(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 564 505**

(51) Int. CI.:

H04L 9/06 (2006.01)
H04L 12/22 (2006.01)
G06F 21/55 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.03.2011 E 11862420 (4)**

(97) Fecha y número de publicación de la concesión europea: **09.12.2015 EP 2693680**

(54) Título: **Aparato a salvo de ataques de análisis de consumo de potencia para encriptación y método para operar el mismo**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.03.2016

(73) Titular/es:

IUCF-HYU (INDUSTRY-UNIVERSITY COOPERATION FOUNDATION HANYANG UNIVERSITY) (100.0%)
17 Haengdang-dong
Seongdong-gu, Seoul 133-791, KR

(72) Inventor/es:

KIM, DONG KYUE;
CHOI, BYONG DEOK y
KIM, TAE WOOK

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Aparato a salvo de ataques de análisis de consumo de potencia para encriptación y método para operar el mismo

Campo técnico

La presente invención se refiere al campo de la seguridad digital, y más en particular, a un aparato de encriptación seguro frente a un ataque de análisis de consumo de potencia y a un método de operación del mismo.

Técnica antecedente

Hasta ahora, un factor importante en la seguridad de un sistema de criptografía ha sido un algoritmo de encriptación que usa una clave secreta. En consecuencia, la búsqueda de la seguridad del sistema de criptografía ha sido enfocada a la protección contra ataques directos sobre la clave secreta y el algoritmo de encriptación.

Sin embargo, un sistema de criptografía real es vulnerable a ataques directos sobre la clave secreta y el algoritmo de encriptación, y a un ataque indirecto mediante la medición de valores físicos, tal como una pluralidad de señales de entrada/salida, por ejemplo una magnitud de tensión o de corriente, y similar, y una diversidad de información de fugas, como por ejemplo la radiación de una onda electromagnética, un cambio de consumo de potencia, y similar.

Una acción de deshabilitación de un sistema de criptografía mediante la medición de tales valores físicos sin desempacar un chip, puede ser mencionada como un ataque no invasivo. Entre tales ataques no invasivos, una acción de deshabilitar el sistema de criptografía usando un valor de entrada, un valor de salida, y otra información física adicional que puede ser mencionada como ataque de canal lateral.

Un ataque sobre un sistema de criptografía puede ser entendido como un análisis sobre la operación de cada módulo en el sistema de criptografía. El ataque de canal lateral puede ser clasificado según unos pocos tipos, en base al esquema de análisis. Un ataque de temporización puede revelar contenidos de un código en base a una diferencia en el tiempo de operación entre operaciones. Un ataque por análisis de consumo de potencia puede poner de relieve el contenido del código midiendo la cantidad de potencia consumida para la encriptación y la desencriptación. Un ataque electromagnético diferencial puede poner de relieve los contenidos del código midiendo una onda electromagnética de fugas durante una operación.

Entre los ataques de canal lateral, el ataque por análisis de consumo de potencia puede ser menciona simplemente como ataque de análisis de potencia. El ataque de análisis de potencia puede ser clasificado según un análisis de medición de potencia simple (PSA) y analizando simplemente un valor de corriente de una fuente de alimentación durante una operación, un análisis de potencia diferencial (DPA) del análisis estadístico de corriente, y un análisis de potencia diferencial de orden superior por realización de un análisis de orden superior mediante la combinación de varios PDAs.

El documento US 2004/0145339 divulga un método para proteger una entidad electrónica tal como una tarjeta inteligente contra análisis de potencia simple/diferencial.

Una técnica de defensa contra un ataque de canal lateral de ese tipo puede incluir una técnica de ocultación de la habilitación de una cantidad de potencia consumida de modo que sea constante o aleatoria para eliminar la correlación entre un consumo de potencia y los datos, principalmente una clave secreta, y una técnica de enmascaramiento para la eliminación de una correlación entre el consumo de potencia y los datos, principalmente la clave secreta, mediante aleatorización de datos durante un proceso intermedio de la operación.

En este caso, la técnica de ocultación puede ser implementada empleando un esquema de enfoque de software o un esquema de enfoque de hardware. En el esquema de enfoque de hardware, se puede ocultar una correlación entre un tipo de operación y un valor de corriente de la fuente de alimentación, y se puede eliminar una diferencia en un patrón del valor de corriente de los valores de entrada y de salida. En consecuencia, el interés del enfoque de hardware se incrementa.

Los sistemas de implementación de la técnica de ocultación para impedir un ataque de análisis de potencia pueden incluir una lógica de precarga mediante la cual, una tensión y/o una corriente que van a constituir la entrada a un módulo de encriptación, y la salida desde el modulo de encriptación, pueden tener valores idénticos.

Aunque la lógica de precarga puede habilitar la tensión y/o la corriente que van a ser introducidos en el módulo de encriptación, y la salida desde el módulo de encriptación para que tengan valores idénticos en teoría, la lógica de precarga puede fallar en cuanto a garantizar la consistencia de la implementación real del modulo de encriptación.

Descripción de la invención

Objetivos técnicos

Un aspecto de la presente invención proporciona un aparato de encriptación y un método de operación del mismo, que pueden garantizar un nivel de consistencia más alto de un valor de tensión o de corriente que constituyen la entrada en, o la salida desde, un módulo de encriptación, en comparación con un aparato de encriptación convencional.

