(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 660 057**

(51) Int. CI.:

G06F 21/77 (2013.01)
G06F 21/55 (2013.01)
G06Q 20/34 (2012.01)
G07F 7/08 (2006.01)
H04L 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.05.1999 PCT/EP1999/03385**

(87) Fecha y número de publicación internacional: **25.11.1999 WO99060534**

(96) Fecha de presentación y número de la solicitud europea: **17.05.1999 E 99924992 (3)**

(97) Fecha y número de publicación de la concesión europea: **03.01.2018 EP 1080454**

(54) Título: **Soporte de almacenamiento de datos de acceso protegido**

(30) Prioridad:

18.05.1998 DE 19822217
18.05.1998 DE 19822220
18.05.1998 DE 19822218

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.03.2018

(73) Titular/es:

GIESECKE + DEVRIENT MOBILE SECURITY GMBH (100.0%)
PRINZREGENTENSTRASSE 159
81677 MÜNCHEN, DE

(72) Inventor/es:

VATER, HARALD;
DREXLER, HERMANN y
JOHNSON, ERIC

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

DESCRIPCIÓN

Soporte de almacenamiento de datos de acceso protegido

La invención se refiere a un soporte de almacenamiento de datos que presenta un chip semiconductor, en el que están almacenados datos secretos. En particular, la invención se refiere a una tarjeta de chip.

Los soportes de almacenamiento de datos que contienen un chip son utilizados en una pluralidad de aplicaciones diferentes, por ejemplo, para realizar transacciones financieras, para pagar productos o servicios o como medio de identificación para regular controles de entrada y acceso. En todas estas aplicaciones, dentro del chip del soporte de almacenamiento de datos generalmente se procesan datos secretos que deben ser protegidos contra el acceso por parte de terceros no autorizados. Esta protección se garantiza, entre otras cosas, por el hecho de que las estructuras internas del chip presentan dimensiones muy pequeñas y, por tanto, un acceso a estas estructuras con el objetivo de espiar los datos que son procesados en estas estructuras resulta muy difícil. Para dificultar aún más un acceso, el chip puede estar incrustado en una masa muy adherente de forma que, en caso de una extracción forzosa, la oblea de semiconductor sea destruida o al menos se destruyan los datos secretos almacenados en la misma. También es posible dotar la oblea de semiconductor durante su fabricación con una capa protectora que no pueda eliminarse sin destruir la oblea de semiconductor.

Con un equipo técnico apropiado que es extremadamente costoso pero, no obstante, en principio está disponible, un atacante podría lograr exponer y analizar la estructura interna del chip. Para exponerla se podrían utilizar, por ejemplo, procedimientos de decapado especiales o un proceso de pulido adecuado. Las estructuras del chip expuestas de este modo como, por ejemplo, las pistas conductoras, podrían analizarse estableciendo el contacto con microsondas o mediante otros procedimientos para determinar los patrones de señales en estas estructuras. A partir de las señales detectadas se podría intentar determinar a continuación los datos secretos del soporte de almacenamiento de datos como, por ejemplo, claves secretas, para su uso con fines de manipulación. Mediante las microsondas también se podría intentar influenciar de forma precisa los patrones de señales en las estructuras expuestas.

Del documento de patente de EE.UU. US A 4.932.053 se conoce un soporte de almacenamiento de datos con chip semiconductor, que presenta al menos una memoria, en la que está almacenado un programa operativo que incluye varios comandos. Cada comando genera señales detectables desde el exterior del chip semiconductor. Las señales son medidas a través del consumo de corriente en las conexiones del circuito integrado, lo que permite sacar conclusiones sobre los datos procesados. Para evitar la lectura está previsto un circuito integrado de protección que genera una secuencia pseudoaleatoria mediante celdas de simulación. De este modo, al comportamiento de la corriente que se puede medir desde el exterior se le superpone una señal aleatoria.

Del documento francés abierto a inspección pública FRA-2 745 924 se conoce el uso de un generador aleatorio para convertir en indescifrables las señales, que conduce a la pérdida de sincronización en la ejecución de secuencias de comandos o secuencias de programas dentro del proceso.

El documento EP 0 908 810 A2 da a conocer un equipo para procesar información de programa estructurada como secuencias de bloques. El equipo comprende un circuito integrado seguro con una CPU, una memoria externa y una memoria caché. Durante la transferencia de una secuencia de bloques de información de programa de la memoria externa a la memoria caché se produce una variación aleatoria del orden de los bloques transferidos dentro de la secuencia.

El objetivo de la invención consiste en proteger los datos secretos contenidos en el chip de un soporte de almacenamiento de datos contra el acceso no autorizado.

Este objetivo se consigue mediante las combinaciones de características de las reivindicaciones independientes.

