(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 777 526**

(51) Int. CI.:

G09C 1/10 (2006.01)
H04L 9/06 (2006.01)
H04L 9/08 (2006.01)
H03K 19/177 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **11.05.2015 PCT/EP2015/060318**

(87) Fecha y número de publicación internacional: **18.02.2016 WO16023650**

(96) Fecha de presentación y número de la solicitud europea: **11.05.2015 E 15724192 (8)**

(97) Fecha y número de publicación de la concesión europea: **11.12.2019 EP 3146520**

(54) Título: **Componente lógico programable, circuito de formación de claves y procedimiento para proporcionar una información de seguridad**

(30) Prioridad:

11.08.2014 DE 102014215898

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.08.2020

(73) Titular/es:

SIEMENS MOBILITY GMBH (100.0%)
Otto-Hahn-Ring 6
81739 München, DE

(72) Inventor/es:

FALK, RAINER y
MERLI, DOMINIK

(74) Agente/Representante:

LOZANO GANDIA, José

DESCRIPCIÓN

Componente lógico programable, circuito de formación de claves y procedimiento para proporcionar una información de seguridad

La invención se refiere a un componente lógico programable que está programado para generar una información de seguridad que se refiere a una clave criptográfica, un circuito de formación de claves correspondiente, un procedimiento correspondiente para proporcionar una información de seguridad en un componente lógico programable y un producto de programa informático.

Los componentes lógicos programables se usan actualmente en muchos sistemas informáticos para poder ejecutar funcionalidades muy rápidamente y para poder cambiar o adaptar de manera flexible la funcionalidad o una interconexión subyacente sin tener que cambiar directamente el hardware. Como componentes lógicos se usan en particular, las matrices de puertas lógicas programables en campo, también llamadas FPGA. Un componente lógico programable semejante contiene diferentes bloques configurables, como registros, que se implementan mediante flip-flops, lógica combinatoria, que se implementan mediante tablas, las llamadas tablas de búsqueda, memorias, bloques de entrada / salida, generadores de reloj y otros.

Un componente lógico programable semejante se puede configurar por medio de un flujo de bits, es decir, los circuitos se establecen en el componente lógico mediante el flujo de bits. El término flujo de bits se usa en este documento con el mismo significado que el término técnico inglés "*bitstream*". Un flujo de bits generalmente se carga en el componente lógico desde un módulo de memoria cuando se inicia un sistema, por ejemplo, un sistema informático. Este se configura en función del flujo de bits cargado. No obstante, también se conocen módulos lógicos que almacenan sus datos de configuración internamente. Para este propósito, está prevista una memoria de configuración en el componente lógico, por ejemplo, una memoria flash o una memoria antifusible. Mediante un componente lógico programable semejante también se pueden implementar los cálculos criptográficos, por ejemplo, procedimientos de encriptación simétricos, como un estándar de encriptación ampliado AES, o funciones unidireccionales, como HMAC-SHA256. Estos procedimientos criptográficos requieren como parámetro una información de seguridad, en particular una clave criptográfica, que debe estar disponible dentro del componente lógico programable.

El documento DE 10 2010 026688 A1 describe un procedimiento y un generador aleatorio para generar bits aleatorios con una alta entropía. El generador aleatorio se compone de al menos un oscilador de anillo en cascada, que se puede componer de puertas conmutadas cíclicamente, y un dispositivo de exploración que explora los estados de conmutación del oscilador de anillo en cascada para generar los bits aleatorios.

El documento US 2014/016778 A1 describe un procedimiento y un generador de flujo de bits aleatorio para generar una clave continua para una encriptación de flujo o para el uso como un generador de números pseudo-aleatorio.

El documento US 2006/098820 A1 describe un procedimiento para generar un flujo de claves. Para este propósito, un generador de flujo de clave recibe un flujo de bits de entrada continuo, que mediante el generador de flujo de bits de claves procesa en un flujo de bits de salida emitido continuo.

Sin embargo, esta información de seguridad no se tiene que poder leer a partir del flujo de bits con medios simples durante la configuración, ya que de lo contrario un atacante puede descifrar sin problemas un flujo de datos encriptación en base a la información de seguridad o la clave criptográfica.

Para evitar que se lea dicha información de seguridad criptográfica, se conoce cargar el flujo de bits en el componente lógico programable solo en forma encriptada criptográficamente. Sin embargo, también existen componentes lógicos programables que no soportan flujos de bits encriptados. Una encriptación semejante de flujo de bits, en particular en el caso de algunos módulos FPGA, se puede romper por un ataque de canal lateral. También se conoce leer un flujo de bits desde un módulo lógico con una memoria de configuración interna. Un flujo de bits se puede analizar entonces mediante ingeniería inversa, denominada *Reverse Engineering*, para determinar luna información de seguridad contenida en el mismo.

También se conoce concebir un circuito digital de modo que solo funcione correctamente en función de una clave. Por ejemplo, en una máquina automática de estados, un modo funcional normal solo se activa al aplicar una clave correcta.

Para obtener una lectura de la clave o una indicación de la clave criptográfica cuando se programa un componente lógico programable, igualmente se conoce expandir un circuito lógico con estado en una pluralidad de estados no funcionales y determinar un estado de inicio individualmente para los componentes. Solo el diseñador del circuito puede construir una secuencia de estados que conduzca desde el estado de inicio individual para los componentes a un estado desde el que se logra la funcionalidad esperada.

Las distintas medidas conocidas solo están limitadas a ciertos módulos lógicos programables o, a su vez, requieren

una clave para la activación.

Por lo tanto, el objeto de la presente invención es hacer que esté disponible una información de seguridad o una clave criptográfica dentro de un componente lógico programable de una manera semejante para el cálculo criptográfico, de modo que una lectura de la clave del flujo de bits solo sea posible con gran esfuerzo. En particular, una clave criptográfica o también una información de seguridad que se refiere la clave criptográfica debería ser difícil de determinar mediante ingeniería inversa, también llamada *Reverse Engineering*.

El objetivo se consigue mediante las medidas descritas en las reivindicaciones independientes. En las reivindicaciones dependientes están representados perfeccionamientos ventajosos de la invención.

El componente lógico programable según la invención está programado para presentar un circuito de formación de claves que genera una información de seguridad, que se refiere a una clave criptográfica, en el tiempo de ejecución y que se puede proporcionar a una unidad criptográfica como parámetro de entrada, donde la generación de la información de seguridad (K) se realiza utilizando los datos de inicialización que están contenidos en el flujo de bits.

