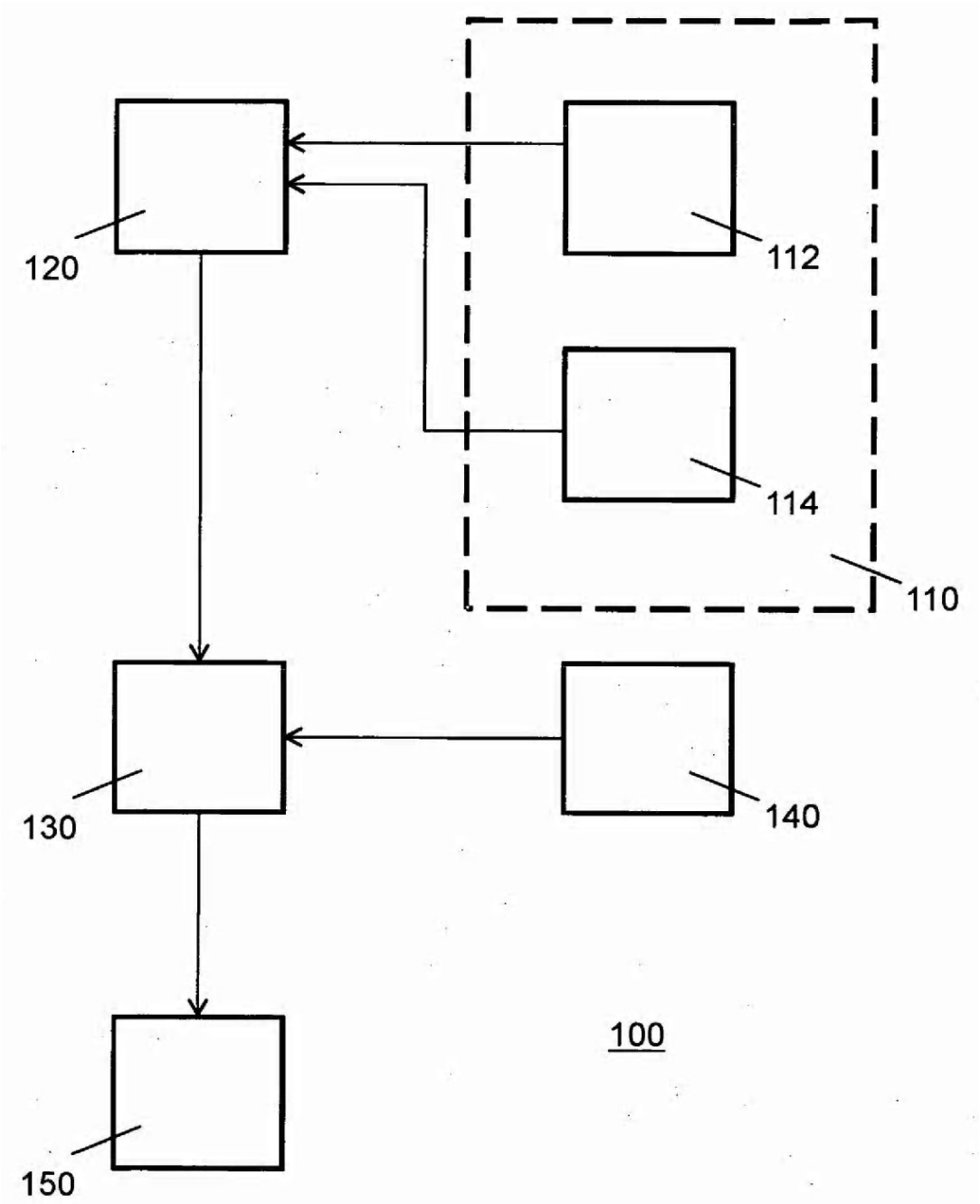

Figura 1

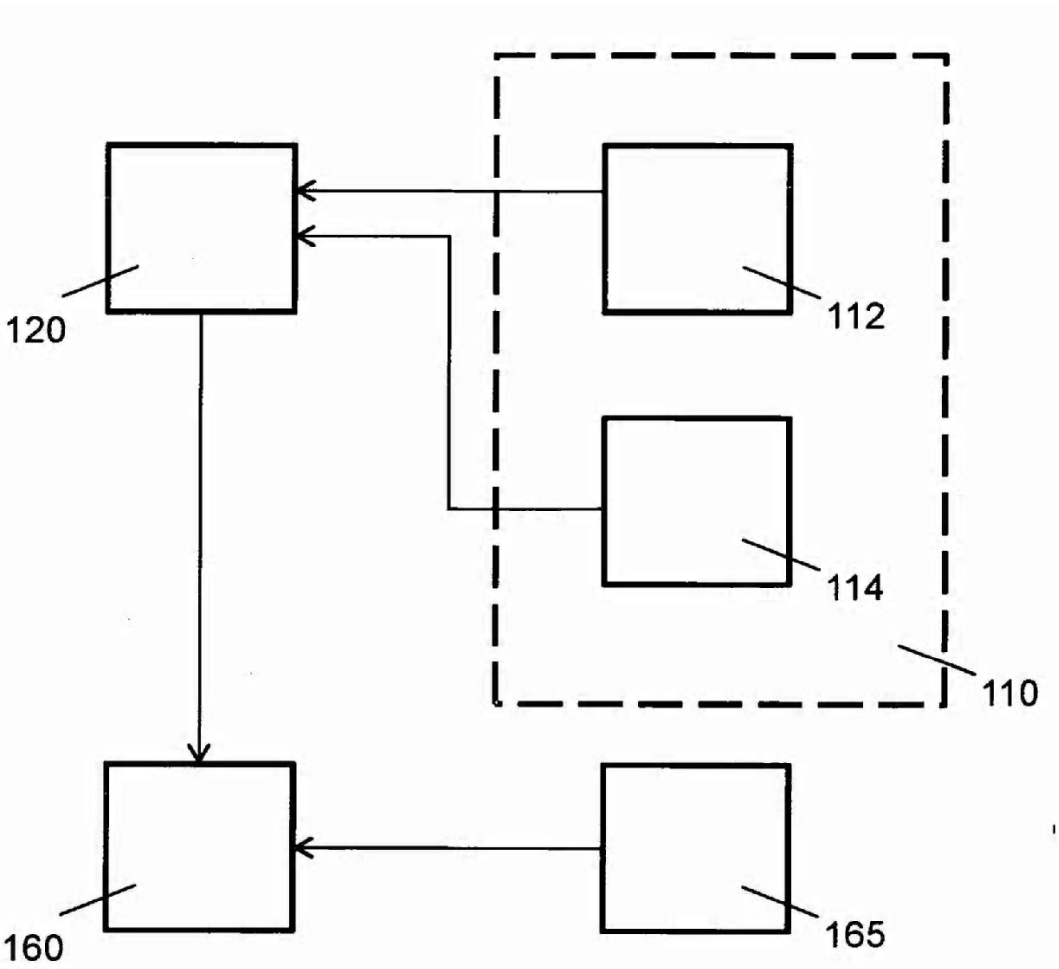

Figura 2

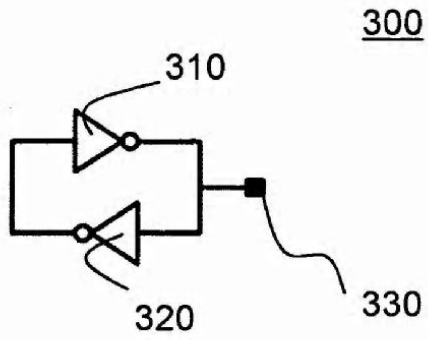