Soluciones técnicas

De acuerdo con un aspecto de la presente invención, se proporciona un aparato de encriptación que incluye un módulo de encriptación para ejecutar un algoritmo de encriptación, y un módulo de control para controlar la transferencia de carga desde una fuente de alimentación externa hasta el módulo de encriptación mediante el control de una trayectoria de paso de corriente entre el módulo de encriptación y la fuente de alimentación externa.

En este caso, el módulo de control puede bloquear eléctricamente la trayectoria de paso de corriente entre el módulo de encriptación y la fuente de alimentación externa.

El módulo de control puede incluir una unidad de almacenaje de carga para almacenar una carga, y para suministrar la carga almacenada al módulo de encriptación.

El módulo de encriptación puede estar conectado a un nodo de tierra separado diferente de un nodo de tierra de la fuente de alimentación externa.

La unidad de almacenaje de carga puede incluir un condensador para almacenar una carga. En este ejemplo, el módulo de control puede incluir además una primera unidad de transferencia de carga para cargar el condensador transfiriendo, hasta la unidad de almacenaje de carga, la carga suministrada por la fuente de alimentación externa, en un primer estado correspondiente a un período de tiempo anterior a que se ejecute el algoritmo de encriptación.

La primera unidad de transferencia de carga puede incluir un primer conmutador para cerrar o abrir una conexión eléctrica entre un nodo VDD correspondiente a un ánodo de la fuente de alimentación externa y un primer terminal del condensador, y un segundo conmutador, activado con el primer conmutador, simultáneamente, para cerrar o abrir una conexión eléctrica entre un GND (nodo de tierra) correspondiente a un nodo de tierra de la fuente de alimentación externa y un segundo terminal del condensador.

El módulo de control puede incluir además una segunda unidad de transferencia de carga para transferir, al módulo de encriptación, una carga suministrada por la unidad de almacenaje de carga, en un segundo estado correspondiente a un período de tiempo durante el que se ejecuta el algoritmo de encriptación.

La segunda unidad de transferencia de carga puede incluir un tercer conmutador para cerrar o abrir una conexión eléctrica entre un primer terminal del condensador y un primer terminal del módulo de encriptación y un cuarto conmutador, accionado con el tercer conmutador, simultáneamente, para cerrar o abrir una conexión eléctrica entre un segundo terminal del condensador y un segundo terminal del módulo de encriptación.

La unidad de almacenaje de carga puede incluir además un quinto conmutador, para que sea cerrado en un tercer estado correspondiente a un período de tiempo posterior a la ejecución del algoritmo de encriptación, para descargar el condensador incluido en la unidad de almacenaje de carga.

Según otro aspecto de la presente invención, se proporciona un aparato de encriptación, que incluye un módulo de encriptación para ejecutar un algoritmo de encriptación, una primera unidad de transferencia de carga para recibir potencia suministrada por una fuente de alimentación externa, en un primer estado correspondiente a un período de tiempo anterior a que se ejecute el algoritmo de encriptación una unidad de almacenaje de carga para almacenar una carga recibida y transferida por la primera unidad de transferencia de carga, en el primer estado, y una segunda unidad de transferencia de carga para transferir la carga almacenada en el unidad de almacenaje de carga al módulo de encriptación, en un segundo estado correspondiente a un período de tiempo durante el que se ejecuta el algoritmo de encriptación,. En este caso, la primera unidad de transferencia de carga puede desconectar un terminal de tierra del módulo de encriptación de un terminal de tierra de la fuente de alimentación externa, en el segundo estado.

Según otro aspecto más de la presente invención, se proporciona un método de operación de un aparato de encriptación que incluye un módulo de encriptación para ejecutar un algoritmo de encriptación, incluyendo el método almacenar, mediante una primera unidad de transferencia de carga incluida en el aparato de encriptación, potencia suministrada por una fuente de alimentación externa en una unidad de almacenaje de carga incluida en el aparato de encriptación, en un primer estado correspondiente a un período de tiempo anterior a que se ejecute el algoritmo de encriptación; transferir, mediante una segunda unidad de transferencia de carga incluida en el aparato de encriptación, una carga almacenada en la unidad de almacenaje de carga al módulo de encriptación, y llevar a cago, mediante el módulo de encriptación, el algoritmo de encriptación, en un segundo estado correspondiente a un período de tiempo durante el que se ejecuta el algoritmo de encriptación, y descargar, mediante la unidad de

almacenaje de carga, un dispositivo de almacenaje de carga incluido en una porción interna de la unidad de almacenaje de carga que almacena una carga, en un tercer estado correspondiente a un período de tiempo después de que se haya ejecutado el algoritmo de encriptación.

Efectos ventajosos

Según una realización de la presente invención, se puede evitar un ataque de análisis de potencia sobre un modulo de encriptación, permitiendo que se suministre una corriente por parte de la fuente de alimentación externa al módulo de encriptación que sea completamente ajena a la operación de un algoritmo del modulo de encriptación, y garantizar un nivel de consistencia más alto de un valor de tensión o de corriente que va a ser introducido en, o presentado a la salida del, modulo de encriptación.

Breve descripción de los dibujos

La figura 1 ilustra un aparato de encriptación según una realización de la presente invención.

La figura 2 ilustra un ejemplo detallado de un aparato de encriptación según una realización de la presente invención.

La figura 3 ilustra un primer estado en el que un aparato de encriptación puede cargar un condensador usando una carga suministrada desde una fuente de alimentación externa según una realización de la presente invención.

La figura 4 ilustra un segundo estado en el que un aparato de encriptación puede ejecutar un algoritmo de encriptación usando una carga almacenada en un condensador según una realización de la presente invención.

