(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 754 266**

(51) Int. CI.:

G06F 21/75 (2013.01)
G06F 12/14 (2006.01)
G06F 21/60 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.03.2016 PCT/EP2016/056188**

(87) Fecha y número de publicación internacional: **06.10.2016 WO16156095**

(96) Fecha de presentación y número de la solicitud europea: **22.03.2016 E 16715257 (8)**

(97) Fecha y número de publicación de la concesión europea: **14.08.2019 EP 3254227**

(54) Título: **Procedimiento para proteger datos relevantes para la seguridad en una memoria caché**

(30) Prioridad:

31.03.2015 DE 102015205827

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.04.2020

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Werner-von-Siemens-Straße 1
80333 München, DE

(72) Inventor/es:

ASCHAUER, HANS y
HEINTEL, MARKUS

(74) Agente/Representante:

LOZANO GANDIA, José

DESCRIPCIÓN

Procedimiento para proteger datos relevantes para la seguridad en una memoria caché

En microprocesadores modernos, que se utilizan en sistemas de computadoras, se utilizan memorias caché para acelerar el acceso a la memoria, para almacenar transitoriamente (tamponar) datos de zonas de direcciones frecuentemente utilizadas de la memoria de trabajo. Esta aceleración del acceso a la memoria se logra siendo claramente más rápido el acceso del procesador a la memoria caché que el acceso a datos de la memoria de trabajo. No obstante, a partir de la información relativa a qué partes de la memoria de trabajo están cargadas en ese momento en el caché, pueden obtenerse informaciones sobre el proceso que se ejecuta en ese momento. Éstas son por ejemplo registros de una tabla utilizados con frecuencia.

En particular en aplicaciones criptográficas esto significa la existencia de un canal lateral crítico que, cuando se evalúa adecuadamente, puede conducir por ejemplo a la pérdida de claves secretas, que llegan a un atacante. Los ataques se aprovechan de que la asociación de direcciones de la memoria de trabajo a la posición dentro del caché del procesador sólo presenta una variabilidad reducida y por lo tanto puede evaluarse estadísticamente. En general se intenta obtener informaciones sobre la modificación del contenido del caché mediante el proceso a analizar, por ejemplo un criptoalgoritmo.

Una estrategia común es el procedimiento evict-and-probe (desalojar y probar). Un proceso de análisis llena primeramente el caché con datos propios y mide a continuación tiempos de acceso a la memoria. Entonces pueden medirse por ejemplo aciertos de caché (en inglés cache hits) o un fallo de caché (en inglés cache miss). Si se realiza este análisis durante un largo periodo de tiempo, entonces pueden extraerse conclusiones relativas a los datos relevantes para la seguridad de un procedimiento de encriptado, por ejemplo claves criptográficas para el procedimiento AES y le resulta a un atacante por ejemplo posible reconstruir estos datos relevantes para la seguridad.

El documento US 2014/0095797 A1 se refiere a una memoria caché para aumentar características de prestaciones y de seguridad. La memoria caché incluye una matriz de datos para memorizar una pluralidad de bloques de datos, una matriz de tags para memorizar un bloque de tags. La cantidad de tags corresponde a la cantidad de bloques de datos. Además incluye la memoria caché un decodificador de direcciones para un mapeado dinámico memoria-a-caché, para aumentar la seguridad.

Zhenghong Wang describe en “Information leakage due to cache and processor architectures” (Fugas de información debidas a arquitecturas de caché y procesador) la permutación de mapeado memoria-a-caché utilizando tablas de permutación. Además se describe un “re-mapeado” dinámico memoria-a-caché.

El objetivo de la presente invención es proteger datos relevantes para la seguridad en una memoria caché.

El objetivo se logra mediante las medidas descritas en las reivindicaciones independientes 1 y 11. En las reivindicaciones secundarias se exponen ventajosos perfeccionamientos de la invención.

Según un primer aspecto, se refiere la invención a un procedimiento para proteger datos relevantes para la seguridad en una memoria caché, archivándose una copia de los datos relevantes para la seguridad de una memoria general en la memoria caché. Según el procedimiento se fijan parámetros de ofuscación. Se determina una primera dirección de bloque caché de una dirección de memoria correspondiente a la memoria general, en la que están archivados los datos relevantes para la seguridad. Se genera una primera dirección de bloque caché modificada para el primer bloque caché con una función de generación, utilizando el parámetro de ofuscación y la primera dirección de bloque caché. Se memoriza una copia de los datos relevantes para la seguridad utilizando la primera dirección de bloque caché modificada en una primera línea caché del primer bloque caché.