Figura 3a

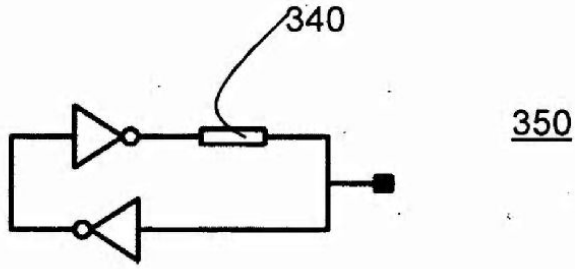

Figura 3b

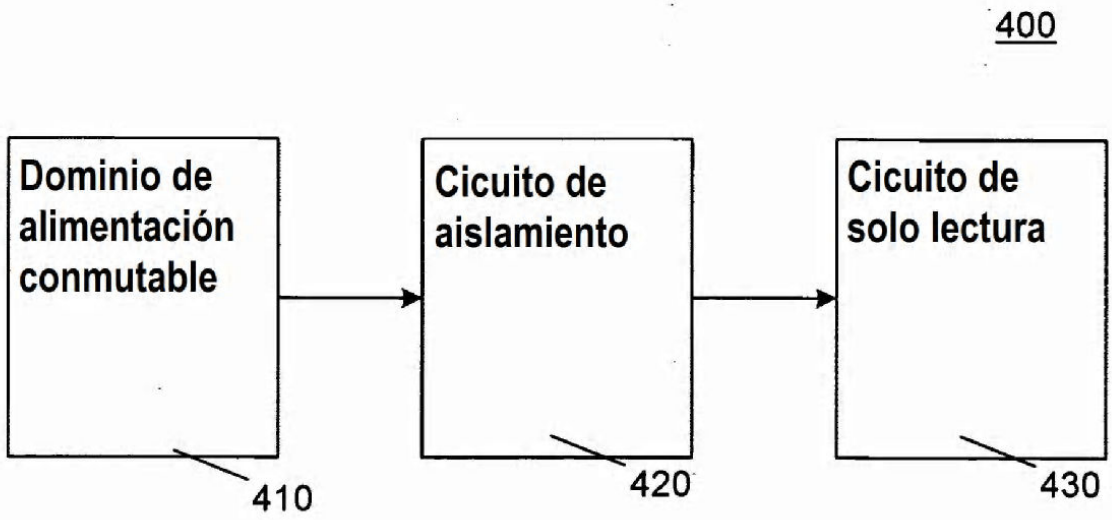

Figura 4