En la solución según la invención, al contrario del estado de la técnica, no se toman medidas para evitar exponer las estructuras internas del chip y la colocación de microsondas. En lugar de ello, se toman medidas que dificultan a un atacante potencial sacar conclusiones sobre informaciones secretas a partir de los patrones de señales que puedan haber sido captados. Los patrones de señales dependen de las operaciones que el chip está ejecutando en ese momento. El control de estas operaciones tiene lugar con la ayuda de un programa operativo que está almacenado en una memoria del chip. El programa operativo está compuesto por una serie de comandos individuales que desencadenan respectivamente una operación exactamente definida. Para que el chip pueda ejecutar las funciones que se le han asignado se debe definir una secuencia de comandos correspondiente para cada una de estas funciones. Una función de este tipo puede ser, por ejemplo, el cifrado de datos con la ayuda de una clave secreta. Para que un atacante que capta los procesos en el chip mediante microsondas montadas en el mismo obtenga la menor cantidad de información posible sobre los comandos respectivamente ejecutados y los datos utilizados en la ejecución de los comandos, según una primera solución alternativa de la presente invención, para la realización de una función deseada preferentemente se utilizan tales comandos o se utilizan de tal manera que el espionaje de informaciones resulte difícil o imposible. En otras palabras, según la primera alternativa de la invención no se debe

utilizar ningún comando o secuencia de comandos que permita, en caso de captación, sacar fácilmente conclusiones sobre los datos procesados.

Sacar conclusiones sobre los datos es siempre especialmente fácil si el comando solo procesa muy pocos datos, por ejemplo, un único bit. Por esta razón, según una realización de la primera alternativa, al menos para todas las operaciones relevantes para la seguridad como, por ejemplo, el cifrado de datos, se utilizan preferentemente aquellos comandos que procesan simultáneamente varios bits, por ejemplo, respectivamente un byte. Al procesar simultáneamente varios bits, la influencia que tienen los bits individuales sobre el patrón de señales generado por el comando se difumina en una señal total, a partir de la cual es muy difícil sacar conclusiones sobre los bits individuales. El patrón de señales es esencialmente más complejo que en el caso del procesamiento de bits individuales y no resulta evidente qué parte de la señal corresponde a qué bit de los datos procesados.

Según la primera alternativa es posible dificultar adicional o alternativamente el acceso a los datos procesados utilizando para las operaciones relevantes para la seguridad exclusivamente aquellos comandos que desencadenan un patrón de señales idéntico o muy similar o bien comandos en los cuales los datos procesados no tienen o solo tienen una influencia mínima sobre el patrón de señales.

Según otra segunda alternativa de la invención se prevé no realizar operaciones relevantes para la seguridad con datos secretos reales, sino con datos secretos falseados, a partir de los cuales no es posible determinar los datos secretos reales sin recurrir a otras informaciones secretas adicionales. Esto tiene la consecuencia de que un atacante, incluso si logra determinar los datos secretos utilizados en una operación, no puede utilizarlos para causar daño, ya que los datos espiados no son los datos secretos reales sino los datos secretos falseados.

Para garantizar el modo de funcionamiento del soporte de almacenamiento de datos se debe asegurar que el soporte de almacenamiento de datos, si se utiliza de forma adecuada, proporciona los resultados correctos a pesar de los datos secretos falseados. Esto se consigue determinando en primer lugar una función con la que se falsean los datos secretos reales, por ejemplo, una vinculación EXOR de los datos secretos a un número aleatorio. Los datos secretos reales son falseados con la función determinada de este modo. Con los datos secretos falseados, en el soporte de almacenamiento de datos se realizan todas aquellas operaciones que permiten compensar a continuación nuevamente el falseo de los datos secretos. En el caso de datos secretos falseados mediante vinculación EXOR serían operaciones lineales en relación con las vinculaciones EXOR. Antes de ejecutar una operación que no admite una compensación de este tipo, por ejemplo, una operación no lineal en relación con la vinculación EXOR, se deben volver a recuperar los datos secretos reales para que esta operación se ejecute con los datos secretos reales. La recuperación de los datos secretos reales tras la aplicación de una función compensable tiene lugar, por ejemplo, mediante vinculación EXOR del valor de función determinado mediante los datos secretos falseados a un valor de función correspondiente del número aleatorio utilizado para el falseo. En este contexto es importante que el número aleatorio y el valor de función hayan sido determinados y almacenados previamente en un entorno seguro para que el cálculo del valor de función a partir del número aleatorio no pueda ser captado.

El procedimiento anterior tiene la consecuencia de que los datos secretos reales solo se utilizan para la ejecución de las operaciones para las cuales esto es estrictamente necesario como, por ejemplo, operaciones no lineales, es decir, operaciones que no pueden ejecutarse, en su lugar, con datos secretos falseados. Puesto que este tipo de operaciones generalmente son muy complejas y difíciles de analizar, para un atacante potencial es extremadamente difícil, si no incluso imposible, descubrir los datos secretos reales a partir de un análisis de los patrones de señales generados por estas operaciones. Puesto que las funciones de estructura sencilla, para las cuales es posible una compensación posterior del falseo, se realizan con datos secretos falseados, el procedimiento descrito dificulta enormemente la determinación de los datos secretos reales del soporte de almacenamiento de datos a partir de patrones de señales captados sin autorización.