La utilización de la dirección de bloque caché modificada dificulta el análisis de los datos caché, para obtener informaciones sobre datos relevantes para la seguridad, como por ejemplo el criptoalgoritmo utilizado y los datos criptográficos del criptoalgoritmo. De esta manera pueden protegerse los datos criptográficos de manera efectiva frente al acceso de personas no autorizadas. Mediante el procedimiento correspondiente a la invención se segmentan los datos en la memoria caché y se dispersan en la memoria caché entre varios bloques caché.

En una primera forma de ejecución del procedimiento se determina una dirección de bloque a partir de una dirección de memoria, formándose un primer identificador de la dirección de bloque y utilizando la función de generación adicionalmente la dirección de bloque o el primer identificador para generar la primera dirección de bloque caché modificada.

La utilización adicional del primer identificador o de la dirección de bloque al generarse la primera dirección de bloque caché modificada, aumenta la seguridad del procedimiento.

En otras formas de ejecución del procedimiento se realiza el acceso a los datos relevantes para la seguridad en la memoria caché mediante el primer identificador, la primera dirección de bloque caché y la función de generación, utilizando la función de generación el parámetro de ofuscación, la primera dirección de bloque caché y el primer identificador para generar la primera dirección de bloque caché modificada.

Para acceder a los datos caché es necesario por ejemplo que pueda realizarse por ejemplo una asociación de la primera dirección de bloque caché modificada a la primera dirección de bloque caché. Esto puede realizarse por ejemplo utilizando al memorizar los datos relevantes para la seguridad una tabla, que contiene las informaciones necesarias para esta asociación. Cuando se genera una dirección de bloque caché modificada, por ejemplo la primera dirección de bloque caché modificada, al memorizar datos relevantes para la seguridad, se memoriza en la tabla en la memoria caché la dirección de bloque caché modificada y la dirección de bloque caché (sin modificar). Puesto que esta tabla puede ocultar por un lado riesgos para la seguridad y adicionalmente ocupa espacio en la memoria caché, el cálculo directo del bloque caché modificado al realizar el acceso por un lado aumenta la seguridad y por otro lado el procedimiento ahorra memoria.

En otras formas de ejecución del procedimiento se realiza una modificación de los parámetros de ofuscación según reglas predeterminadas, realizándose mediante la modificación de los parámetros de ofuscación una reorganización de la memoria caché.

Mediante la modificación de los parámetros de ofuscación y la reorganización de la memoria caché, le resulta aún más difícil a un atacante analizar la memoria caché y aumenta así aún más la seguridad del procedimiento.

En otras formas de ejecución del procedimiento, al realizar la reorganización se reproducen los datos de la primera línea caché del primer bloque caché en una segunda línea caché de un segundo bloque caché, reproduciéndose otros datos de otras líneas caché del primer bloque caché total o parcialmente en otras líneas caché de otros bloques caché.

Mediante la reproducción de una línea caché del primer bloque caché en el segundo bloque caché y la reproducción de otras líneas caché del primer bloque caché total o parcialmente en otras líneas caché de otros bloques caché, se dificulta aún más el análisis por parte de atacantes o terceros no autorizados tras una reorganización de la memoria caché. En consecuencia se logra así una protección adicional de los datos relevantes para la seguridad.

En otras formas de ejecución del procedimiento la función de generación es una función que genera la primera dirección de bloque caché modificada mediante una permutación de la primera dirección de bloque caché utilizando los parámetros de ofuscación y el primer identificador.

El acceso a datos de la memoria caché debe realizarse idealmente tan rápido como sea posible. Operaciones de permutación como por ejemplo una operación O-exclusivo, que se realiza bit a bit en la primera dirección de bloque caché utilizando el parámetro de ofuscación y el primer identificador, pueden calcularse de manera sencilla y muy eficiente. Esto tiene la ventaja de que no tiene que integrarse ningún hardware complejo o adicional en la memoria caché o un equipo de gestión caché.

En otras formas de ejecución del procedimiento se modifican los parámetros de ofuscación tras una cantidad previamente definida de accesos con acierto a la memoria caché.

El número de accesos con acierto a la memoria caché puede calcularse muy fácilmente, por lo cual no tiene que integrarse ningún hardware complejo o adicional en la memoria caché o un equipo de gestión caché.

En otras formas de ejecución del procedimiento se modifican los parámetros de ofuscación mediante una solicitud de interrupción.