La unidad criptográfica puede ser implementada como parte del componente lógico programable. Por lo tanto, se puede situar en el mismo componente lógico programable que el circuito de formación de claves. En principio, no obstante, también es posible que una clave formada se le proporcione a una unidad criptográfica externa.

La información de seguridad puede presentar, por ejemplo, una anchura de 64 bits, 128 bits, 256 bits, 384 bits, 512 bits. La generación comprende al menos una operación lógica que se realiza mediante un circuito lógico configurable del componente lógico. La generación de la información de seguridad se realiza preferentemente de manera determinista por medio de operaciones lógicas y/o registros. Además, la generación de la información de seguridad se realiza preferentemente sin usar los datos de inicialización o sin usar datos de inicialización que están contenidos en el flujo de bits.

Un componente lógico programable correspondiente puede ser, por ejemplo, una matriz de puertas programable en campo, también llamada FPGA. El circuito de formación de claves es una estructura funcional que está fijada por la programación de bloques universales individuales en el componente lógico programable y su interconexión entre sí. La información de seguridad generada puede ser, por un lado, una clave criptográfica o un parámetro o una información a partir de la que se genera la clave criptográfica mediante pasos de procesamiento adicionales. La información de seguridad solo se genera en el tiempo de ejecución del componente lógico programable, es decir, tan pronto como se aplica corriente al componente lógico o se activa el componente lógico.

Un componente lógico programable correspondiente tiene la ventaja de que un circuito de formación de claves se implementa con relativa facilidad y solo pocos requiere recursos en el componente lógico. Sin embargo, incluso a partir de un flujo de bits disponible para el atacante o un producto de programa informático correspondiente que contenga el flujo de bits, una clave oculta en el mismo según la invención solo se puede extraer con un esfuerzo extremadamente grande. Esto se debe a que la información de seguridad generada no está contenida directamente en el flujo de bits. Un atacante tendría que determinar la funcionalidad lógica que se implementa mediante el flujo de bits para un ataque exitoso. Esto solo es posible con un esfuerzo extremadamente grande.

En una forma de realización ventajosa, el circuito de formación de claves comprende un circuito lógico sin estado, que está concebido en particular como un circuito lógico combinatorio.

Un circuito de formación de claves semejante proporciona una información de seguridad dentro del componente lógico, por ejemplo en un bloque de encriptación o un bloque de derivación de clave. Un circuito lógico combinatorio o sin estado proporciona el circuito de formación de claves directamente cuando se activa el componente lógico. Por lo tanto, la información de seguridad está disponible para un uso posterior muy pronto después de la activación del componente lógico.

En una variante del componente lógico programable según la invención, el circuito de formación de claves comprende un circuito lógico con estado.

Un circuito lógico con estado semejante puede ser implementado, por ejemplo, como una máquina automática de estados. Esto tiene la ventaja de que se genera un valor de salida en un circuito lógico con estado, por ejemplo, al ocurrir o al abandonar un estado. Por lo tanto, no es directamente necesario un valor de inicialización, que se requiere para iniciar o ejecutar el circuito lógico. Por lo tanto, esta información no se tiene que proporcionar y por lo tanto aumenta la seguridad de la información de seguridad generada.

En una forma de realización ventajosa, el circuito de formación de claves comprende una combinación de circuitos lógicos sin estado y con estado.

Mediante una combinación de circuitos lógicos sin estado y con estado se puede adaptar el circuito de formación

de claves de manera muy flexible a los requisitos específicos de una aplicación.

En un ejemplo de realización ventajoso, un valor de inicialización del circuito de formación de claves está presente de una manera fija predeterminada o un valor de inicialización solo se forma antes de su uso en el circuito de formación de claves.

Si un valor de inicialización del circuito de formación de claves está presente de una manera fija predeterminada, entonces la información de seguridad se puede proporcionar muy rápidamente. Si se forma primero un valor de inicialización, por ejemplo, en el componente lógico antes de su uso en el circuito de formación de claves, entonces el valor de inicialización no está contenido directamente en el flujo de bits y, por lo tanto, no se puede leer.

En un ejemplo de realización, el circuito de formación de claves está concebido para proporcionar la información de seguridad solo durante un período predeterminado de tiempo y/o después de un número predeterminado específico de ciclos de reloj.

Esto tiene la ventaja de que se puede generar una información de seguridad diferente en diferentes momentos o después de un número diferente de ciclos de reloj, y por lo tanto, mediante un componente lógico programable se puede proporcionar una información de seguridad múltiple, por ejemplo, para diferentes aplicaciones. Además, un atacante debe saber la hora o el período de tiempo para poder acceder a la información de seguridad.

En una forma de realización del componente lógico programable, el circuito de formación de claves está concebido para generar y emitir solo una parte de la información de seguridad respectivamente en un momento.

Esto tiene la ventaja de que la información de seguridad completa no está presente en ningún momento en el componente lógico o en el circuito de formación de claves. Esto es posible en particular en interacción con, por ejemplo, un algoritmo AES, cuya programación de clave interna solo utiliza una parte de la clave AES en una ronda.

En otra variante, el circuito de formación de claves está concebido para generar diferentes partes de la información de seguridad en base a diferentes valores de inicialización.

Por lo tanto, el valor de inicialización completo para formar toda la información de seguridad no está disponible en ningún momento. Un atacante primero debe reconocer los diferentes valores de inicialización para las partes de la información de seguridad y aplicarlos en el orden correcto para obtener toda la información de seguridad.

En una forma de realización ventajosa, el circuito de formación de claves está concebido para generar la información de seguridad o las partes de la información de seguridad de manera cambiada por un parámetro de enmascaramiento.

Esto tiene la ventaja de que incluso una lectura del valor de salida aún no representa la información de seguridad en sí o partes de la información de seguridad en sí. Se necesitan más pasos de desenmascaramiento, es decir, las reglas de vinculación entre la información de seguridad y los parámetros de enmascaramiento, y el conocimiento de los parámetros de enmascaramiento en sí para obtener la información de seguridad real. Por ejemplo, una operación OR exclusiva, una operación de suma o una operación de multiplicación se pueden usare como la operación de enmascaramiento.

En una variante del componente lógico mencionado anteriormente, el circuito de formación de claves está concebido para cambiar dinámicamente los parámetros de enmascaramiento.