Los patrones de señales dependen de las operaciones que el chip está ejecutando en ese momento. Si estas operaciones siempre se realizan según el mismo esquema rígido, es decir, en particular, siempre en el mismo orden, y el atacante conoce este orden, entonces un atacante debe superar muchas menos dificultades para espiar los datos que si no supiera qué operación está siendo ejecutada en qué momento. Por esta razón, según la invención está previsto desviarse lo más ampliamente posible de un esquema de procesos rígido durante la ejecución de las operaciones relevantes para la seguridad dentro de la tarjeta de chip para, de este modo, ofrecer al atacante la menor cantidad posible de puntos de partida para un análisis de los datos secretos. Esto se consigue ejecutando la mayor cantidad posible de operaciones, en caso ideal incluso todas las operaciones, que sean independientes entre sí en el sentido de que cada una de las operaciones no requiera datos que deban ser determinados por las otras operaciones, en un orden variable, por ejemplo, aleatorio o dependiente de los datos de entrada. De este modo se consigue que un atacante, que generalmente se orientará en el orden de las operaciones, no pueda descubrir sin más qué operación se está ejecutando en ese momento. Esto es válido especialmente cuando las operaciones son muy similares o incluso iguales en relación con el patrón de señales generado por estas para los mismos datos de entrada. Si el atacante ni siquiera conoce el tipo de operación que está siendo ejecutada en ese momento, resulta extremadamente difícil espiar datos de forma precisa. Si existe el peligro de que un atacante realice muchos intentos de espionaje para descubrir la variación aleatoria del orden, se recomienda hacer que la variación dependa de los datos de entrada.

La invención se describe a continuación en base a los modos de realización representados en las figuras.

Muestran:

La figura 1, una tarjeta de chip en vista superior y
la figura 2, una sección muy aumentada en vista superior del chip de la tarjeta de chip representada en la figura 1,
la figura 3, una representación esquemática de una parte de una secuencia funcional dentro de la tarjeta de chip,
la figura 4, una variante de la secuencia funcional representada en la figura 3,
la figura 5, una representación esquemática de la secuencia en la ejecución de algunas operaciones en la tarjeta de chip.

En la figura 1 se representa una tarjeta de chip -1- como un ejemplo del soporte de almacenamiento de datos. La tarjeta de chip -1- está compuesta por un cuerpo de tarjeta -2- y un módulo de chip -3- que está insertado en una entalladura del cuerpo de tarjeta -2- prevista para ello. Los componentes principales del módulo de chip -3- son las superficies de contacto -4-, a través de las cuales se puede establecer una conexión eléctrica a un equipo externo, y un chip -5-, que está conectado eléctricamente a las superficies de contacto -4-. Alternativa o adicionalmente a las superficies de contacto -4-, también se puede disponer una bobina u otro medio de transmisión no representado en la figura 1 para establecer la conexión de comunicación entre el chip -5- y un equipo externo.

En la figura 2 está representada una sección muy ampliada en vista superior del chip -5- de la figura -1-. Lo especial de la figura 2 consiste en que está representada la superficie activa del chip -5-, es decir, que todas las capas que protegen en general la capa activa del chip -5- no están representadas en la figura 2. La información sobre los patrones de señales en el interior del chip se puede obtener, por ejemplo, estableciendo el contacto entre las estructuras expuestas -6- y las microsondas. Las microsondas consisten en agujas muy finas que son puestas en contacto eléctrico con las estructuras expuestas -6-, por ejemplo, pistas conductoras, mediante un dispositivo de ubicación de precisión. Los patrones de señales registrados con las microsondas son procesados a continuación con dispositivos de medición y valoración adecuados con el objetivo de sacar conclusiones sobre datos secretos del chip.

Con la invención se logra que un atacante, incluso si ha logrado eliminar la capa protectora del chip -5- sin dañar el circuito integrado y establecer el contacto entre las estructuras expuestas -6- del chip -5- y las microsondas o captarlas de otro modo, logre solo con gran dificultad o no logre acceder especialmente a los datos secretos del chip. Naturalmente, la invención también se aplica si un atacante logra acceder a los patrones de señales del chip -5- de otro modo.

Según la primera alternativa de la invención, los comandos o secuencias de comandos del programa operativo del chip se eligen, al menos para todas las operaciones relevantes para la seguridad, de forma que a partir de los patrones de señales captados o bien no sea posible de ningún modo o al menos resulte muy complicado sacar conclusiones sobre los datos procesados con los comandos.

Esto se puede conseguir, por ejemplo, prescindiendo en el caso de operaciones de seguridad básicamente de todos los comandos que procesan bits individuales como, por ejemplo, el desplazamiento de bits individuales, a través del cual se pretende lograr una permutación de los bits de una cadena de bits. En lugar de comandos de bits se puede recurrir, por ejemplo, a comandos de bytes como, por ejemplo, comandos de copia o rotación que, en lugar de procesar un bit individual, procesan directamente un byte completo compuesto por ocho bits. El comando de bytes desencadena, al contrario que el comando de bits, un patrón de señales esencialmente más complejo, lo que dificulta enormemente una asignación entre bits individuales y segmentos parciales del patrón de señales. Esto conduce a una ocultación de la información procesada con el comando de bytes y dificulta por tanto el espionaje de esta información.