Los sistemas operativos que se utilizan en sistemas de alta seguridad proporcionan una pluralidad de funciones de seguridad, para impedir un acceso a datos relevantes para la seguridad por parte de atacantes. Un tal sistema operativo puede ejecutar tras detectar un ataque una pluralidad de medidas para llevar el sistema de alta seguridad a un estado seguro cuando se detecta un ataque. A ellas pertenece también el que una reorganización o bien una modificación de los parámetros de ofuscación pueda ser provocada activamente por parte del sistema operativo mediante una solicitud de interrupción. El sistema operativo fija entonces los nuevos parámetros de ofuscación por sí mismo o bien aprovecha un equipo de generación para parámetros de ofuscación para fijar nuevos parámetros de ofuscación.

En otras formas de ejecución del procedimiento se modifica el parámetro de ofuscación dentro de un intervalo de tiempo predeterminado.

Mediante la modificación del parámetro de ofuscación dentro de intervalos de tiempo predeterminados queda asegurado que un atacante sólo dispone de poco tiempo para analizar la memoria caché. Debido a ello le es muy difícil al atacante obtener suficientes informaciones en el análisis, para obtener informaciones sobre datos relevantes para la seguridad.

En otras formas de ejecución del procedimiento contiene el parámetro de ofuscación un número aleatorio, que con preferencia se forma de nuevo cuando tiene lugar un rearranque del sistema.

La utilización de un número aleatorio dificulta a los atacantes adivinar el parámetro de ofuscación. Así se logra una protección elevada de los datos relevantes para la seguridad.

En otras formas de ejecución del procedimiento incluye el parámetro de ofuscación un identificador de hardware inequívoco.

La utilización de un identificador de hardware con otros datos distintos del parámetro de ofuscación permite utilizar un parámetro de ofuscación que puede asociarse fijamente a un aparato. Esto tiene la ventaja de que los sistemas de seguridad detectan cuándo se ha sustituido un aparato, ya que una parte del parámetro de ofuscación no corresponde al identificador de hardware utilizado hasta ahora.

Según otro aspecto se refiere la invención a un sistema para proteger datos relevantes para la seguridad en una memoria caché, archivándose una copia de los datos relevantes para la seguridad de una memoria general en la memoria caché. El sistema presenta un primer equipo de determinación, un equipo de fijación, un primer equipo de generación y un equipo de memoria. El equipo de fijación está constituido para fijar parámetros de ofuscación. El primer equipo de determinación está constituido para determinar una primera dirección de bloque caché de una dirección de memoria de la memoria general en la que están archivados los datos relevantes para la seguridad. El primer equipo de generación está constituido para generar una primera dirección de bloque caché modificada para un primer bloque caché con un equipo de generación utilizando los parámetros de ofuscación y la primera dirección de bloque caché. El equipo de memoria está constituido para memorizar la copia de los datos relevantes para la seguridad utilizando la primera dirección de bloque caché modificada en una primera línea caché del primer bloque caché.

La utilización de la dirección de bloque caché modificada dificulta el análisis de los datos caché para obtener informaciones sobre datos relevantes para la seguridad, como por ejemplo el criptoalgoritmo utilizado y los datos criptográficos del criptoalgoritmo. De esta forma pueden protegerse los datos criptográficos con efectividad frente al acceso de personas no autorizadas.

En una primera forma de ejecución presenta el sistema un segundo equipo de determinación, que está constituido para determinar una dirección de bloque a partir de la dirección de memoria, formándose un primer identificador de la dirección de bloque y utilizando el equipo de generación adicionalmente la dirección de bloque o el primer identificador para generar la primera dirección de bloque caché modificada.

La utilización adicional del primer identificador o de la dirección de bloque cuando se genera la primera dirección de bloque caché modificada, aumenta más aún la seguridad del procedimiento.

En otras formas de ejecución presenta el sistema un equipo de acceso, que está constituido para acceder a los datos relevantes para la seguridad en la memoria caché mediante el primer identificador, la primera dirección de bloque caché y el equipo de generación, utilizando el equipo de generación el parámetro de ofuscación, la primera dirección de bloque caché y el primer identificador para generar la primera dirección de bloque caché modificada para el acceso en la memoria caché.

Para acceder a los datos caché es necesario por ejemplo para el equipo de acceso que por ejemplo pueda realizarse una asociación de la primera dirección de bloque caché modificada a la primera dirección de bloque caché. Esto puede realizarse por ejemplo utilizando al memorizar los datos mediante el equipo de memoria una tabla, que contiene las informaciones necesarias para esta asociación. Si se genera una dirección de bloque caché modificada, por ejemplo la primera dirección de bloque caché, al memorizar datos, se memorizan en la tabla en la memoria caché la dirección de bloque caché modificada y la dirección de bloque caché (sin modificar). Puesto que esta tabla por un lado puede ocultar riesgos para la seguridad y adicionalmente ocupa espacio de memoria en la memoria caché, aumenta el cálculo directo del bloque caché modificado al realizar el acceso por un lado la seguridad y por otro lado el procedimiento ahorra espacio de memoria.