La figura 5 ilustra un tercer estado en el que un aparato de encriptación puede descargar un condensador hasta un nivel predeterminado y/o descargarlo completamente después de que se ejecute un algoritmo de encriptación según una realización de la presente invención.

Mejor modo de llevar a cabo la invención

Ahora se hará referencia con detalle a realizaciones de la presente invención, de las que se han ilustrado ejemplos en los dibujos que se acompañan, en donde las mismas referencias numéricas se refieren a elementos iguales a través de los mismos. Las realizaciones se describen a continuación a efectos de explicar la presente invención mediante referencia a las figuras.

La figura 1 ilustra un aparato de encriptación 100 según una realización de la presente invención.

El aparato de encriptación 100 puede incluir un modulo de encriptación 110, y un módulo de control 200. El módulo de encriptación 110 puede ejecutar un algoritmo con la recepción de una carga suministrada por el módulo de control 200. El módulo de control 200 puede estar conectado a un nodo VDD y a un nodo de tierra (GND), y puede recibir una carga alimentada por una fuente de alimentación externa, y puede suministrar la carga recibida al modulo de encriptación 110 por medio de un método de operación que se describirá más adelante.

El módulo de encriptación 110 puede que no se haya construido para limitarse a una configuración o un algoritmo de un circuito de encriptación específico. En consecuencia, a menos que se mencione lo contrario, el módulo de encriptación 110 puede incluir varias configuraciones bien conocidas para ejecutar un algoritmo de encriptación usando una clave de encriptación.

Según se muestra en la figura 1, conforme a realizaciones de la presente invención, una corriente I_{VDD} que es la entrada desde un nodo VDD que alimenta una corriente al aparato de encriptación 100, puede tener un valor constante, con independencia de que la clave de encriptación esté operada por el módulo de encriptación 110. Una corriente I_{GND} que constituye la salida desde el aparato de encriptación 100 hasta un nodo de GND puede tener también un valor constante, con independencia de que la clave de encriptación esté operada por el módulo de encriptación 110. En consecuencia, un ataque de análisis de potencia usando un esquema no invasivo, puede ser impedido de una manera efectiva.

De acuerdo con una tecnología convencional, el aparato de encriptación 100 puede tener otra conexión física a un sistema externo, adicionalmente al nodo VDD y al nodo GND, en realidad, con independencia de un diseño previsto.

En particular, el nodo GND puede ser un nodo común entre el aparato de encriptación 100 y otros circuitos externos. En consecuencia, cuando se abre una conexión entre el aparato de encriptación 100 y el nodo VDD de tal modo que $I_{VDD} = 0$, la corriente de salida I_{GND} puede no corresponder exactamente con 0.

De acuerdo con la tecnología convencional, una posibilidad de ataque de análisis de potencia mediante sondeo de la tensión del nodo GND, o mediante medición de I_{GND} de un nivel preciso, no puede ser excluida por completo.

Sin embargo, de acuerdo con realizaciones de la presente invención, cuando la conexión entre el aparato de encriptación 100 y el nodo VDD está abierta, se puede abrir también una conexión entre el aparato de encriptación 100 y el nodo GND. En consecuencia, se puede bloquear la posibilidad de ataque de análisis de potencia a través de un sondeo de la tensión en el nodo GND mientras se ejecuta el algoritmo de encriptación.

Una configuración del aparato de encriptación 100 y un método de operación del mismo van a ser descritos con detalle con referencia a la figura 2 y a los dibujos subsiguientes.

La figura 2 ilustra un ejemplo detallado del aparato de encriptación 100 de acuerdo con una realización de la presente invención.

El módulo de control 200 puede incluir una primera unidad de transferencia de carga 210, una unidad de almacenaje de carga 220, y una segunda unidad de transferencia de carga 230.

La primera unidad de transferencia de carga 210 puede incluir un conmutador S11 para determinar si la conexión entre el aparato de encriptación 100 y el nodo VDD debe estar cerrada o abierta, y un conmutador S12 para determinar si la conexión entre el aparato de encriptación 100 y el nodo GND debe estar cerrada o abierta.

En este caso, el conmutador S11 y el conmutador S12 pueden ser activados simultáneamente. Cuando la conexión entre el aparato de encriptación 100 y el nodo VDD se abre, la conexión entre el aparato de encriptación 100 y el nodo GND puede estar abierta por completo.

La unidad de almacenaje de carga 220 puede incluir un condensador C22 para almacenar una carga recibida desde la primera unidad de transferencia de carga 210, y un conmutador de derivación S21 para descargar el condensador C22, según sea necesario.

La segunda unidad de transferencia de carga 230 puede incluir un conmutador S31 y un conmutador S32 como partes que pueden transferir una corriente para ser usada en la operación del módulo de encriptación 110, desde la unidad de almacenaje de carga 220 hasta el módulo de encriptación 110.

El conmutador S31 y el conmutador S32 pueden ser accionados simultáneamente. Cuando el conmutador S31 y el conmutador S32 están abiertos, un nodo entre el módulo de encriptación 110 y la segunda unidad de transferencia de carga 230 en el aparato de encriptación 100 puede estar completamente abierto.

Cada elemento ilustrado en forma de circuito puede estar implementado por varios módulos de circuito o dispositivos que puedan ser implementables en realidad. Por ejemplo, los conmutadores de acuerdo con una realización de la presente invención pueden ser implementados por medio de varios dispositivos bien conocidos, por ejemplo, un conmutador de semiconductor de óxido metálico complementario (CMOS), y similares.