Además, en el marco de la primera alternativa de la invención también existe la posibilidad de utilizar en las operaciones relevantes para la seguridad básicamente solo comandos que desencadenen un patrón de señales muy similar, de forma que la diferenciación de los comandos que están siendo ejecutados en ese momento mediante los patrones de señales resulte muy compleja. También es posible configurar los comandos de forma que el tipo de datos procesado no tengan ninguna o solo muy poco influencia sobre el patrón de señales desencadenado por el comando.

Las variantes mencionadas se pueden aplicar en relación con los comandos individuales de forma alternativa o bien combinada. Por lo tanto, un conjunto de comandos relevantes para la seguridad puede estar compuesto por comandos que pertenecen a una o varias de las variantes mencionadas anteriormente. También se puede utilizar un conjunto de comandos en el que todos los comandos pertenecen a la misma variante, aunque también puede estar permitido que algunos o incluso todos los comandos también pertenezcan adicionalmente a otras variantes. De este modo, por ejemplo, pueden estar permitidos exclusivamente los comandos de bytes, utilizándose preferentemente aquellos comandos que además desencadenan un patrón de señales muy similar.

Se consideran operaciones relevantes para la seguridad, por ejemplo, las operaciones de cifrado, que frecuentemente también son utilizadas en tarjetas de chip. En el marco de estos cifrados se ejecutan una serie de operaciones individuales que conducen a modificaciones a nivel de bits en una palabra de datos. Según la primera alternativa de la invención, todos estos comandos son sustituidos por comandos de bytes y/o se toman las otras medidas mencionadas anteriormente. De este modo resulta aún más difícil para un atacante sacar conclusiones sobre las claves secretas utilizadas para el cifrado a partir de los patrones de señales captados y se evita el uso indebido de estas claves secretas.

La figura 3 muestra una representación esquemática de una parte de una secuencia funcional en la tarjeta de chip. Para la representación se eligió, a modo de ejemplo, una operación de cifrado. No obstante, los principios descritos en este ejemplo también son aplicables a cualquier otra operación relevante para la seguridad. Al comienzo de la sección de la operación de cifrado representada en la figura 3 se introducen datos -abc-, que pueden estar disponibles como texto no cifrado o ya cifrado, a un punto de vinculación -7-. En el punto de vinculación -7- tiene lugar una vinculación de los datos -abc- a una clave -K1-. En el presente ejemplo, esta vinculación consiste en una vinculación EXOR, aunque también se pueden utilizar otras formas de vinculación adecuadas. Al resultado de la vinculación se aplica a continuación una función no lineal en un bloque de función -8-. Para representar que el bloque de función -8- representa una función no lineal, este se muestra en la figura 3 en forma de un rectángulo sesgado. Según la segunda alternativa de la invención, los datos generados con el bloque de función -8- son vinculados en un punto de vinculación -9- mediante vinculación EXOR a un número aleatorio -Z- y a continuación procesados en un bloque de función -10-. Mediante la vinculación al número aleatorio -Z- tiene lugar un falseo de los datos que dificulta a un atacante un análisis de los procesos en el bloque de función -10-, que representa una función lineal mediante una función -f-. Como símbolo para una función lineal, en la figura 3 se utiliza un rectángulo no sesgado. Según la segunda alternativa, los datos generados en el bloque de función -10- son vinculados en un punto de vinculación -11- a datos -f (Z)- que fueron generados previamente, por ejemplo, durante la fabricación de la tarjeta mediante aplicación de la función -f- al número aleatorio -Z-. Esta vinculación compensa el falseo de los datos con el número aleatorio -Z- en el punto de vinculación -9-. Esta compensación es necesaria porque, a continuación, la función no lineal -g- será aplicada en el bloque de función -12- a los datos y tras la aplicación de una función no lineal a los datos ya no es posible una compensación del falseo. Además, los datos son vinculados en el punto de vinculación -11- mediante vinculación EXOR a una clave -K2- que es necesaria en el marco de la operación de cifrado.

La vinculación en el punto de vinculación -11- a los datos -f (Z)- y -K2- puede tener lugar o bien con los componentes individuales -K2- y -f (Z)- o con el resultado de una vinculación EXOR de estos componentes individuales. El último procedimiento ofrece la posibilidad de que la clave -K2- no deba estar disponible como texto no cifrado sino tan solo la clave -K2- vinculada mediante vinculación EXOR a -f (Z)-. Si este valor de vinculación ya fue calculado previamente, por ejemplo, durante la inicialización o personalización de la tarjeta de chip -1- y almacenado en la memoria de la tarjeta, no es necesario almacenar la clave -K2- como texto no cifrado en la tarjeta de chip -1-. Esto permite aumentar aún más la seguridad de la tarjeta de chip -1-.

Tras aplicar la función -g- a los datos en el bloque de función -12-, el resultado así determinado es vinculado nuevamente al número aleatorio -Z- en un punto de vinculación -13- y, por tanto, falseado. En el bloque de función -14- se vuelve a aplicar la función lineal -f- al resultado de la vinculación. Finalmente, en un punto de vinculación -15- tiene lugar una vinculación EXOR de los datos a los resultados de aplicar la función -f- al número aleatorio -Z- y con una clave -K3-. A esta operación le pueden seguir otros pasos de procesamiento que, no obstante, no están representados en la figura 3.