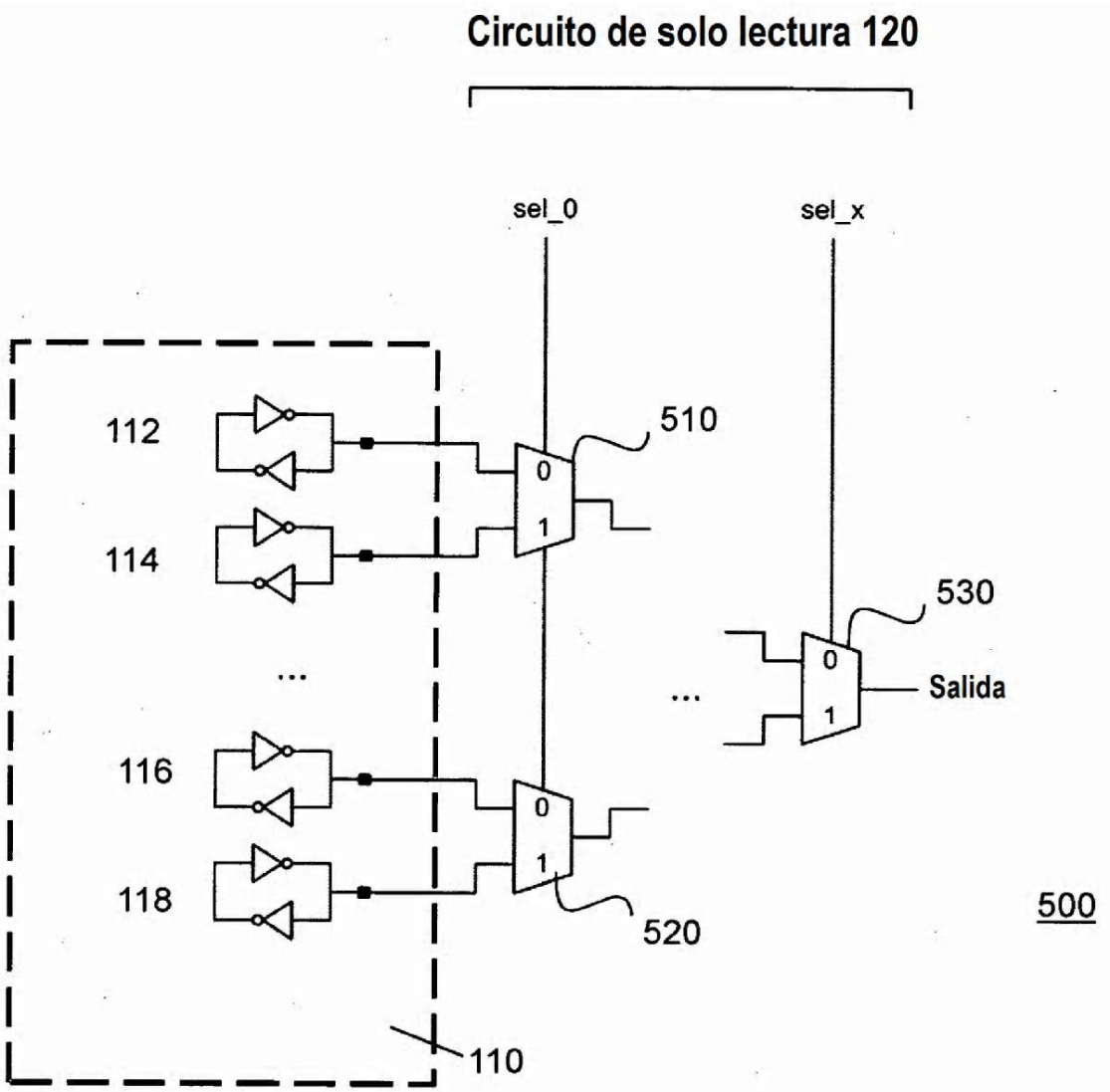
Circuito de solo lectura 120
sel_0
sel_x
112
114
116
118
510
520
530
0
1
Salida
500
110