Una serie de operaciones para recibir una carga suministrada por una fuente de alimentación externa a través del nodo VDD y del nodo GND, y que realizan un algoritmo de encriptación usando la carga suministrada en el aparato de encriptación 100, pueden ser llevadas a cabo secuencialmente, y pueden ser clasificadas en tres estados, los cuales pueden ser iterados como necesarios.

Los tres estados pueden incluir un primer estado S1 en el que la primera unidad de transferencia de carga 210 puede transferir la carga suministrada por la fuente de alimentación externa hasta la unidad de almacenaje de carga 220 para cargar el condensador C22, un segundo estado S2 en el que la segunda unidad de transferencia de carga 230 puede transferir la carga almacenada en el condensador C22 al módulo de encriptación 110, y el algoritmo de encriptación puede ser ejecutado, y un tercer estado S3 en el que el condensador C22 puede ser descargado.

El primer estado S1, el segundo estado S2 y el tercer estado S3 pueden constituir un único ciclo de ejecución del algoritmo de encriptación, y el primer estado S1, el segundo estado S2 y el tercer estado S3 pueden ser iterados en base al ciclo, según sea necesario, por ejemplo en el orden S1 – S2 – S3 – S1 - ...

Las operaciones de la primera unidad de transferencia de carga 210, de la unidad de almacenaje de carga 220 y de la segunda unidad de transferencia de carga 220 en cada uno de entre el primer estado S1, el segundo estado S2 y el tercer estado S3, van a ser mejor descritas con referencia a las figuras 3 a 5.

La figura 3 ilustra el primer estado S1 en el que el aparato de encriptación 100 de la figura 1 puede cargar el condensador C22 de la figura 2 usando una carga suministrada de acuerdo con una realización de la presente invención.

En el primer estado S1, la primera unidad de transferencia de carga 210 puede transferir una carga suministrada por la fuente de alimentación externa al condensador C22 de la unidad de almacenaje de carga 220, para cargar el condensador C22.

En el primer estado S1, aunque el conmutador S11 y el conmutador S12 puedan estar cerrados para cargar el condensador C22, el conmutador S31 y el conmutador S32 pueden estar abiertos para desconectar el módulo de encriptación 110 de la parte exterior del aparato de encriptación 100. Es decir, en el primer estado S1, la segunda unidad de transferencia de carga 230 puede bloquear una conexión entre la unidad de almacenaje de carga 220 y el módulo de encriptación 110.

En este caso, el condensador C22 puede estar constantemente en estado de descarga completa. En consecuencia, la corriente i_{VDD} suministrada por la fuente de alimentación externa puede ser determinada en base solamente a la capacitancia del condensador C22. Es decir, la corriente i_{VDD} alimentada por la fuente de alimentación externa puede ser completamente ajena a un valor de una clave de encriptación del módulo de encriptación 110 que se ejecuta en un estado anterior.

La figura 4 ilustra el segundo estado S2 en el que el aparato de encriptación 100 de la figura 1 puede ejecutar un algoritmo de encriptación usando una carga usada para cargar el condensador C22 de acuerdo con una realización de la presente invención.

En el segundo estado S2, la primera unidad de transferencia de carga 210 puede desconectar completamente la unidad de almacenaje de carga 220 de la parte exterior del aparato de encriptación 100. Según se muestra en la figura 4, el conmutador S11 y el conmutador S12 pueden ser abiertos simultáneamente, y la unidad de almacenaje de carga 220 en el aparato de encriptación 100 puede estar completamente separada tanto del nodo VDD como del nodo GND, es decir, dos nodos de la fuente de alimentación externa.

En el segundo estado S2, la unidad de almacenaje de carga 220 puede suministrar una carga al módulo de encriptación 110 a través de la segunda unidad de transferencia de carga 230, y el módulo de encriptación 110 puede ejecutar el algoritmo de encriptación usando la carga suministrada.

Durante el proceso de encriptación, una cantidad de carga consumida por el módulo de encriptación 110, es decir, una cantidad de corriente, puede ser dependiente del valor de una clave de encriptación. Sin embargo, puesto que la parte exterior del aparato de encriptación 100, por ejemplo, el nodo NDD y el nodo GND de la figura 2, puede ser desconectada del módulo de encriptación 110, puede resultar imposible un ataque de análisis de potencia.

Una carga residual después de la alimentación del módulo de encriptación 110 puede estar aún presente en el condensador C22. Puesto que la carga residual puede corresponder a una cantidad de carga que permanece tras ser usada en el módulo de encriptación 110, la carga residual puede ser dependiente del valor de la clave de encriptación. Por consiguiente, cuando la carga residual se descarga directamente en el nodo GND, un ataque de análisis de potencia puede resultar posible midiendo la corriente i_{VDD} que circula a través del nodo GND. De ese modo, con el fin de evitar el ataque de análisis de potencia, el primer estado S1 para la recarga puede avanzar después de que se descargue la carga residual mediante disipación y radiación térmica, cortocircuitando ambos extremos del condensador C22, en vez de descargando la carga residual en el nodo GND.

La figura 5 ilustra el tercer estado S3 en el que el aparato de encriptación de la figura 1 puede descargar el condensador C22 hasta un nivel predeterminado y/o descargarlo completamente después de que se ejecute un algoritmo de encriptación de acuerdo con una realización de la presente invención.