En general, el procedimiento representado en la figura 3, que corresponde a la segunda alternativa de la invención, se puede resumir de tal manera que los datos procesados en la operación de vinculación son falseados mediante vinculación EXOR con un número aleatorio -Z-, siempre que esto es posible, para evitar el espionaje de datos secretos. El falseo es posible básicamente para todas las funciones -f- que muestran un comportamiento lineal en relación con las vinculaciones EXOR. En el caso de funciones no lineales -g- se deben utilizar datos no falseados. Por lo tanto es necesario que antes de la aplicación de la función no lineal -g- a los datos se compense el falseo mediante una vinculación EXOR de los datos al valor de función -f (Z)-. En este sentido, en cuanto a aspectos de seguridad, es poco crítico que las funciones no lineales -g- solo puedan aplicarse a los datos no falseados, ya que estas funciones no lineales -g- son de por sí esencialmente más difíciles de espiar que las funciones lineales -f-. El esquema representado en la figura 3 es aplicable, tanto para funciones -g- iguales o funciones -f- iguales, como también para funciones respectivamente diferentes.

Con el esquema representado en la figura 3 se consigue que el espionaje de datos secretos durante el procesamiento de los datos -abc- sea algo prácticamente imposible. No obstante, puesto que al poner a disposición las claves secretas -K1-, -K2- y -K3- se deben realizar operaciones con estas claves, que a su vez podrían ser el objetivo de un intento de espionaje por parte de un atacante, se recomienda tomar las medidas de seguridad correspondientes durante el procesamiento de las claves. Un modo de realización de la invención, en el que están previstas este tipo de medidas de seguridad, está representado en la figura 4.

La figura 4 muestra una parte de una secuencia funcional de una tarjeta de chip conforme a la figura 3 para otra variante de la segunda alternativa de la invención. El procesamiento de los datos -abc- tiene lugar de forma idéntica que en la figura 3 y por tanto no se vuelve a explicar a continuación. Sin embargo, al contrario que en la figura 3, en la figura 4 no se introducen las claves -K1-, -K2- y -K3- en los puntos de vinculación -7-, -11- y -15-. En su lugar se introducen las claves falseadas -K1'-, -K2'- y -K3'-, junto con los números aleatorios -Z1-, -Z2- y -Z3- necesarios para compensar el falseo, introduciéndose preferentemente primero las claves falseadas y luego los números aleatorios. De este modo se asegura que las claves correctas -K1-, -K2- y -K3- no aparecen en absoluto. Este procedimiento se puede aplicar de forma especialmente ventajosa en procedimientos de cifrado, en los que las claves -K1-, -K2- y -K3- son derivadas de una clave -K- común. En este caso, en la tarjeta de chip -1- se almacena la clave falseada -K- con el número aleatorio -Z- y en la tarjeta de chip -1- se almacenan los números aleatorios -Z1-, -Z2- y -Z3- determinados mediante aplicación del procedimiento de derivación de clave al número aleatorio -Z-. Este almacenamiento debe tener lugar en un entorno seguro, por ejemplo, en la fase de personalización de la tarjeta de chip -1-.

Para realizar el esquema de funcionamiento representado en la figura 4 se requieren, además de los datos almacenados, también las claves falseadas derivadas -K1'-, -K2'- y -K3'-. Estas claves se pueden derivar luego, cuando son necesarias, de la clave falseada -K-. En este procedimiento no se realiza ninguna operación con la clave real -K- o con las claves reales derivadas -K1-, -K2- y -K3-, de forma que resulta prácticamente imposible espiar estas claves. Puesto que también los números aleatorios derivados -Z1-, -Z2- y -Z3- ya fueron determinados y almacenados en la tarjeta de chip -1- previamente, tampoco con ellos se realiza ninguna operación que pudiera ser espiada por un atacante. De este modo, tampoco es posible acceder a las claves reales derivadas -K1-, -K2- y -K3- mediante espionaje de las claves falseadas derivadas -K1'-, -K2'- y -K3'-, ya que para ello se requieren los números aleatorios derivados -Z1-, -Z2- y -Z3-.

Para aumentar aún más la seguridad, también es posible utilizar para cada vinculación EXOR otro número aleatorio -Z-, debiendo tenerse en cuenta que entonces también se debe disponer respectivamente de un -f (Z)- para compensar el falseo. En un modo de realización, todos los números aleatorios -Z- y valores de función -f (Z)- se almacenan en la memoria de la tarjeta de chip. Pero también es posible almacenar respectivamente solo un número reducido de números aleatorios -R- y valores de función -f (Z)- y determinar, cada vez que se requieren estos valores, nuevos números aleatorios -Z- y valores de función -f (Z)- mediante vinculación EXOR u otra operación adecuada de varios números aleatorios -Z- y valores de función -F (Z)- almacenados. Los números aleatorios -Z- para la vinculación EXOR pueden elegirse de forma aleatoria del conjunto de números aleatorios -Z- almacenados.