Esto dificulta considerablemente una decodificación o enmascaramiento del valor de salida del circuito de formación de claves y, por lo tanto, la obtención de la información de seguridad en el texto sin formato.

En una variante, el circuito de formación de claves está concebido para generar la información de seguridad solo a demanda.

Esto tiene la ventaja de que, en el caso de una ingeniería inversa, la señal que dispara una solicitud también se debe reconocer.

En otra variante, el circuito de formación de claves está concebido para proporcionar un identificador de disponibilidad cuando está preparada una información de seguridad válida para la emisión.

Esto igualmente dificulta el reconocimiento y la lectura de una información de seguridad válida como tal.

En una forma de realización ventajosa, el circuito de formación de claves está concebido para proporcionar una información de seguridad distinta para diferentes aplicaciones en distintos momentos.

Esto tiene la ventaja de que mediante el mismo componente lógico se puede proporcionar una pluralidad de información de seguridad en muy poco tiempo.

En una forma de realización ventajosa, el componente lógico programable comprende adicionalmente una unidad criptográfica.

Por lo tanto, la información de seguridad se puede usar en el mismo componente lógico y se puede llevar a cabo un procedimiento de encriptación a partir de ella. Debido a la interfaz interna del componente lógico para transferir la información de seguridad al elemento criptográfico es extremadamente difícil una lectura o acceso a la información de seguridad.

En una forma de realización ventajosa, el flujo de bits contiene información de marca de agua oculta y el circuito de formación de claves proporciona la información de marca de agua después de un número de ciclos de reloj para formar una información de seguridad.

Esto aprovecha una marca de agua para la transmisión velada de información de seguridad, y el circuito de formación de claves solo se utiliza para extraer la marca de agua del flujo de bits.

Además, se reivindica un circuito de formación de claves para generar y proporcionar una información de seguridad, que se refiere a una clave criptográfica, que está concebida según las características mencionadas anteriormente del componente lógico programable.

También se reivindica un procedimiento para proporcionar una información de seguridad que se refiere a una clave criptográfica en un componente lógico programable, cuyo circuito lógico se programa por un flujo de bits y está concebido según las características mencionadas anteriormente. El procedimiento comprende, como pasos del procedimiento, una transmisión de un circuito de formación de claves a través de un flujo de bits al componente lógico, una generación de la información de seguridad por medio de la ejecución del circuito de formación de claves en el componente lógico y una facilitación de la información de seguridad como parámetros de entrada para una unidad criptográfica, donde la generación de la información de seguridad (K) se realiza utilizando los datos de inicialización que están contenidos en el flujo de bits.

Además, se reivindica un producto de programa informático que genera un flujo de bits para cargar en un componente lógico programable y el flujo de bits está concebido para configurar un circuito de formación de claves, que se refiere a una clave criptográfica, en un componente lógico programable según las características mencionadas anteriormente.

Típicamente, el módulo lógico programable se configura una vez para cada uso por un flujo de bits para una función concreta. No obstante, el componente lógico pierde esta función nuevamente al desconectar la tensión de funcionamiento. El flujo de bits en sí también se puede actualizar mediante el uso de un producto de programa informático, que está concebido en particular como una memoria de solo lectura programable y borrable (EEPROM).

Los ejemplos de realización del componente lógico programable según la invención, del circuito de formación de claves y del procedimiento para proporcionar una información de seguridad están representados a modo de ejemplo en los dibujos y se explican más en detalle en referencia a la siguiente descripción. Muestran:

Figura 1 un ejemplo de realización de un componente lógico programable en representación esquemática;

Figura 2 un ejemplo de realización de un circuito lógico combinatorio en un diagrama de bloques;

Figura 3 un segundo ejemplo de realización de un componente lógico programable con un circuito de formación de claves con estado en representación esquemática;

Figura 4 un primer ejemplo de realización de un circuito de formación de claves con un circuito lógico con estado en un diagrama de bloques;

Figura 5 un segundo ejemplo de realización de un circuito de formación de claves con un circuito lógico sin estado y con estado en un diagrama de bloques;

Figura 6 un tercer ejemplo de realización de un circuito de formación de claves con circuitos lógicos con estado y sin estado y registros adicionales en representación en bloques; y

Figura 7 un ejemplo de realización del procedimiento según la invención en forma de un diagrama de flujo.

Las partes correspondientes entre sí están provistas en todas las figuras con las mismas referencias.

La figura 1 muestra un componente lógico programable 10 con un circuito de formación de claves 11, que está concebido aquí en forma de un bloque de generación de claves, y se configura mediante un flujo de bits 13. El circuito de formación de claves 11 le proporciona a una unidad criptográfica 12, que está concebida aquí en el mismo componente lógico, una información de seguridad K que se refiere a una clave criptográfica. Esta información de seguridad K puede ser, por ejemplo, una clave criptográfica completa o solo una parte de una clave criptográfica, que se emite como texto sin formato o codificada por un parámetro de enmascaramiento y se le proporciona a la unidad criptográfica 12 para el uso posterior. A este respecto, la información de seguridad K se puede proporcionar, por ejemplo, como un bloque de 128 bits o como un bloque de 256 bits. La información de seguridad K también se puede proporcionar en partes de, por ejemplo, 8 bits, 16 bits, 32 bits o 64 bits. Estas partes se usan directamente por una unidad criptográfica 12 para ejecutar una función criptográfica, o se recopilan varias partes y a partir de ellas se forma una información de seguridad completa K o una clave criptográfica completa, que luego solo entra en una función criptográfica como parámetro.

Además, la información de seguridad K se puede proporcionar en forma enmascarada, por ejemplo vinculando la información de seguridad K generada a un parámetro de enmascaramiento, por ejemplo mediante una función OR exclusiva (XOR), y añadiendo el valor resultante a los parámetros de enmascaramiento. El parámetro de enmascaramiento se puede generar, por ejemplo, dinámicamente por un generador de números aleatorios. Esto tiene la ventaja de que, por ejemplo, se dificultan los ataques de canal lateral. La función de formación de claves 11 proporciona la información de seguridad K en forma enmascarada.