En el tercer estado S3, se puede descargar una carga residual del condensador C22 hasta el nivel predeterminado y/o descargarlo completamente después de que se haya ejecutado el algoritmo de encriptación.

En el tercer estado S3, el conmutador de derivación S21 puede ser cerrado para descargar el condensador C22. La descarga puede ser determinada en base a un componente de resistencia (no representado) entre el conmutador de derivación S21 y el condensador C22, y una capacitancia del condensador C22. Sin embargo, puesto que la descarga puede ser llevada a cabo en un período de tiempo extremadamente corto, la descarga puede ser completada hasta un nivel predeterminado en el que un análisis de potencia sea imposible, con anterioridad a que se inicie un primer estado S1 de un ciclo posterior. El nivel predeterminado puede ser entendido como un nivel en el que pueda ser imposible un ataque de análisis de potencia.

En el tercer estado S3, la primera unidad de transferencia de carga 210 puede desconectar la unidad de almacenaje de carga 220 de la fuente de alimentación externa, y la segunda unidad de transferencia de carga 230 puede desconectar la unidad de almacenaje de carga 220 del módulo de encriptación 110.

Dependiendo de las realizaciones, se puede añadir una operación de apertura de todos los conmutadores a una transición de estado de cada estado de entre el primer estado S1, el segundo estado S2, y el tercer estado S3, de modo que los estados no puedan solaparse entre sí. Se pueden ampliar varias realizaciones con respecto a otras operaciones para evitar el ataque de análisis de potencia.

Según se ha descrito con anterioridad, la corriente i_{VDD} que va a ser introducida a través del nodo VDD que alimenta

corriente al aparato de encriptación 100 puede tener un valor constante, con independencia de una clave de encriptación que va a ser operada por el módulo de encriptación 110, y la corriente i_{GND} que va a estar presente en la salida del aparato de encriptación 100 para el nodo GND puede tener también un valor constante, con independencia de la clave de encriptación que va a ser operada por el modulo de encriptación 110.

Por consiguiente, el ataque de análisis de potencia puede ser impedido de forma efectiva mientras se ejecuta el algoritmo de encriptación, y/o en diversos estados, por ejemplo, mientras la unidad de almacenaje de carga 220 recibe una carga suministrada por la fuente de alimentación externa, y similares.

Los ejemplos de realización de la presente invención descritos en lo que antecede pueden estar grabados en medios legibles con ordenador que incluyan instrucciones de programa para implementar diversas operaciones materializadas mediante un ordenador. Los medios pueden incluir también, solos o en combinación con las instrucciones de programa, archivos de datos, estructuras de datos, y similares. Ejemplos de medios legibles con ordenador incluyen medios magnéticos tales como discos duros, discos flotantes, y cinta magnética; medios ópticos tales como discos CD ROM y DVDs; medios magneto-ópticos tales como discos floptical; y dispositivos de hardware que estén específicamente configurados para almacenar y ejecutar instrucciones de programa, tal como memoria de solo lectura (ROM), memoria de acceso aleatorio (RA), memoria flash, y similares. Ejemplos de instrucciones de programa incluyen tanto código máquina, tal como el producido por un compilador, como archivos que contengan un código de nivel superior que pueda ser ejecutado mediante el ordenador usando un intérprete. Los dispositivos de hardware descritos pueden estar configurados para que actúen como uno o más módulos de software con el fin de realizar las operaciones de los ejemplos de realizaciones de la presente invención descritos con anterioridad, o viceversa.

Aunque se han mostrado y descrito unas pocas realizaciones de la presente invención, la presente invención no se limita a las realizaciones descritas. Por el contrario, los expertos en la materia podrán apreciar que se pueden hacer cambios en esas realizaciones sin apartarse de los principios de la invención, cuyo alcance se define mediante las reivindicaciones y sus equivalentes.

REIVINDICACIONES

1.- Un aparato de encriptación, que comprende:

un módulo de encriptación para ejecutar un algoritmo de encriptación,

un módulo de control adaptado para transferir, al módulo de encriptación, una carga suministrada por una fuente de alimentación externa mediante el control de una trayectoria de paso de corriente entre el módulo de encriptación y la fuente de alimentación externa, al menos en un período de tiempo anterior a que se ejecute el algoritmo de encriptación y en un período de tiempo durante el cual se ejecuta el algoritmo de encriptación;

caracterizado porque el control de una trayectoria de paso de corriente entre el módulo de encriptación y la fuente de alimentación externa comprende desconectar un terminal de tierra del módulo de encriptación de un terminal de tierra de la fuente de alimentación externa en el período de tiempo durante el que se ejecuta el algoritmo de encriptación.

2.- El aparato de encriptación conforme a la reivindicación 1, en el que el módulo de control comprende:

una primera unidad de transferencia de carga para recibir carga suministrada por la fuente de alimentación externa, en un primer estado correspondiente a un período de tiempo anterior a que se ejecute el algoritmo de encriptación;

una unidad de almacenaje de carga para almacenar una carga recibida y transferida por la primera unidad de transferencia de carga, en el primer estado, y

una segunda unidad de transferencia de carga para transferir la carga almacenada en la unidad de almacenaje de carga al módulo de encriptación, en un segundo estado correspondiente a un período de tiempo durante el que se ejecuta el algoritmo de encriptación.

3.- El aparato de encriptación conforme a la reivindicación 2, en el que la primera unidad de transferencia de carga está adaptada para desconectar un terminal de tierra del módulo de encriptación de un terminal de tierra de la fuente de alimentación externa, en el segundo estado.