En otras formas de ejecución del sistema, está constituido el equipo de modificación para modificar los parámetros de ofuscación según reglas predeterminadas y se realiza mediante la modificación de los parámetros de ofuscación una reorganización de la memoria caché.

Mediante la modificación de los parámetros de ofuscación por parte del equipo de modificación y la reorganización de la memoria caché, le resulta aún más difícil a los atacantes analizar la memoria caché y esto aumenta así aún más la seguridad del procedimiento.

En otras formas de ejecución del sistema el equipo de generación es un equipo de permutación, que genera la primera dirección de bloque caché modificada mediante una permutación de la primera dirección de bloque caché utilizando los parámetros de ofuscación y el primer identificador.

El acceso a datos de la memoria caché debe realizarse idealmente tan rápido como sea posible. Operaciones de permutación como las que proporciona el equipo de permutación, son por ejemplo una operación O-exclusivo. Éstas pueden aplicarse bit a bit a la primera dirección de bloque caché utilizando el parámetro de ofuscación y el primer identificador y pueden calcularse de manera sencilla y muy eficiente. Esto tiene la ventaja de que no tiene que integrarse ningún hardware complejo o adicional en la memoria caché o bien un equipo de gestión caché.

En otras formas de ejecución del sistema están constituidos el primer equipo de determinación y el segundo equipo de determinación como un equipo de determinación integral.

Las características, particularidades y ventajas de esta invención antes descritas, así como la forma en la que se alcanzan las mismas, quedarán más claras y fáciles de entender en relación con la siguiente descripción de los ejemplos de ejecución, que se describirán más en detalle en relación con los dibujos. Al respecto muestran:

figura 1 una representación esquemática de un sistema convencional para memorizar datos en una memoria caché;
figura 2 un diagrama secuencial del procedimiento correspondiente a la invención para proteger datos relevantes para la seguridad en una memoria caché;
figura 3 una representación esquemática de un módulo de ofuscación correspondiente a la invención y
figura 4 una representación esquemática de un sistema correspondiente a la invención para memorizar datos en una memoria caché.

En las figuras se han dotado elementos que tienen la misma función de las mismas referencias, siempre que no se indique otra cosa.

La figura 1 muestra una representación esquemática simplificada de un sistema convencional que memoriza datos en una memoria caché. Un cache o memoria caché es una memoria tampón (buffer) más rápida, que ayuda a evitar accesos repetidos a una memoria lenta o bien un nuevo cálculo de datos. Para ello se memorizan transitoriamente datos que se han cargado o generado una sola vez en la memoria caché, con lo que pueden bajarse más rápidamente en un posterior acceso. Adicionalmente es posible cargar de antemano en la memoria caché datos a los que se accederá pronto con una elevada probabilidad.

La figura 1 muestra la organización típica de una memoria caché para sistemas actuales, siendo k la cantidad de líneas caché por cada bloque caché ($k \geq 1$). La cantidad de bloques caché n resulta de n = tamaño del caché/(k*longitud de una línea caché).

La secuencia básica según la que se memorizan datos de manera convencional en la memoria caché, se describirá en el siguiente apartado. Adicionalmente se incidirá en que este procedimiento convencional es problemático en cuanto a los datos relevantes para la seguridad.

Primeramente se reproducen los datos de un sistema de computadora en forma de bloques de datos 133, 143, 153, 137, 147, 157 en una memoria que puede direccionarse mediante direcciones de memoria 110 de un campo de direcciones 160. En la práctica existen un campo de direcciones virtual y un campo de direcciones físico, no siendo necesarias estas informaciones para mostrar patentemente el procedimiento y por ello no se entrará en las mismas más en detalle.

Con una dirección de memoria puede direccionarse en este ejemplo en cada caso un byte. Cuando se memoriza un bloque de datos, ocupa el mismo al menos un byte, y puede accederse al mismo mediante una dirección de memoria. Las direcciones de memoria pueden asociarse en cada caso a distintas zonas de direcciones, para direccionar por ejemplo bloques de datos que ocupan varios bytes mediante una zona de direcciones con una dirección de memoria, que se denomina dirección inicial.

En consecuencia está dividido el campo de direcciones 160 en varias zonas de direcciones, en las cuales están archivados por ejemplo un primer bloque de datos 133, un segundo bloque de datos 143, un tercer

bloque de datos 153, un bloque de datos número m1 137, un bloque de datos número m2 147 y un bloque de datos número m3 157. En la figura 1 está archivado en una primera dirección de memoria 161 el primer bloque de datos 133 y en una segunda memoria de direcciones el bloque de datos número m1.