La función de formación de claves puede estar implementada en particular en un componente lógico programable, como, por ejemplo, una matriz de puertas programable en campo, también llamada módulo de FPGA. El circuito de formación de claves 11 se puede cargar en el componente lógico programable en forma de un flujo de bits, de modo que la información de seguridad K se forma dentro del componente lógico en el tiempo de ejecución mediante una función lógica digital. La información de seguridad K formada no está contenida en el texto sin formato en el flujo de bits y, en particular, tampoco se transmite como un valor de inicialización de celdas de memoria o registros. La ejecución de la función de formación de claves en el tiempo de ejecución significa que la función se ejecuta tan pronto como se activa el componente lógico, es decir, se aplica corriente o la ejecución de la función de formación de claves se inicia de manera dedicada por ciertas señales.

La unidad criptográfica 12 generalmente puede implementar cualquier función criptográfica que use la información de seguridad K proporcionada como parámetro. La función criptográfica 12 se puede implementar preferiblemente en el mismo componente lógico 10, de modo que la información de seguridad K solo se transfiere internamente dentro del componente lógico programable 10 desde la función de formación de claves 11 a la unidad criptográfica 12. La unidad criptográfica 12 puede implementar una encriptación y/o desencriptación, por ejemplo, en base del estándar de encriptación expandido AES. La unidad criptográfica 12 también puede estar configurada para generar o verificar sumas de verificación criptográficas, por ejemplo, un código de autenticación de mensaje encriptado como HMAC-SHA2. Pero, la unidad criptográfica 11 también puede implementar una función para abrir una memoria de claves, de modo que las claves almacenadas allí sean accesibles. Además, la unidad criptográfica 12 puede ejecutar una función de autenticación o una función para calcular una clave derivada.

La figura 2 muestra ahora un ejemplo de realización de una función de formación de claves 20, que comprende un circuito lógico sin estado que se compone de varias puertas lógicas 21 a 28, y un registro 29. Este circuito lógico puramente combinatorio comprende, por ejemplo, las puertas NOR 21, 23, 26, 28, una puerta AND 25 y una puerta XOR 27. El registro 29 le proporciona al circuito lógico combinatorio, es decir, sin estado, con un valor de inicialización IV. Un bit de la información clave K se forma mediante el circuito lógico combinatorio. El registro 29 del valor de inicialización IV aquí contiene, por ejemplo, seis bits, pero generalmente puede comprender cualquier número de bits. En general, el valor de inicialización puede estar implementado como un registro o como una señal constante.

Mediante un circuito semejante se pueden formar correspondientemente varios bits de información de seguridad. Por ejemplo, se pueden proporcionar 128 circuitos de este tipo en un componente lógico 10 para formar una información de seguridad K con una longitud de 128 bits.

En una variante del circuito de formación de claves 20 se pueden formar diferentes partes de la información de seguridad K mediante diferentes valores de inicialización IV, no mostrados. A este respecto puede estar previsto un valor de inicialización propio IV por cada bit o un grupo de bits de la información de seguridad K. No obstante, un valor de inicialización común IV se usa preferiblemente para determinar todos los bits de la información de seguridad y en particular de la clave criptográfica.

La figura 3 muestra ahora un componente lógico programable 30 que presenta un circuito de formación de claves 31 que comprende un circuito lógico vinculado al estado. Un circuito lógico con estado semejante también se denomina máquina automática de estados y comprende un número finito de estados. Una señal de reloj CLK se aplica externamente al circuito de formación de claves 31. Por ejemplo, la máquina automática de estados realiza una transición de estado en cada flanco de la señal de reloj CLK y pasa a un nuevo estado. De este modo se proporciona una información de seguridad K y se le transfiere a una unidad criptográfica 32.

A este respecto, en una variante, la información de seguridad K solo se puede proporcionar si se aplica una señal de activación enable en el circuito de formación de claves. En otra variante, la información de seguridad K también se puede generar partiendo de una señal de reinicio Reset y, por ejemplo, solo se puede proporcionar durante un cierto período de tiempo. Por ejemplo, la información de clave K solo está disponible entre el ciclo 100 y 200 después de que se haya producido señal de reinicio Reset.

La figura 4 muestra ahora un ejemplo de realización de un circuito de formación de claves 40 con un circuito lógico con estado. Este circuito de estado o máquina automática de estados comprende un registro de estado 41 y un elemento de transición de estado 42. Aquí se puede usar para determinar el estado final o de salida, por ejemplo, a través de una tabla de transición, que define un estado final para cada estado de entrada cuando existen diferentes condiciones, y que de nuevo se transfieren al registro de estado 41. En el circuito de formación de claves 40, el registro de estado 41 de la máquina automática de estados se usa directamente como un registro de clave. Así solo se requiere un número mínimo de registros y, por ejemplo, se pueden procesar 128 bits por ciclo. Partiendo de un valor inicial, las transiciones se aplican a los datos del registro cuando se establece la señal de habilitación. En un momento determinado, el registro de estado 41 contiene la información de seguridad K. Al desactivar la señal de activación enable, la información de seguridad K se proporciona durante cualquier período de tiempo y se sobrescribe automáticamente cuando la señal de activación enable se establece de nuevo. Esto representa una implementación particularmente eficiente, por ejemplo, para una clave de 128 bits.

La figura 5 muestra ahora una variante del circuito de formación de claves 40 de la figura 4. En este caso, la información de seguridad K, por ejemplo de 128 bits de longitud, está formada por una secuencia de bits que es mayor que 128 bits, por un registro de estado 51 y un elemento de transición de estado 52. La información de seguridad K se crea en texto sin formato solo por medio de un circuito lógico combinatorio 53, que realiza la decodificación o desenmascaramiento. El circuito de generación de claves 50 tiene, por lo tanto, la ventaja de que la información de seguridad real nunca está presente en el registro de estado o de clave 51. El circuito de generación de claves 50 está construido así como una combinación de un circuito lógico con estado y uno sin estado.

La figura 6 muestra ahora un ejemplo de realización de un circuito de formación de claves 60, en el que un circuito lógico con estado 66 implementa un estado codificado a partir de 32 bits. El circuito lógico con estado 66 reproducido comprende un registro de estado 61 y un elemento de transición de estado 62 en el que, por ejemplo, la transición de estado se genera aleatoriamente. El estado o valor de estado modificado por el elemento de transición de estado 62 se introduce nuevamente en el registro de estado. El estado emitido del registro de estado 61, identificado aquí por la longitud del valor de estado de 32 bits con 32, se decodifica, por ejemplo, para excitar un registro de clave 65. Al registro de clave 65 se le proporciona una información de dirección addr, con aquí, por ejemplo, 4 bits de longitud, una señal de escritura we y una palabra de datos data de 8 bits de longitud. Después de pasar por un cierto número de estados del circuito lógico con estado 66, se escribe un cierto valor en el registro de clave 65. La información de seguridad K está presente después de un cierto número de ciclos de reloj.