Figura 5

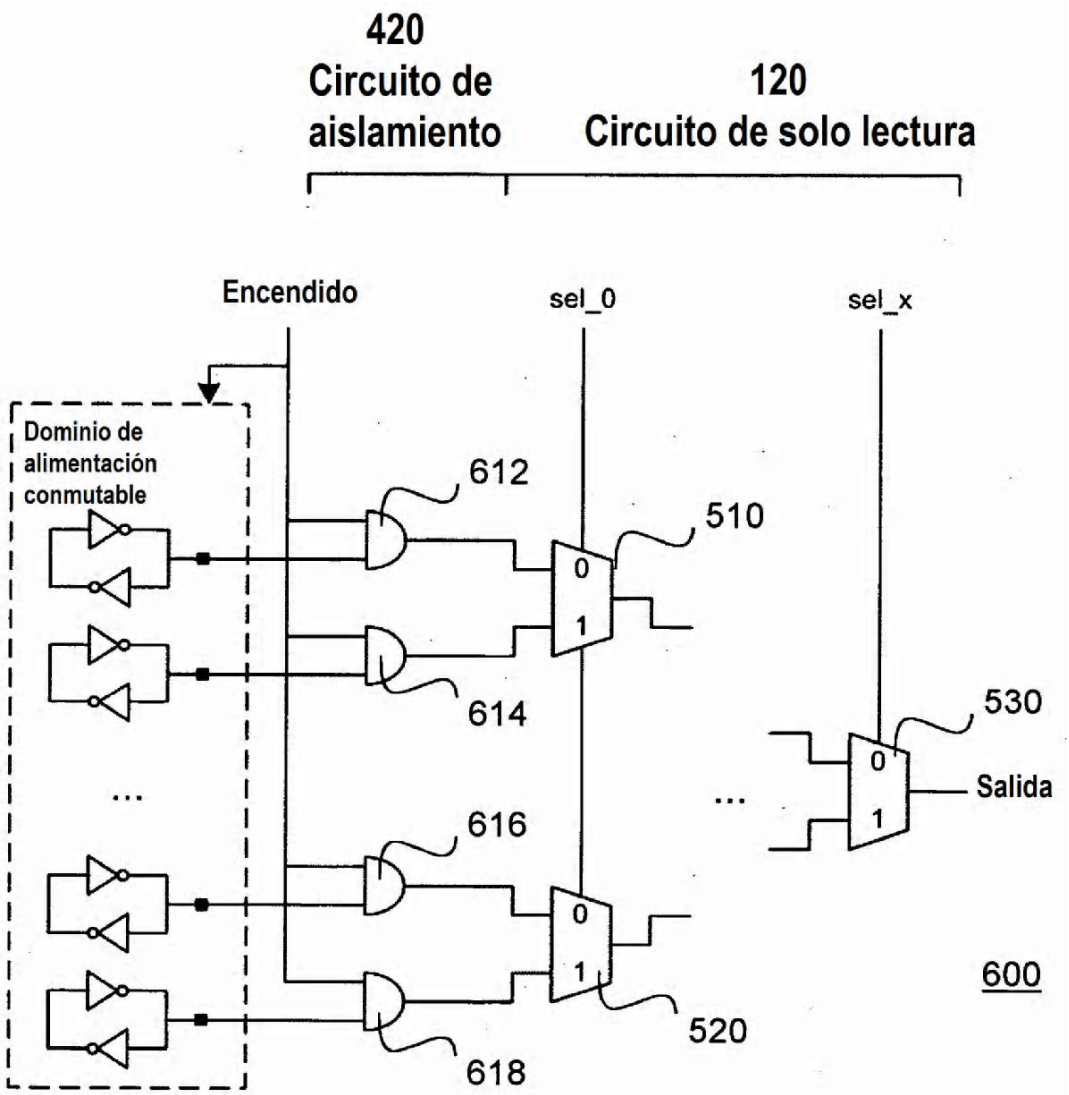
420
Circuito de aislamiento
120
Circuito de solo lectura
Encendido
sel_0
sel_x
Dominio de alimentación conmutable
612
510
614
530
Salida
616
520
618
600