La memoria caché presenta usualmente varios bloques caché 130, 140, 150, para alojar una copia del bloque de datos del campo de direcciones 160. En la figura 1 se representan un primer bloque caché 130, un segundo bloque caché 140 y un bloque caché número n 150. En detalle presenta un bloque caché una pluralidad de líneas caché, línea caché 1 hasta línea caché k, para memorizar en una línea caché uno de los bloques de datos 133, 143, 153, 137, 147, 157.

El primer bloque caché 130 representado está archivado en una primera dirección de bloque caché 112 en la memoria caché, presentando el primer bloque caché 130 una pluralidad de líneas caché, en las que ha de archivarse una copia de los bloques de datos 133 y 137. En detalle se representan una primera línea caché 131 y una línea caché número k 135 para el primer bloque caché 130 en la figura 1, correspondiendo la línea caché número k 135 a la última línea caché en el primer bloque caché 130.

Cuando se carga una copia del primer bloque de datos 133 en la memoria caché, se forma a partir de una dirección de memoria 110 del bloque de datos 133 una dirección de bloque 111 y la primera dirección de bloque caché 112. Para ello se eligen por ejemplo en un sistema de 64 bits del bit 13 al bit 64 de la dirección de memoria 110 para la dirección de bloque 111 y de los bits 7 a 12 para la primera dirección de bloque caché 112. Los bits que no se utilizaron para formar la dirección de bloque 111 y la primera dirección de bloque caché 112, son bits 113 irrelevantes, que no se utilizan para ningún cálculo adicional.

La dirección de bloque 111 se utiliza entonces como un primer identificador 132. Si el bloque de datos 133 no se encuentra aún en la memoria caché, se elige y se borra en el bloque caché 130 una línea caché 132, por ejemplo el acceso utilizado con menos frecuencia o el que se encuentra más atrás. En su lugar entra el bloque de datos actual 133. El primer identificador 132 se archiva igualmente, para hacer posible posteriormente, cuando se accede al caché, una asociación inequívoca. En la figura 1 se determina primeramente la primera dirección de bloque caché 112 del primer bloque caché 130 y a continuación el primer bloque de datos 133 con el primer identificador 132 en la primera línea caché 131.

De la misma manera se archiva el bloque de datos m1 137 de la segunda zona de memoria 162 mediante una dirección de memoria m1 del bloque de datos m1 137 en la línea caché número k 135 del primer bloque caché 130. Para ello se determina de nuevo una dirección de bloque y a partir de la misma se forma un identificador m1 136. La primera dirección de bloque caché 112 se determina igualmente en base a la dirección de memoria m1.

La asociación que determina qué bloque de datos se archiva en qué bloque caché depende de la dirección de memoria del bloque de datos. Las zonas de dirección cuya dirección de memoria se diferencia en un múltiplo de la longitud de un bloque de datos, se reproducen usualmente en una línea caché en el mismo bloque de datos. Bajo ello se entienden direcciones de memoria que se diferencian en un múltiplo de la cantidad de bytes por cada línea caché. Esto tiene el efecto de que los distintos bits de la dirección de memoria 110 que determinan la dirección del bloque caché, son idénticos. Referido al ejemplo antes descrito, este sería el caso de direcciones de memoria cuyos bits 7-12 son idénticos. En la figura 1 se diferencian la primera zona de direcciones 161 y la segunda zona direcciones 162 por lo tanto sólo en un múltiplo de su tamaño máximo del bloque de datos.

Mediante el mismo procedimiento que antes se ha descrito, se reproduce el segundo bloque de datos 143 mediante su segunda dirección de memoria en el segundo bloque caché 140. Aquí se determinan igualmente una dirección de bloque, un segundo identificador 142 y una segunda dirección de bloque caché para el segundo bloque caché 140 a partir de la segunda dirección de memoria.

Puesto que los bits 7-12 de la dirección de memoria m del bloque de datos m2 147 y de la segunda dirección de memoria son idénticos, se reproduce el bloque de datos m2 147 en una línea caché k 146 del segundo bloque caché 140 y se memoriza con un identificador m2 146, que corresponde a una dirección de bloque de la dirección de memoria m2 del bloque de datos m2 147, en el segundo bloque caché 140.

Según el mismo procedimiento se reproducen el tercer bloque de datos 153 y el bloque de datos m3 157 en las líneas caché del bloque caché n 150.