La información de dirección y la señal de escritura se generan por un decodificador de dirección de clave 63 a partir del valor de estado suministrado por la máquina automática de estados 66. A este respecto, un decodificador de valor de clave 64 es preferentemente un circuito lógico combinatorio que, partiendo de un valor de inicialización, proporciona uno o varios bits de una información de seguridad K o partes de la información de seguridad K. El valor actual del registro de estado 61 sirve en este caso como valor de inicialización. El decodificador de dirección de clave 63 también puede estar implementado como un circuito lógico combinatorio, es decir, sin estado.

En una variante del circuito de formación de claves 60, una información de seguridad enmascarada MK también se puede proporcionar como un valor de salida, ver flecha a trazos.

Aquí, por ejemplo, una información de seguridad de 128 bits K como información de seguridad enmascarada de 256 bits MK se genera por concatenación, es decir una yuxtaposición, de un primer valor de enmascaramiento M1 y un segundo valor de enmascaramiento M2,

MK == M1 II M2

representado, de modo que, por ejemplo, para la información de seguridad desenmascarada K se aplica

K == M1 XOR M2

. Una representación enmascarada MK de la información clave K se puede escribir de manera determinista en el registro de clave 65.

En otra forma de realización, un valor inicial enmascarado aleatoriamente, por ejemplo el valor 0, se puede escribir primero en un registro de clave 65. Para este propósito, una máscara M1 se puede determinar aleatoriamente y una máscara M2 se puede formar como una inversa de M1. Este valor se escribe como un valor inicial en el registro

de clave 65, mostrado a trazos en la figura 6. En el caso de acceso de escritura al registro de clave 65, un valor de estado almacenado no se sobrescribe, sino que ya se vincula al valor de estado por medio de una función OR exclusiva. El valor de estado emitido como información de seguridad enmascarada MK de aquí, por ejemplo, 256 bits se le proporciona a una unidad criptográfica. Los valores de enmascaramiento M1 y M2 entonces deben ser conocidos igualmente por la unidad criptográfica.

La información de seguridad proporcionada K o la información de claves enmascarada MK se pueden sobrescribir en ciclos de reloj posteriores. Sin embargo, también es posible que después de la facilitación de todos los bytes de la información de seguridad K no se realice una sobreescritura posterior del registro de clave 65.

Además, el circuito de formación de claves no puede proporcionar un identificador de disponibilidad, por ejemplo, una señal de validación, no representada, cuando una información de seguridad válida K, MK está preparada para la emisión, o indicar si el valor actual del registro de claves 65 es válido. Se puede establecer una señal de validación, por ejemplo, si cada byte de la información de seguridad K, MK del registro de clave 65 se ha escrito al menos una vez. Para este propósito, también se puede proporcionar un registro de conjunto de bytes en el registro de clave 65 para cada byte de la información de clave K, que se establece durante un acceso de escritura a un registro del registro de clave 65. Esto indica si el byte correspondiente se ha escrito al menos una vez. La señal de habilitación resulta entonces como una operación AND de todos los registros de conjuntos de bytes.

En el caso de un acceso de escritura a un byte de información de seguridad que ya se ha escrito, el valor se puede reemplazar o el valor ya puesto se puede conservar. También es posible que se realice una operación lógica del valor antiguo y del valor escrito para determinar el nuevo valor. Esto puede ser una operación XOR, por ejemplo. No obstante, aquí también se realiza una operación mediante un circuito lógico combinatorio, como se describe en el decodificador de dirección de clave 63 o en el decodificador de valor de clave 64.

En una variante, también es posible proporcionar una información de seguridad diferente en diferentes momentos. Estos se pueden usar para diferentes propósitos o aplicaciones. No obstante, es posible en particular que solo se use parte de la información de seguridad.

La información de seguridad K generalmente se puede proporcionar en distintos momentos o durante distintos períodos característicos por uno de los circuitos de formación de claves 11, 31, 40, 50, 60 mencionados. Por ejemplo, la información de seguridad K solo puede estar preparada permanentemente durante una fase de inicialización, por ejemplo, entre un ciclo de inicio predeterminado y un ciclo de finalización predeterminado después del inicio del componente lógico o el dispositivo de cálculo en el que está implementado el componente lógico. Pero, la información de seguridad K también se puede generar y proporcionar solo a solicitud, por ejemplo, mediante una señal de solicitud request. Después de que se haya aplicado la solicitud de señal de solicitud, la información de seguridad solo puede estar disponible por un período de tiempo predefinible.

Sin embargo, la información de seguridad K solo puede estar preparada o proporcionarse en ciertos momentos o períodos de tiempo. Un período de tiempo semejante se puede mostrar, por ejemplo, mediante una señal de validación de clave. En otros instantes, cuando la señal de validación de clave presenta el valor lleno, se emiten otros valores diferentes o aleatorios. También es posible generar un vector de señal de validación de clave en lugar de una señal de validación. Un circuito de evaluación separado puede verificar el vector de señal de validación de clave para determinar si el valor actual emitido o proporcionado por el circuito de formación de claves representa realmente una información de seguridad válida.

En una variante adicional, una máquina automática de estados o un circuito lógico con estado puede contener una información de marca de agua. De este modo, una información secreta seleccionable se puede ocultar en una máquina automática de estados. Mediante una determinada secuencia de estado, por ejemplo, partes del valor de salida de la máquina automática de estados se pueden tomar de la información secreta de la marca de agua y escribirse en el registro de clave.

En la figura 7 se describe un ejemplo de realización de un procedimiento correspondiente para proporcionar una información de seguridad que se refiere a una clave criptográfica en forma de un diagrama de flujo 70. En el estado inicial 71 está presente un componente lógico programable, cuyo circuito lógico se puede programar por medio de un flujo de bits. A este respecto, un componente lógico programable, cuyo circuito lógico se programa por un flujo de bits, se modifica por los pasos del procedimiento mencionados.