Figura 6

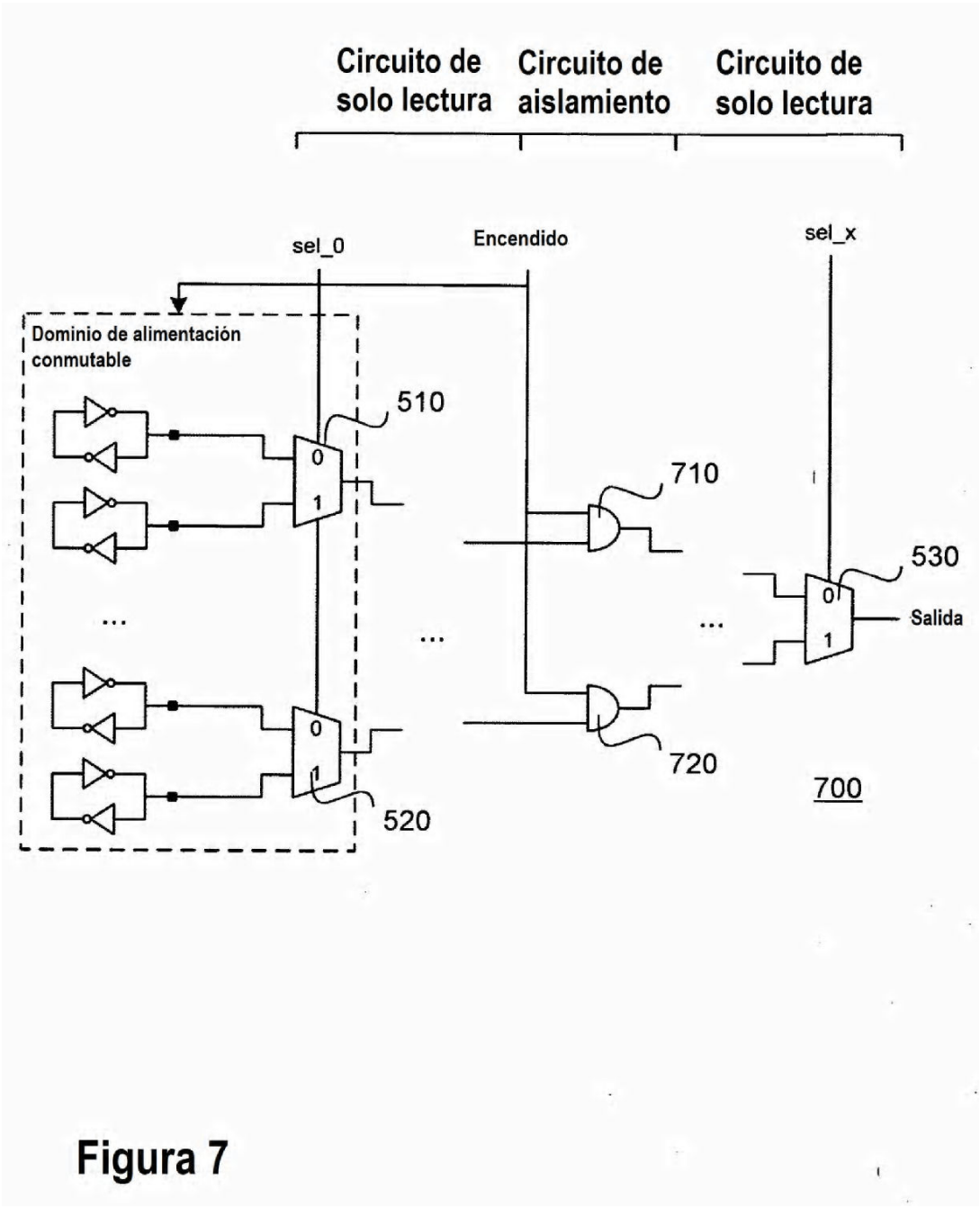
Circuito de solo lectura
Circuito de aislamiento
Circuito de solo lectura
sel_0
Encendido
sel_x
Dominio de alimentación conmutable