No obstante esta organización del caché es vulnerable para ataques de canal lateral al caché en forma de ataques timing (análisis de la duración de la respuesta) y oculta por lo tanto un riesgo para la seguridad de datos relevantes para la seguridad. Este problema se describió ampliamente por ejemplo en la publicación de Daniel J. Bernstein “Cache-timing attacks on AES” (ataques timing al caché en AES). En general se intenta obtener informaciones sobre la modificación del contenido del caché mediante el proceso a analizar, por ejemplo un criptoalgoritmo. Una estrategia usual es el procedimiento evict-and-probe (desalojar y probar). Un proceso de análisis llena primeramente el caché con datos propios y mide a continuación tiempos de acceso a la memoria. Entonces pueden medirse por ejemplo aciertos de caché

(en inglés cache hits) o un fallo de caché (en inglés cache miss). Si se realiza este análisis a lo largo de un periodo de tiempo más largo, entonces pueden extraerse conclusiones relativas a los datos relevantes para la seguridad de un procedimiento de encriptado, por ejemplo claves criptográficas para el procedimiento AES y en el caso más desfavorable le resulta a un atacante posible reconstruir estos datos relevantes para la seguridad.

La figura 2 muestra un diagrama secuencial del procedimiento correspondiente a la invención 200 para proteger datos relevantes para la seguridad en una memoria caché.

El procedimiento 200 es capaz de no reproducir ya en una línea caché en el mismo bloque caché zonas de direcciones cuya dirección de memoria se diferencia sólo en un múltiplo de la máxima longitud de bloque de datos, tras una reorganización de la memoria caché.

Para proteger una copia de un bloque de datos que contiene datos relevantes para la seguridad frente a ataques de canal lateral, se fija al memorizar los datos en la memoria caché, caso de que no se haya hecho ya, un parámetro de ofuscación en una etapa del procedimiento 210. El parámetro de ofuscación es en este ejemplo de ejecución un bloque de números aleatorios.

Si debe tamponarse en la memoria caché el bloque de datos, que por ejemplo contiene los datos relevantes para la seguridad en forma de informaciones codificadas para un procedimiento criptográfico o bien debe archivarse una copia de los datos, se determina primeramente en una etapa del procedimiento 220 una dirección de bloque caché a partir de la dirección de memoria del bloque de datos.

Para depositar una copia del bloque de datos en la memoria caché, se determina adicionalmente una dirección de bloque a partir de la dirección de memoria y se forma un primer identificador de la dirección del bloque. Mediante la primera dirección de bloque caché debe resultarle posible al sistema de computadora depositar la copia del bloque de datos en la memoria caché y acceder a la copia del bloque de datos.

En una etapa del procedimiento 230 se genera mediante una función de generación, el parámetro de ofuscación y el primer identificador, a partir de la primera dirección de bloque caché, una primera dirección de bloque caché modificada. En este ejemplo de ejecución la función de generación es una función O-exclusivo, que se aplica bit a bit con el parámetro de ofuscación y el primer identificador a la primera dirección de bloque caché.

Por ejemplo para un primer identificador con una longitud de 52 bits, se amplía el mismo con dos bits 0 de cabecera a 54 bits. Estos 54 bits se reparten a continuación en nueve palabras de 6 bits w1 a w9. Adicionalmente se determina un parámetro de ofuscación o de 6 bits y la dirección de bloque caché de 6 bits sin modificar s, compuesta por los bits 7-12 de la dirección de memoria. La dirección de bloque caché modificada se genera entonces mediante la ecuación

$$A = w1 \oplus w2 \oplus \ldots \oplus w9 \oplus s \oplus o \quad \text{(fórmula 1)}$$

siendo "$\oplus$" XOR o bien la función O-exclusivo y A la dirección de bloque caché s modificada. Al respecto se aplican en cada caso una sobre otra bit a bit las distintas palabras de 6 bits, el parámetro de ofuscación de 6 bits y la dirección de bloque caché de 6 bits sin modificar mediante la función O-exclusivo.

Mediante la primera dirección de bloque caché modificada se fija dónde se encuentra un primer bloque caché en la memoria caché. La copia del primer bloque de datos y el primer identificador se memorizan a continuación en una etapa del procedimiento 240 en una primera línea caché del primer bloque caché.

La asociación de la primera dirección de bloque caché modificada a la primera dirección de bloque caché puede realizarse mediante una tabla. En esta tabla se inscribe la primera dirección de bloque caché modificada, una vez que la misma haya sido generada mediante la función de generación. Alternativamente puede calcularse también la tabla por completo con anterioridad.

Cuando luego ha de accederse al primer bloque de datos en la memoria caché, se utiliza la primera dirección de bloque caché, para determinar mediante la tabla la primera dirección de bloque caché modificada. Mediante la primera dirección de bloque caché modificada y el primer identificador se accede a continuación al bloque de datos en la memoria caché, en el caso de que este bloque de datos haya sido ya archivado en la memoria caché.