4.- El aparato de encriptación de la reivindicación 1, en el que el módulo de encriptación está conectado a un nodo de tierra separado, diferente del nodo de tierra de la fuente de alimentación externa.

5.- El aparato de encriptación de la reivindicación 2, en el que la unidad de almacenaje de carga comprende:

un condensador para almacenar una carga.

6.- El aparato de encriptación de la reivindicación 5, en el que la primera unidad de transferencia de carga comprende:

un primer conmutador para cerrar o abrir una conexión eléctrica entre un nodo VDD correspondiente a un ánodo de la fuente de alimentación externa y un primer terminal del condensador, y

un segundo conmutador, accionado con el primer conmutador, simultáneamente, para cerrar o abrir una conexión eléctrica entre un GND correspondiente a un nodo de tierra de la fuente de alimentación externa y un segundo terminal del condensador.

7.- El aparato de encriptación de la reivindicación 5, en el que la segunda unidad de transferencia de carga comprende:

un tercer conmutador para cerrar o abrir una conexión eléctrica entre un primer terminal del condensador y un primer terminal del módulo de encriptación, y

un cuarto conmutador, accionado con el tercer conmutador, simultáneamente, para cerrar o abrir una conexión eléctrica entre un segundo terminal del condensador y un segundo terminal del módulo de encriptación.

8.- El aparato de encriptación de la reivindicación 5, en el que la unidad de almacenaje de carga comprende además:

un quinto conmutador, para ser cerrado en un tercer estado correspondiente a un período de tiempo posterior a que se ejecute el algoritmo de encriptación y correspondiente a un periodo de tiempo anterior a que se ejecute un algoritmo de encriptación separado siguiente al algoritmo de encriptación, para descargar el condensador incluido en la unidad de almacenaje de carga.

9.- El aparato de encriptación de la reivindicación 8, en el que el quinto conmutador está adaptado para descargar el condensador cortocircuitando dos terminales del condensador.

10.- Un método de operación de un aparato de encriptación que incluye un módulo de encriptación para ejecutar un algoritmo de encriptación, comprendiendo el método:

controlar una trayectoria de paso de corriente entre el módulo de encriptación y una fuente de alimentación externa al menos en un período de tiempo anterior a que se ejecute el algoritmo de encriptación y en un período de tiempo durante el que se ejecuta el algoritmo de encriptación, para transferir al módulo de encriptación una carga suministrada por la fuente de alimentación externa;

en el que controlar una trayectoria de paso de corriente entre el módulo de encriptación y la fuente de alimentación externa comprende desconectar un terminal de tierra del módulo de encriptación de un terminal de tierra de la fuente de alimentación externa, en el período de tiempo durante el que se ejecuta el algoritmo de encriptación.

11.- El método de operación conforme a la reivindicación 10, comprendiendo el método:

almacenar, mediante una primera unidad de transferencia de carga incluida en el aparato de encriptación, carga suministrada por una fuente de alimentación externa en una unidad de almacenaje de carga incluida en el aparato de encriptación, en un primer estado correspondiente a un período de tiempo anterior a que se ejecute el algoritmo de encriptación, y

transferir, mediante una segunda unidad de transferencia de carga incluida en el aparato de encriptación, una carga almacenada en la unidad de almacenaje de carga al módulo de encriptación, y ejecutar, mediante el módulo de encriptación, el algoritmo de encriptación, en un segundo estado correspondiente a un período de tiempo durante el que se ejecuta el algoritmo de encriptación.

12.- El método de operación conforme a la reivindicación 11, comprendiendo además el método:

descargar, mediante la unidad de almacenaje de carga, un dispositivo de almacenamiento de carga incluido en una porción interna de la unidad de almacenaje de carga que almacena una carga, en un tercer estado correspondiente a un período de tiempo posterior a que se ejecute el algoritmo de encriptación.