510
710
530
Salida
520
720
700

Figura 7

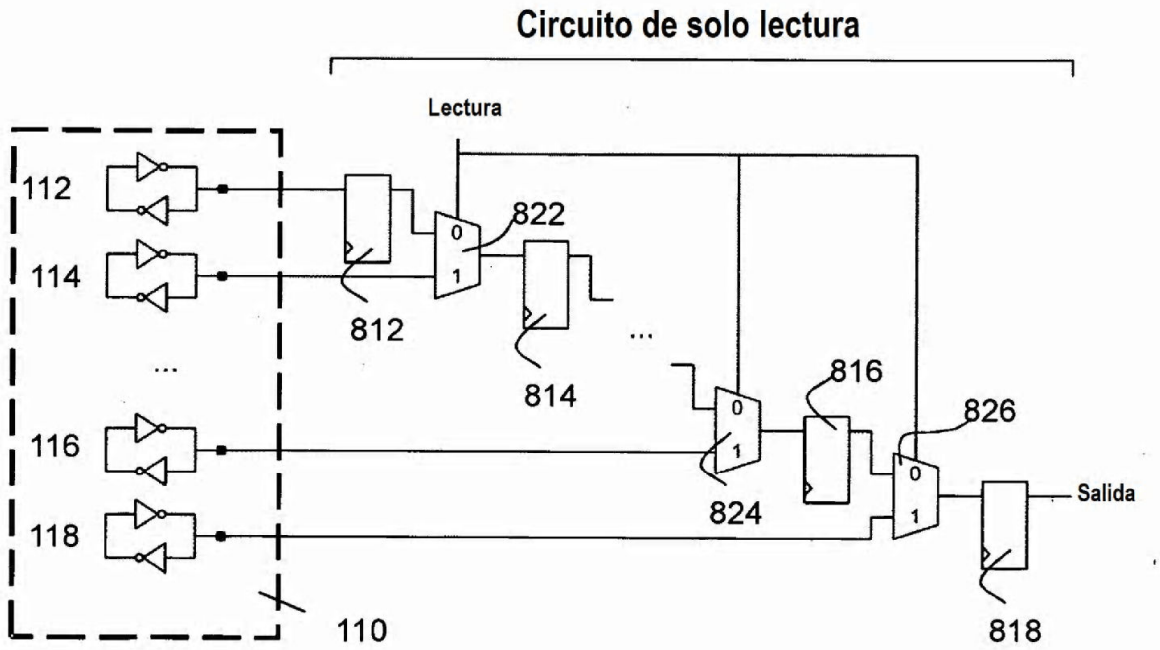
Circuito de solo lectura
Lectura
112
114
116
118
110
812
822
814
816
824
826
Salida
818