En otro modo de realización de la segunda alternativa se prescinde del almacenamiento de los números aleatorios -Z- y valores de función -f (Z)-, ya que estos son generados en caso necesario mediante generadores adecuados. Es importante que el o los generadores no generen los valores de función -f (Z)- aplicando la función lineal -f- al número aleatorio -Z- sino que generen pares de números aleatorios -Z- y valores de función -f (Z)- de otro modo, ya que, en caso contrario, captando la aplicación de la función -f- al número aleatorio -Z- podría espiarse este número aleatorio -Z- y, con ayuda de esta información, podrían determinarse otros datos secretos.

Según la segunda alternativa de la invención, se pueden falsear básicamente todos los datos relevantes para la seguridad, por ejemplo, también claves, con la ayuda de otros datos, por ejemplo, números aleatorios, y luego introducirse al procesamiento posterior. De este modo se consigue que un atacante que espía este procesamiento posterior solo pueda determinar datos falseados y sin valor. Al final del procesamiento posterior se vuelve a deshacer el falseo.

La figura 5 muestra una representación esquemática de la secuencia en la ejecución de algunas operaciones en la tarjeta de chip para visualizar la invención. En la figura 5 se representa, en particular, qué operaciones deben ser ejecutadas obligatoriamente de forma secuencial por la tarjeta de chip -1-, ya que son dependientes entre sí, y qué operaciones pueden ejecutarse, en principio, en paralelo y, por tanto, también en cualquier orden. A este respecto, en la figura 5 está representada una parte de una secuencia de programa de la tarjeta de chip -1-, en la que se procesan datos -abc-. Todas las operaciones que deben ejecutarse obligatoriamente de forma secuencial están representadas en la figura 5 de forma secuencialmente consecutiva. Todas las operaciones para las cuales no es importante el orden de ejecución entre sí, están dispuestas en paralelo.

El procesamiento de los datos -abc- comienza con una operación -P1- que está representada en forma de un bloque -70-. Al bloque le sigue secuencialmente un bloque -80- que representa la operación -P2-. De la figura 5 se desprende que el orden de procesamiento de las operaciones -P1- y -P2- no se puede intercambiar, es decir, es obligatoriamente fija. El esquema representado en la figura 5 se ramifica después del bloque -80- en cinco bloques -90-, -100-, -110-, -120- y -130-, que representan las operaciones -P3-, -P4-, -P5-, -P6- y -P7-. De esto resulta que los bloques -P3-, -P4-, -P5-, -P6- y -P7- pueden ejecutarse simultáneamente y, por tanto, también en cualquier orden. Según la invención, el orden de ejecución de estas operaciones -P3-, -P4-, -P5-, -P6- y -P7- varía en cada proceso, es decir, el atacante no puede prever cuál de estas operaciones seguirá a la operación -P2-, qué operación a su vez se realizará después, etc. La variación del orden puede tener lugar según un esquema fijo preestablecido o, mejor aún, de forma aleatoria o en función de los datos de entrada, determinándose mediante un número aleatorio o a través de los datos de entrada respectivamente cuál de las operaciones -P3-, -P4-, -P5-, -P6- y -P7- será la

siguiente en ser ejecutada. Mediante esta variación, dado el caso aleatoria, de la ejecución de las operaciones individuales se dificulta un espionaje de los datos procesados con las operaciones. Una vez que han sido ejecutadas todas las operaciones -P3-, -P4-, -P5-, -P6- y -P7-, les sigue obligatoriamente la operación -P8-, cuyo orden de procesamiento no es variable. La operación -P8- está representada por el bloque -140-. A la operación -P8- le pueden seguir otras operaciones, tanto de orden variable como también de orden fijo, que ya no están representadas en la figura 5.

La invención se puede utilizar, por ejemplo, en el marco de la ejecución de algoritmos de cifrado que, frecuentemente, incluyen operaciones similares, cuyo orden de procesamiento es variable. En este sentido, el orden de procesamiento se puede establecer respectivamente antes de la primera operación variable, en común para todas las operaciones intercambiables con esta primera operación, o la siguiente operación que se va a ejecutar también se puede determinar antes de cada operación variable del conjunto de operaciones variables remanentes. En ambos casos, para la determinación del orden de procesamiento se puede recurrir a números aleatorios.

REIVINDICACIONES

1. Soporte de almacenamiento de datos con un chip semiconductor que presenta al menos una memoria, en la que está almacenado un programa operativo, **caracterizado por que** con el programa operativo se puede ejecutar una pluralidad de operaciones, siendo válido al menos para un subconjunto de estas operaciones que el resultado total obtenido en caso de ejecutarse varias operaciones del subconjunto no depende del orden de ejecución de las operaciones, y el orden de ejecución del subconjunto de operaciones mencionado al menos varía cuando el subconjunto incluye una o varias operaciones relevantes para la seguridad.

2. Soporte de almacenamiento de datos, según la reivindicación 1, **caracterizado por que** el orden de la ejecución es variado en cada proceso a través del subconjunto de operaciones mencionado.

3. Soporte de almacenamiento de datos, según cualquiera de las reivindicaciones 1 o 2, **caracterizado por que** el orden de la ejecución es variado según un principio fijo preestablecido.

4. Soporte de almacenamiento de datos, según cualquiera de las reivindicaciones 1 o 2, **caracterizado por que** el orden de la ejecución es variado de forma aleatoria.