El primer paso del procedimiento es la transmisión 72 de un circuito de formación de claves 11, 31 por un flujo de bits 13 al componente lógico 10, 30 de la figura 1 o la figura 3. Como siguiente paso sigue la generación 73 de la información de seguridad por medio de la ejecución del circuito de formación de claves 11, 31 en el componente lógico 10, 30 y a continuación la facilitación 74 de la información de seguridad K como un parámetro de entrada para una unidad criptográfica 12, 32. En el estado final posterior 75, la información de seguridad K está a disposición al menos temporalmente.

La presente invención no se limita a las características y los ejemplos de realización descritos. Todas las

características descritas y/o dibujadas se pueden combinar ventajosamente entre sí en el marco de la invención.

REIVINDICACIONES

1. Componente lógico programable, que se configura por un flujo de bits (13), donde mediante el flujo de bits se configura un circuito de formación de claves (11, 31), que genera de manera determinista una información de seguridad (K), que se refiere a una clave criptográfica, en el tiempo de ejecución, donde la información de seguridad (K) de una unidad criptográfica (12, 32) se puede proporcionar como parámetro de entrada, y donde la generación de la información de seguridad (K) se realiza utilizando los datos de inicialización que están contenidos en el flujo de bits.

2. Componente lógico programable (10, 30) según la reivindicación 1, donde el circuito de formación de claves (20) comprende un circuito lógico sin estado, en particular un circuito lógico combinatorio.

3. Componente lógico programable (10, 30) según la reivindicación 1, donde el circuito de formación de claves (30, 40, 50, 60) comprende un circuito lógico con estado.

4. Componente lógico programable (10, 30) según la reivindicación 2 o 3, donde el circuito de formación de claves (50, 60) comprende una combinación de circuitos lógicos sin estado y con estado.

5. Componente lógico programable (10, 30) según una de las reivindicaciones 1 a 4, donde un valor de inicialización (IV) del circuito de formación de claves (20) está presente de una manera fija predeterminada o solo se forma antes de su uso en el circuito de formación de claves.

6. Componente lógico programable (10, 30) según una de las reivindicaciones 1 a 5, donde el circuito de formación de claves (11, 20, 31, 40, 50, 60) está concebido para proporcionar la información de seguridad (K) solo se durante un período de tiempo predeterminado y/o después de un cierto número predeterminado de ciclos de reloj.

7. Componente lógico programable (10, 30) según una de las reivindicaciones 1 a 6, donde el circuito de formación de claves (11, 20, 31, 40, 50, 60) está concebido para generar y emitir solo una parte de la información de seguridad (K) respectivamente en un momento.

8. Componente lógico programable (10, 30) según la reivindicación 7, donde el circuito de formación de claves (11, 20, 31, 40, 50, 60) está concebido para generar diferentes partes de la información de seguridad (K) en base a diferentes valores de inicialización (IV).

9. Componente lógico programable (10, 30) según una de las reivindicaciones 1 a 8, donde el circuito de formación de claves (60) está concebido para generar una información de seguridad enmascarada (MK) modificadas por al menos un parámetro de enmascaramiento (M1, M2) o partes de una información de seguridad enmascarada (MK).

10. Componente lógico programable (10, 30) según la reivindicación 9, donde el circuito de formación de claves (11, 20, 31, 40, 50, 60) está concebido para cambiar dinámicamente el parámetro de enmascaramiento.

11. Componente lógico programable (10, 30) según una de las reivindicaciones 1 a 10, donde el circuito de formación de claves (11, 20, 31, 40, 50, 60) está concebido para generar la información de seguridad (K) solo a demanda.

12. Componente lógico programable (10, 30) según la reivindicación 11, donde el circuito de formación de claves (11, 20, 31, 40, 50, 60) está concebido para proporcionar un identificador de disponibilidad cuando la información de seguridad válida (K) está preparada para la emisión.

13. Componente lógico programable (10, 30) según una de las reivindicaciones 1 a 12, donde el circuito de formación de claves (11, 20, 31, 40, 50, 60) está concebido para proporcionar distinta información de seguridad (K) para diferentes aplicaciones en distintos momentos.

14. Componente lógico programable (10, 30) según una de las reivindicaciones 1 a 13, que comprende adicionalmente una unidad criptográfica (12, 32).

15. Componente lógico programable (10, 30) según una de las reivindicaciones 1, 3 a 14, donde el flujo de bits (13) contiene una información de marca de agua oculta, y el circuito lógico con estado proporciona la información de marca de agua después de un número de ciclos de reloj para formar una información de seguridad (K).

16. Circuito de formación de claves para generar y proporcionar una información de seguridad (K) que se refiere a una clave criptográfica, que está configurada según las reivindicaciones 1 a 15.

17. Procedimiento para proporcionar una información de seguridad (K), que se refiere a una clave criptográfica, en un componente lógico programable (10, 30), cuyos circuitos lógicos se programan por un flujo de bits (13), con los pasos:

- transmisión de un circuito de formación de claves a través de un flujo de bits al componente lógico (10, 30),

- generación determinista de la información de seguridad (K) por medio de la ejecución del circuito de formación de claves (11, 20, 31, 40, 50, 60) en el componente lógico (10, 30), y

- facilitación de la información de seguridad (K) como parámetro de entrada para una unidad criptográfica (12, 32), donde la generación de la información de seguridad (K) se realiza utilizando los datos de inicialización que están contenidos en el flujo de bits.

18. Producto de programa informático que genera un flujo de bits (13) para la carga en un componente lógico programable (10, 30), y el flujo de bits (13) está concebido para configurar un circuito de formación de claves (11, 20, 31, 40, 50, 60), que se refiere a una clave criptográfica, según las reivindicaciones 1 a 15, en un componente lógico programable (10, 30).