FIG. 1

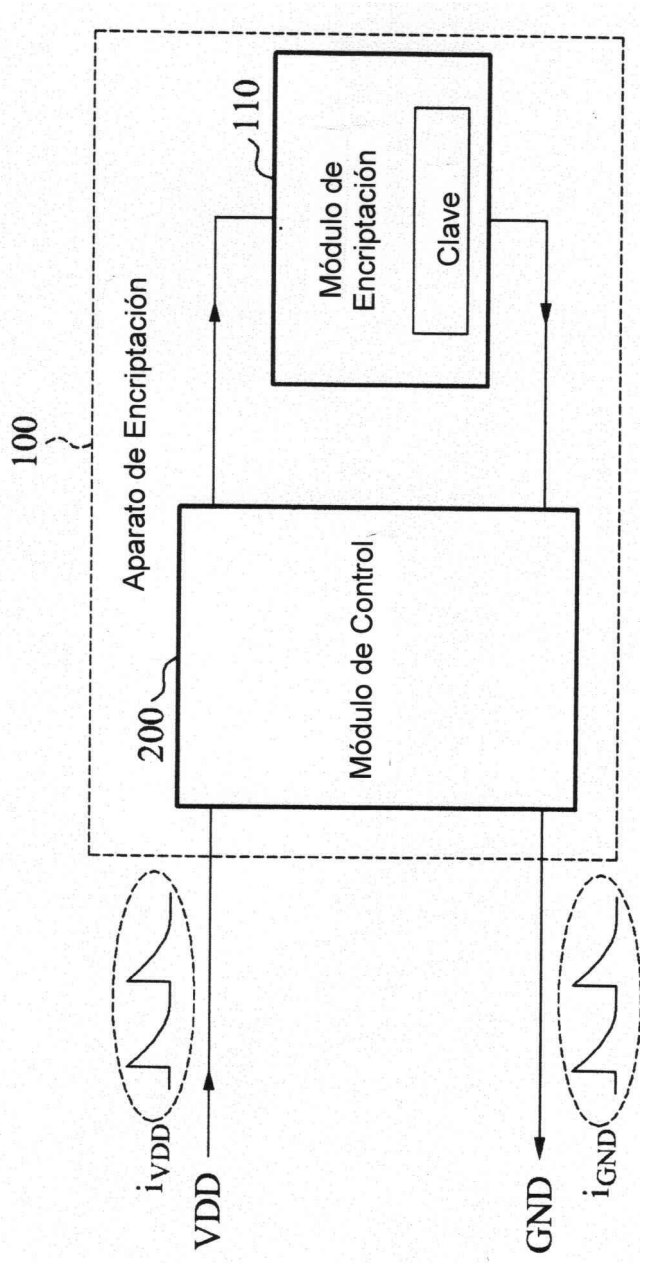

100
Aparato de Encriptación
110
Módulo de Encriptación
Clave
200
Módulo de Control
i_{VDD}
VDD
GND
i_{GND}

FIG. 2

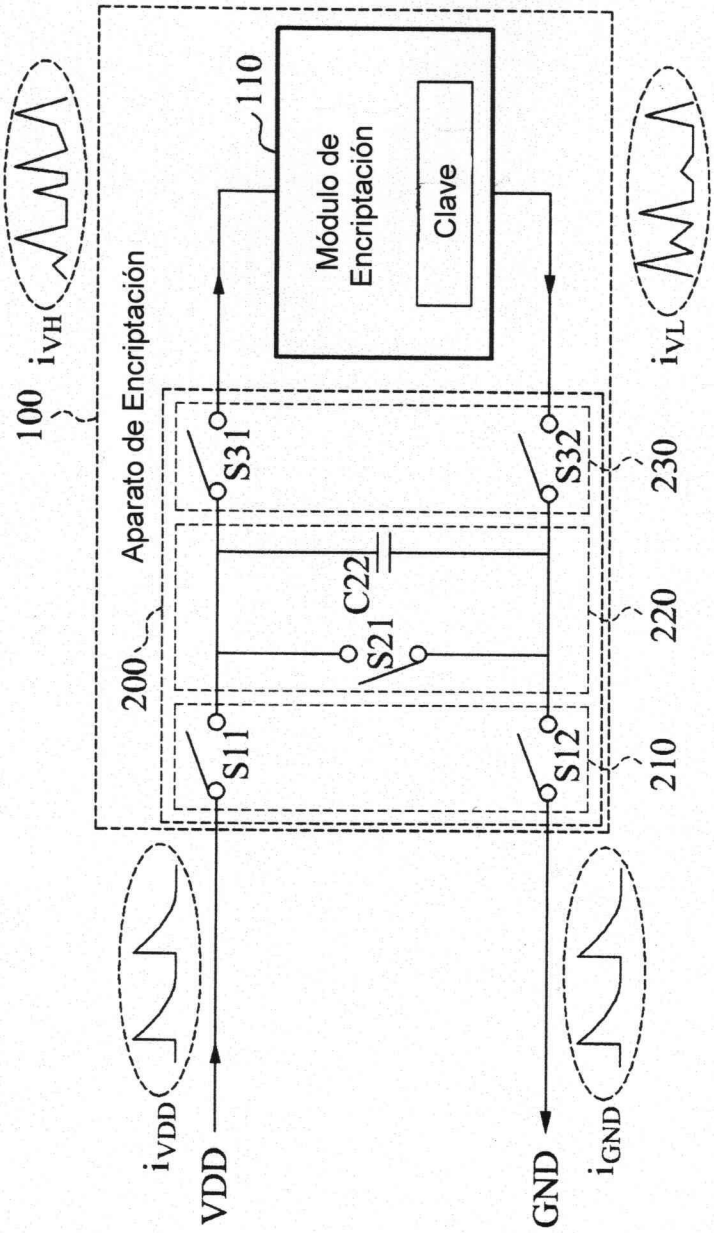

100
Aparato de Encriptación
200
110
Módulo de Encriptación
Clave
i_{VH}
i_{VL}
i_{VDD}
i_{GND}
VDD
GND
S11
S12
S21
S31
S32
C22
210
220
230