Figura 8

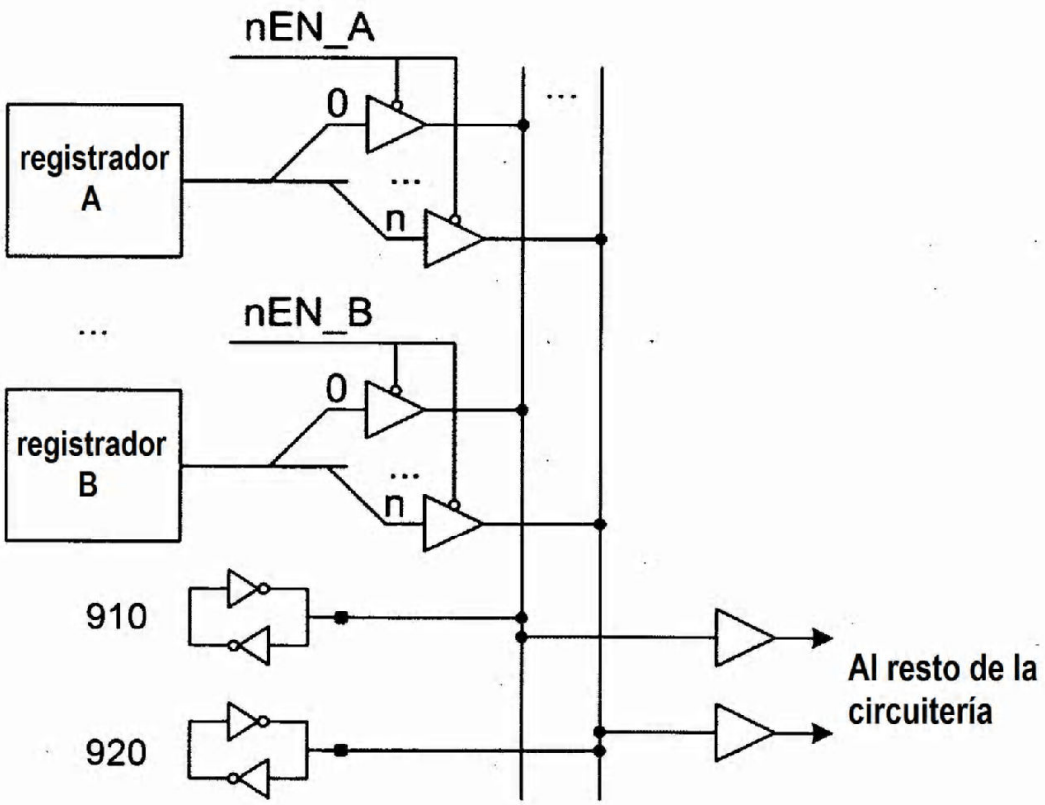
nEN_A
0
...
n
registrador A
...
nEN_B
0
...
n
registrador B
910
920
Al resto de la circuitería

Figura 9