FIG 1

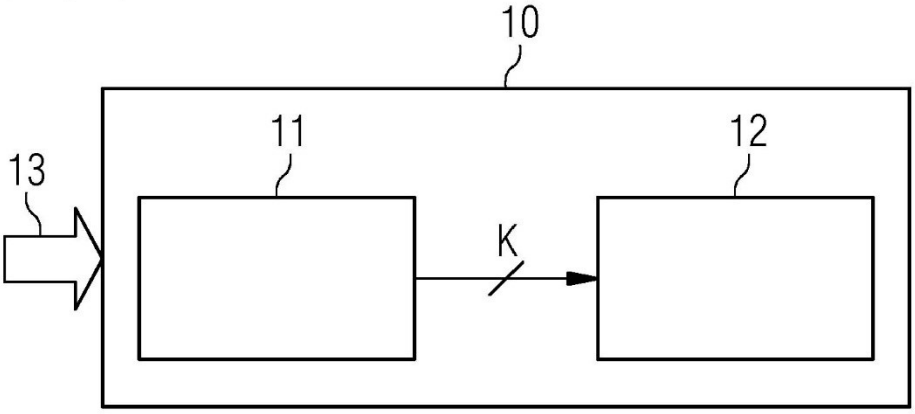

FIG 2

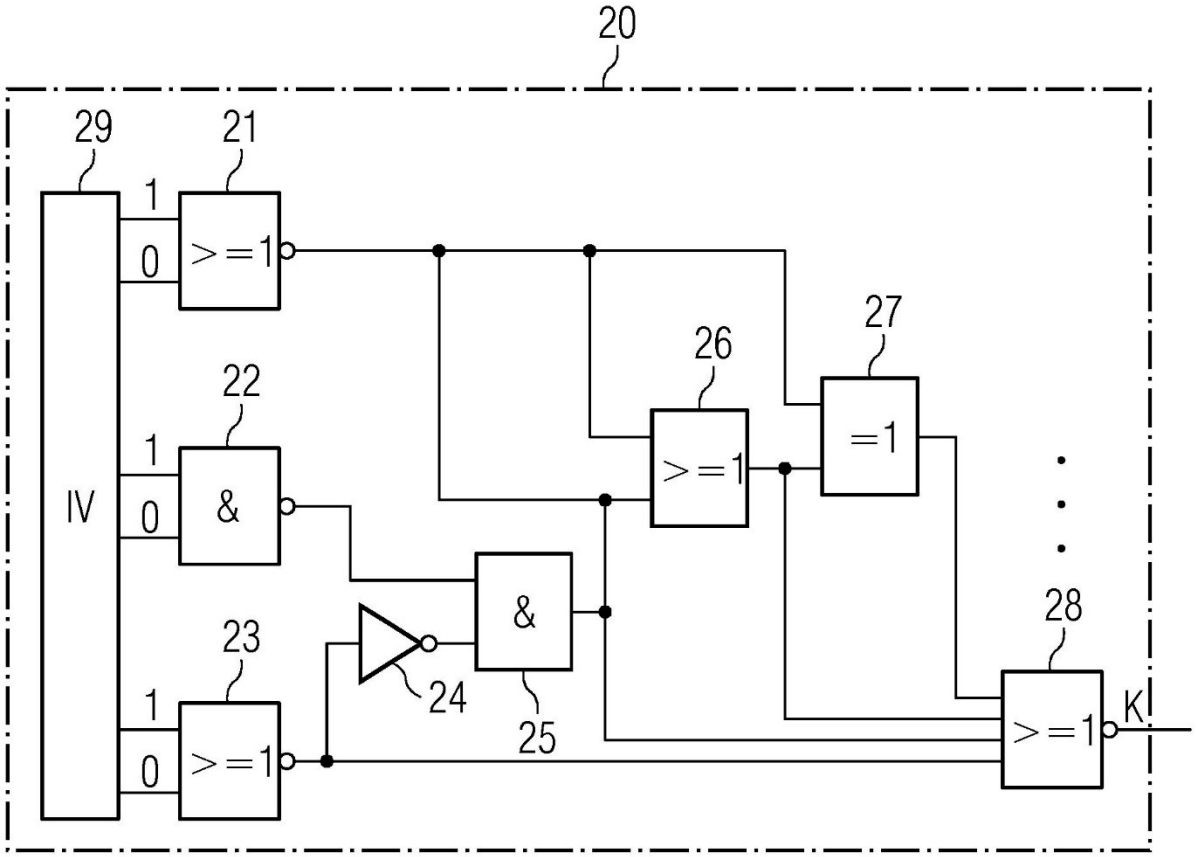

FIG 3

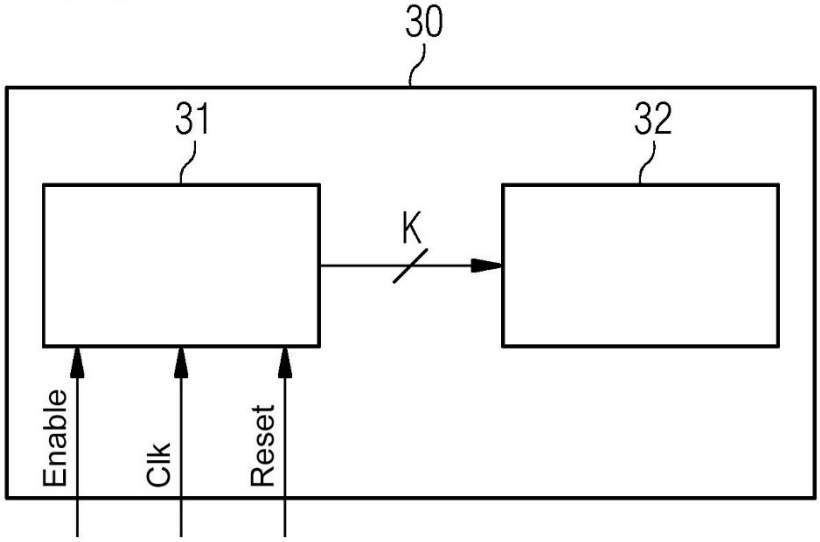

FIG 4

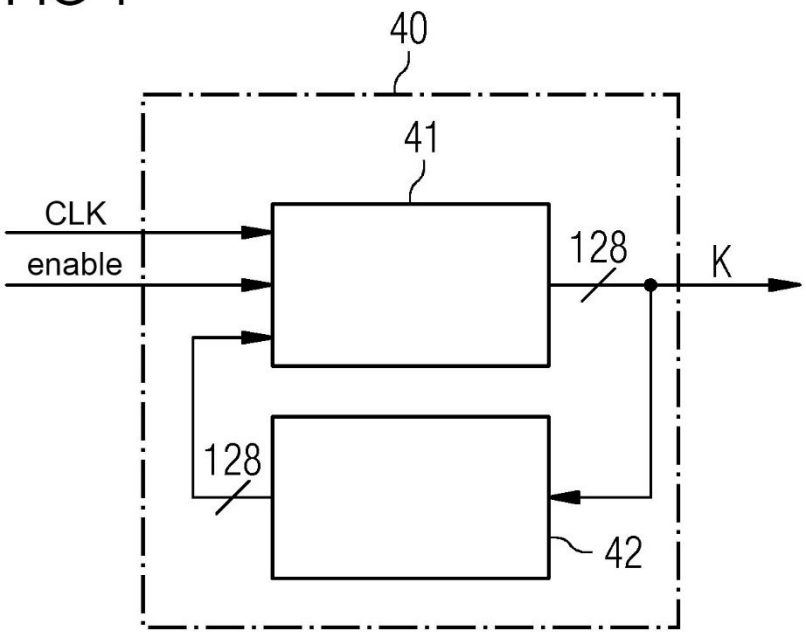

FIG 5