5. Soporte de almacenamiento de datos, según cualquiera de las reivindicaciones 1 o 2, **caracterizado por que** el orden de la ejecución depende de los datos procesados con las operaciones.

6. Soporte de almacenamiento de datos, según cualquiera de las reivindicaciones 1 a 5, **caracterizado por que** el orden de la ejecución se establece respectivamente antes de la ejecución de la primera operación del subconjunto para todas las operaciones del subconjunto cuya ejecución está prevista de forma directamente consecutiva.

7. Soporte de almacenamiento de datos, según cualquiera de las reivindicaciones 1 a 5, **caracterizado por que** respectivamente antes de comenzar la ejecución de una operación del subconjunto se establece cuál de las operaciones del subconjunto, cuya ejecución está prevista de forma consecutiva, será la siguiente en ser ejecutada.

8. Soporte de almacenamiento de datos, según cualquiera de las reivindicaciones anteriores, **caracterizado por que** el soporte de almacenamiento de datos consiste en una tarjeta de chip.

9. Procedimiento, en un soporte de almacenamiento de datos con un chip semiconductor, que presenta al menos una memoria, en la que está almacenado un programa operativo para ejecutar una pluralidad de operaciones dentro del programa operativo del soporte de almacenamiento de datos, siendo válido al menos para un subconjunto de estas operaciones que el resultado total obtenido en caso de ejecutarse varias operaciones del subconjunto no depende del orden de ejecución de las operaciones, y el orden de ejecución del subconjunto de operaciones mencionado al menos varía cuando el subconjunto incluye una o varias operaciones relevantes para la seguridad.

10. Procedimiento, según la reivindicación 9, **caracterizado por que** el orden de la ejecución es variado en cada proceso a través del subconjunto de operaciones mencionado.

11. Procedimiento, según cualquiera de las reivindicaciones 9 o 10, **caracterizado por que** el orden de la ejecución es variado según un principio fijo preestablecido.

12. Procedimiento, según cualquiera de las reivindicaciones 9 o 10, **caracterizado por que** el orden de la ejecución es variado de forma aleatoria.

13. Procedimiento, según cualquiera de las reivindicaciones 9 o 10, **caracterizado por que** el orden de la ejecución depende de los datos procesados con las operaciones.

14. Procedimiento, según cualquiera de las reivindicaciones 9 a 13, **caracterizado por que** el orden de la ejecución se establece respectivamente antes de la ejecución de la primera operación del subconjunto para todas las operaciones del subconjunto.

15. Procedimiento, según cualquiera de las reivindicaciones 9 a 13, **caracterizado por que** respectivamente antes de comenzar la ejecución de una operación del subconjunto se establece cuál de las operaciones del subconjunto, cuya ejecución está prevista de forma consecutiva, será la siguiente en ser ejecutada.