FIG. 3

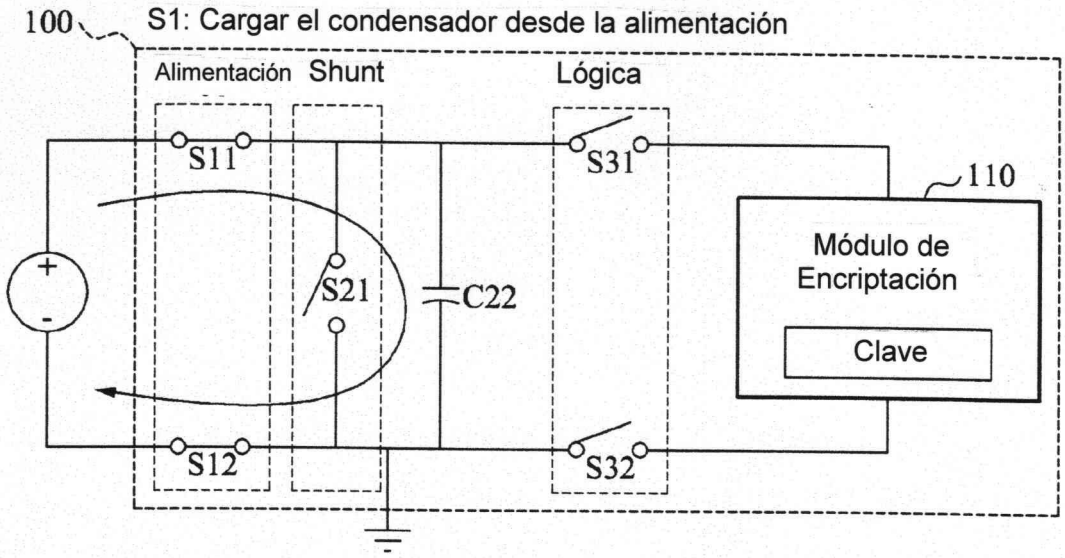

100
S1: Cargar el condensador desde la alimentación
Alimentación
Shunt
Lógica
S11
S21
C22
S31
110
Módulo de Encriptación
Clave
S12
S32
+
-

FIG. 4

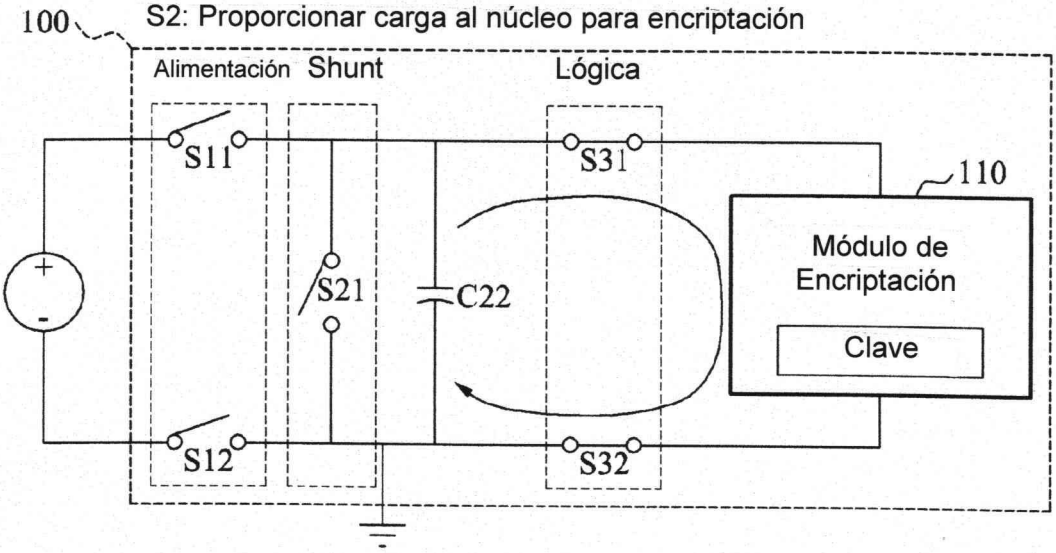
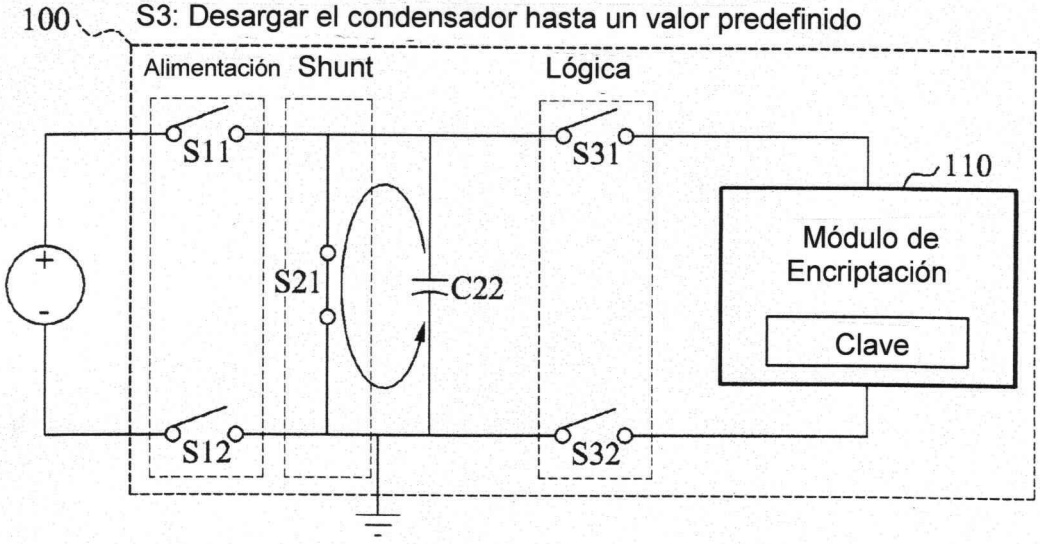

100
S2: Proporcionar carga al núcleo para encriptación
Alimentación
Shunt
Lógica
S11
S21
C22
S31
110
Módulo de Encriptación
Clave
S12
S32
+
-

FIG. 5


100
S3: Desargar el condensador hasta un valor predefinido
Alimentación
Shunt
Lógica
S11
S21
C22
S31
110
Módulo de Encriptación
Clave
S12
S32