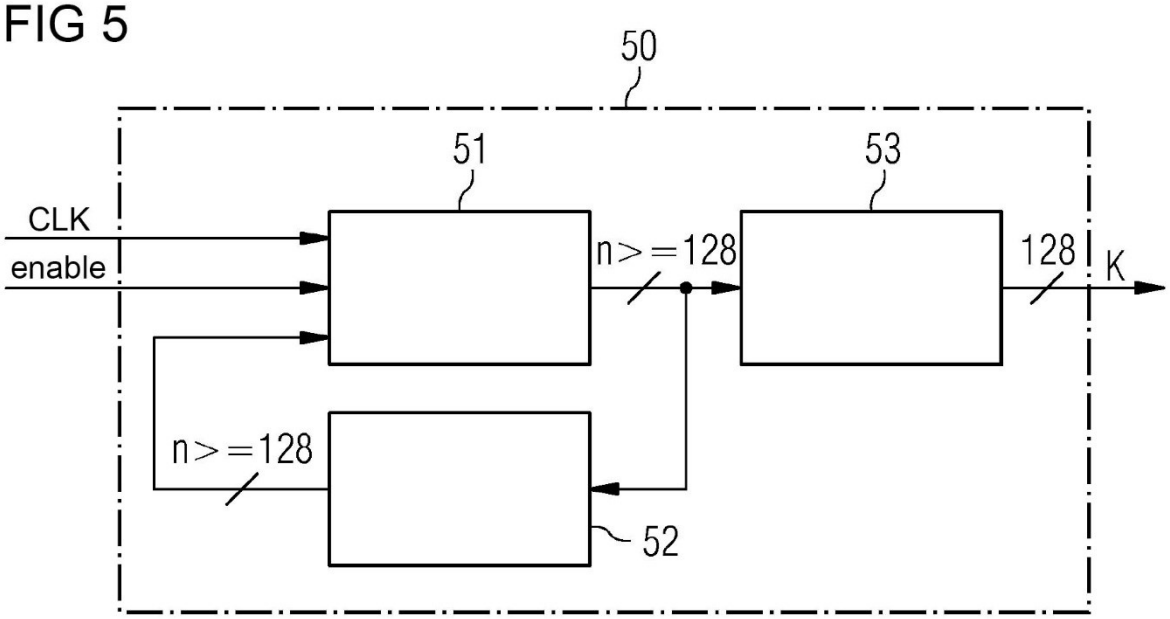
50
51
53
CLK
enable
n>=128
128
K
n>=128
52

FIG 6

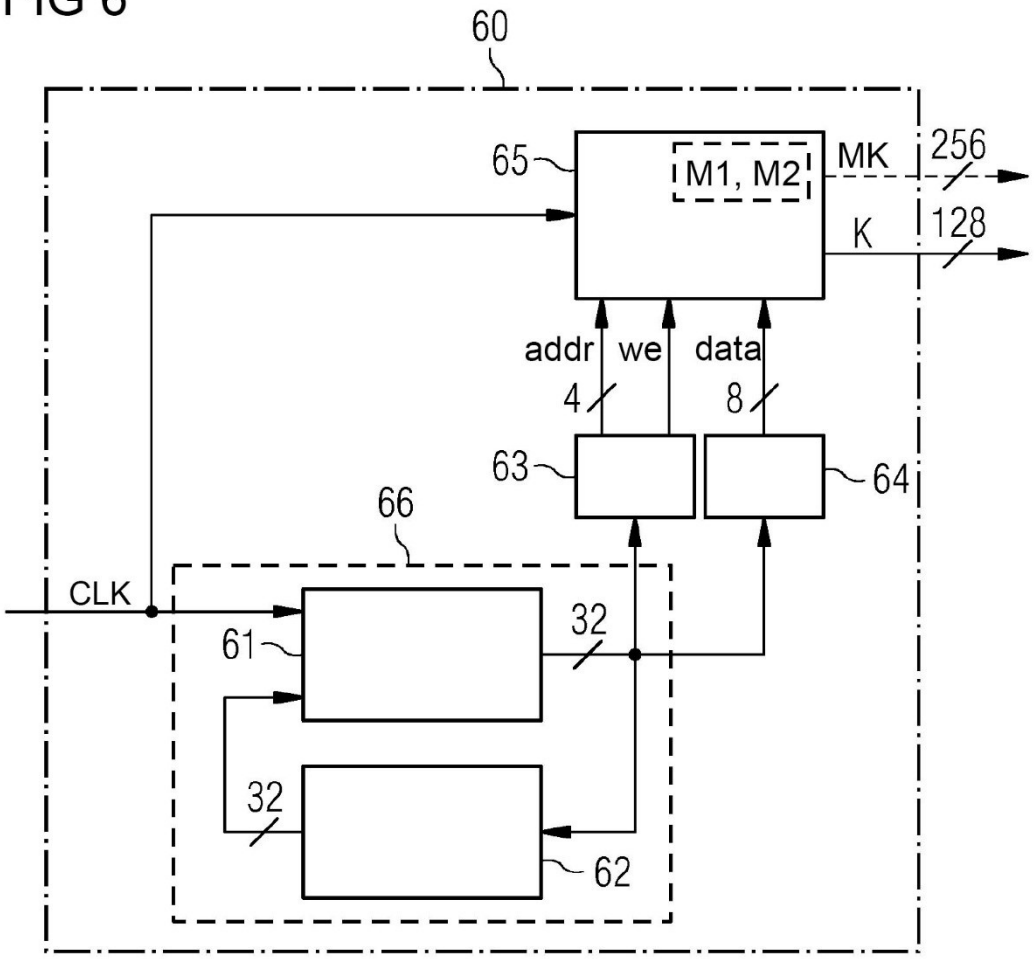
60
65
M1, M2
MK
256
K
128
addr
we
data
4
8
63
64
66
CLK
61
32
32
62

FIG 7