Para proteger los datos frente a ataques de canal lateral, se modifica el parámetro de ofuscación después de por ejemplo un número fijo o elegido aleatoriamente de 500 aciertos caché (en inglés cache hits) y se sustituye por nuevos números aleatorios. Mediante esta modificación debe primeramente reorganizarse la memoria caché, ya que una asociación de direcciones de bloque caché modificadas, por ejemplo la

primera dirección de bloque caché modificada y las correspondientes direcciones de bloque caché, por ejemplo la primera dirección de bloque caché, ya no son correctas.

Mediante la modificación del parámetro de ofuscación se logra que en una reorganización de la memoria caché los datos, que hasta ahora se tamponaban como copias en la primera línea caché del primer bloque caché, se reproduzcan en una nueva memorización de una copia sobre la segunda línea caché de un segundo bloque caché. Adicionalmente se reproducen ahora en este contexto copias de otros datos que se tamponaron en otras líneas caché del primer bloque caché, ahora como nuevas copias total o parcialmente en otras líneas caché de otros bloques caché.

En otras palabras, se fuerza por ejemplo después de 500 aciertos caché la reorganización de la memoria caché. Tras esta reorganización de la memoria caché ya no son accesibles las copias de los datos o bloques de datos en la memoria caché y se produce un fallo de caché. Entonces se escriben con el procedimiento correspondiente a la invención de nuevo copias de los datos que se encuentran en las zonas de dirección del campo de direcciones en la memoria caché y en consecuencia se estructura de nuevo la memoria caché.

La ventaja es que las zonas de direcciones cuya dirección de memoria se diferencia sólo en un múltiplo de la longitud de una línea caché, ya no se reproducen en una línea caché en el mismo bloque caché.

Al reorganizarse una y otra vez la memoria caché, ya no es posible deducir mediante la vigilancia de la memoria caché conclusiones relativas a los datos relevantes para la seguridad que se utilizan en un proceso.

La figura 3 es una representación esquemática de un módulo de ofuscación 300 correspondiente a la invención. El módulo de ofuscación 300 es una forma de ejecución posible de las reivindicaciones, que están orientadas a un sistema.

El módulo de ofuscación 300 presenta un primer equipo de determinación 310, un segundo equipo de determinación 320, un equipo de fijación 330, un primer equipo de generación 340 y un equipo de memoria 350, que están unidos entre sí mediante un bus de datos.

Cuando ha de memorizarse una copia de un bloque de datos en la memoria caché, determina primeramente el primer equipo de determinación 330 una primera dirección de bloque caché de una dirección de memoria del bloque de datos. El bloque de datos puede entonces contener los más diversos datos. Puede tratarse al respecto de datos que son accesibles públicamente. Pero también pueden ser por ejemplo datos referidos a personas, por ejemplo datos de clientes y datos relevantes para la seguridad, por ejemplo datos criptográficos, que sólo deben utilizar personas autorizadas para el acceso.

El segundo equipo de determinación 320 se utiliza para determinar una dirección de bloque de la dirección de memoria y a partir de la dirección de bloque formar un primer identificador. Pero también es posible utilizar la dirección de bloque directamente como primer identificador.

En el caso de que hasta ese momento no se haya fijado ningún parámetro de ofuscación, se fijan mediante el equipo de fijación 330 parámetros de ofuscación. El equipo de generación 340 genera entonces una primera dirección de bloque caché modificada para un primer bloque caché con un equipo de generación utilizando los parámetros de ofuscación, la primera dirección de bloque caché y el primer identificador. El equipo de memoria 350 memoriza entonces los datos relevantes para la seguridad junto con el primer identificador utilizando la primera dirección de bloque caché modificada en una primera línea caché del primer bloque caché.

La figura 4 muestra una representación esquemática de un sistema 400 correspondiente a la invención para memorizar datos en una memoria caché. El sistema 400 correspondiente a la invención utiliza un módulo de ofuscación 300 correspondiente a la invención, tal como se ha descrito en la figura 3.

El ejemplo de ejecución muestra la organización de una memoria caché, siendo k la cantidad de líneas caché por cada bloque caché ($k \geq 1$). La cantidad de bloques caché n resulta de n = tamaño del caché/(k*longitud de una línea caché).

Primeramente se reproducen los datos de un sistema de computadora en forma de bloques de datos en una memoria, que puede direccionarse mediante direcciones de memoria 110.

Con una dirección de memoria puede direccionarse en este ejemplo de ejecución en cada caso un byte. Cuando se memoriza un bloque de datos, ocupa el mismo al menos un byte y es accesible mediante una dirección de memoria. Las direcciones de memoria pueden asociarse en cada caso a distintas zonas de direcciones, para direccionar por ejemplo bloques de datos que ocupan varios bytes mediante una zona de direcciones con una dirección de memoria, que también se denomina dirección inicial.