FIG.1

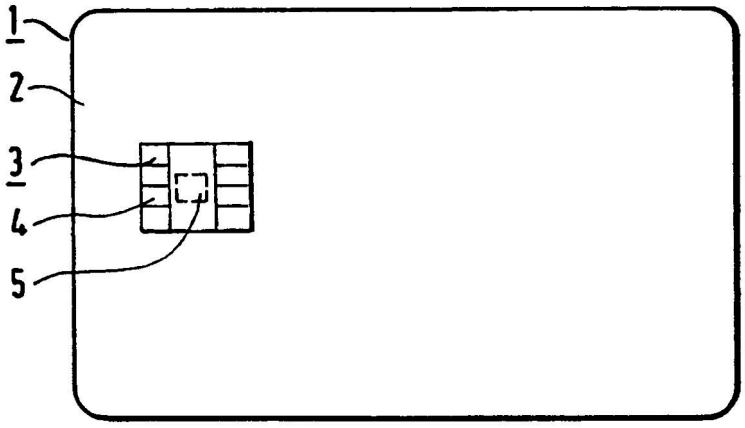

FIG.2

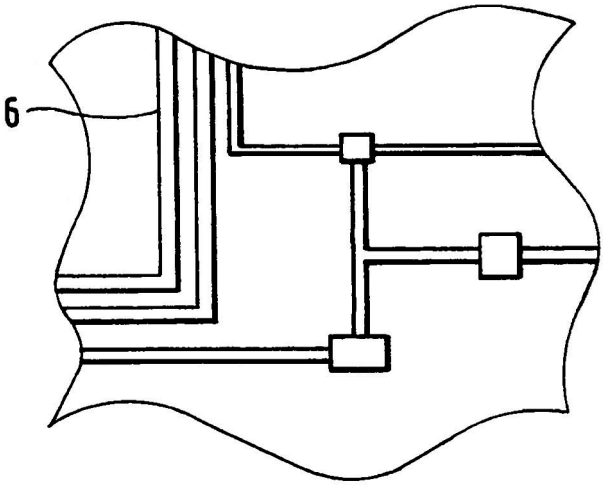

FIG.3

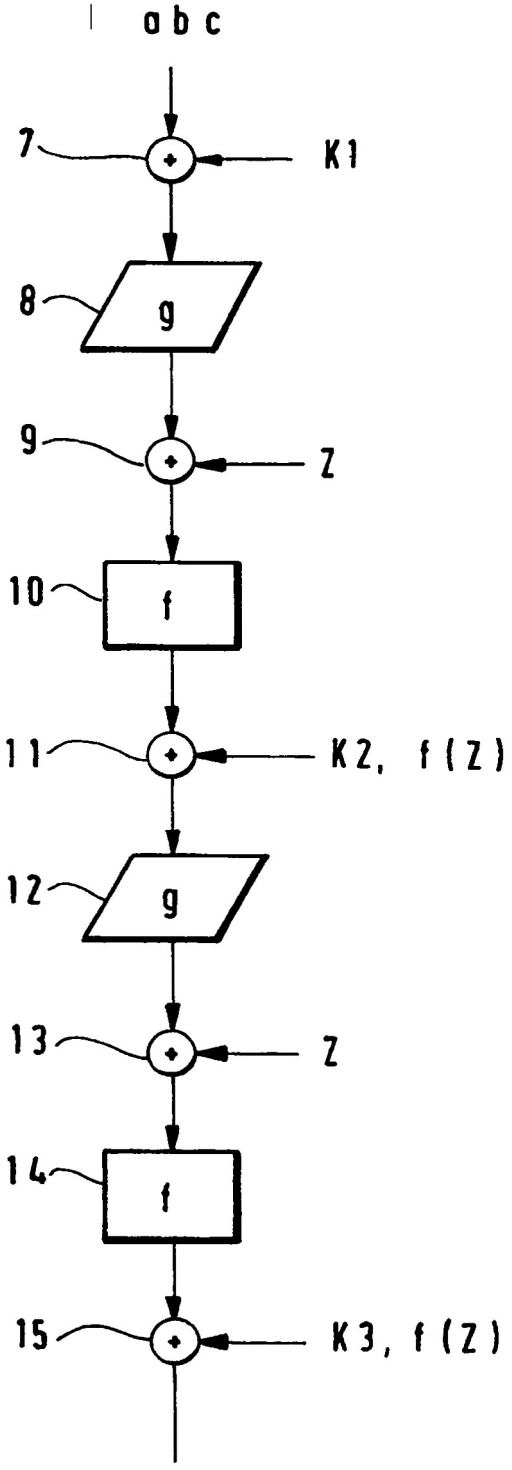

FIG. 4

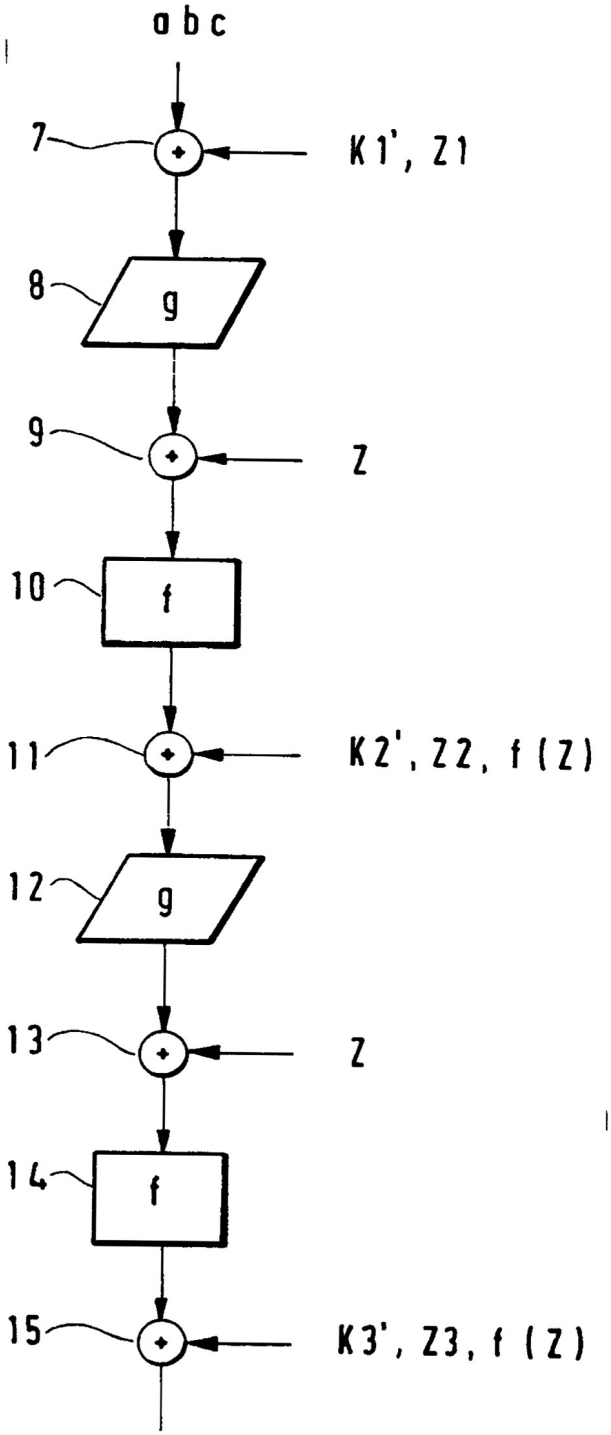

FIG.5