En consecuencia está dividido el campo de direcciones en varias zonas de direcciones, en las cuales están archivados por ejemplo un primer bloque de datos 133, un segundo bloque de datos 143, un tercer bloque de datos 153, un bloque de datos m1 137, un bloque de datos m2 147 y un bloque de datos m3 157.

La memoria caché presenta usualmente varios bloques caché, que pueden alojar una copia de un bloque de datos del campo de direcciones. En la figura 4 se representa un primer bloque caché 430 con una primera dirección de bloque caché modificada 431, un segundo bloque caché 440 con una segunda dirección de bloque caché modificada 441 y un bloque de datos número n 450 con una dirección de bloque caché número n modificada 451. En detalle presenta un bloque caché una pluralidad de líneas caché, línea caché 1 hasta línea caché k, para memorizar en una línea caché uno de los bloques de datos 133, 143, 153, 137, 147, 157.

El primer bloque caché 430 reproducido está archivado en la primera dirección de bloque caché modificada 431 en la memoria caché, presentando el primer bloque caché 430 una pluralidad de líneas caché, en las que ha de archivarse una copia de los bloques de datos 133 y 147. En detalle se representan una primera línea caché 131 y una línea caché número k 135 para el primer bloque caché 430 en la figura 4, correspondiendo la línea caché número k 135 a la última línea caché en el primer bloque caché 430.

Cuando se carga una copia del primer bloque de datos 133 en la memoria caché, véase la figura 1, se forma a partir de una dirección de memoria 110 del bloque de datos 133 una dirección de bloque 111 y la primera dirección de bloque caché 112. Para ello se eligen por ejemplo en un sistema de 64 bits del bit 13 al bit 64 de la dirección de memoria 110 para la dirección de bloque 111 y de los bits 7 a 12 para la primera dirección de bloque caché 112. Los bits que no se utilizaron para formar la dirección de bloque 111 y la primera dirección de bloque caché 112, son bits 113 irrelevantes, que no se utilizan para ningún cálculo adicional.

La dirección de bloque 111 se utiliza entonces como un primer identificador 132. La primera dirección de bloque caché modificada 431, que se utiliza para direccionar el primer bloque caché 430 en la memoria caché y memorizar una copia del bloque de datos 133, se determina como sigue:

Primeramente se fija mediante un equipo de fijación 330 del módulo de ofuscación 300 un parámetro de ofuscación, en el caso de que aún no se haya fijado el mismo. Mediante un primer equipo de generación 340 del módulo de ofuscación 300, se genera entonces, utilizando una función de generación, el parámetro de ofuscación y el primer identificador 132, a partir de la primera dirección de bloque caché 112, la primera dirección de bloque caché modificada 431.

Si aún no se encuentra ninguna copia del bloque de datos 133 en la memoria caché, se elige y se borra una línea caché 131, por ejemplo el acceso utilizado con menos frecuencia o el que se encuentra más atrás en el bloque caché 430. En su lugar entra el bloque de datos actual 133. El primer identificador 132 se archiva igualmente, para hacer posible posteriormente, cuando se acceda al caché, una asociación inequívoca.

De la misma manera se archiva el bloque de datos m2 147 mediante una dirección de memoria m2 del bloque de datos m2 147 en la línea caché número k 135 del primer bloque caché 130. Para ello se determina de nuevo una dirección de bloque y a partir de la misma se forma un identificador m2 146.

Mediante el mismo procedimiento antes indicado se reproduce el segundo bloque de datos 143 mediante su segunda dirección de memoria en el segundo bloque caché 440. Aquí se determina igualmente una dirección de bloque, un segundo identificador 142 y una segunda dirección de bloque caché modificada para el segundo bloque caché 440 a partir de la segunda dirección de memoria.

Según el mismo procedimiento se reproducen el tercer bloque de datos 153 y el bloque de datos m3 157 en líneas caché del bloque caché n 150.

Mediante la primera dirección de bloque caché modificada 431 se fija así dónde se encuentra el primer bloque caché 430 en la memoria caché. La asociación de la primera dirección de bloque caché modificada 431 a la primera dirección de bloque caché 112 puede realizarse mediante una tabla. En esta tabla se inscribe la primera dirección de bloque caché modificada 431, una vez que la misma haya sido generada por la función de generación.

Si ahora debe accederse al primer bloque de datos 133 en la memoria caché, se utiliza la primera dirección de bloque caché 112 para determinar mediante la tabla la primera dirección de bloque caché modificada 431. Mediante la primera dirección de bloque caché modificada 431 y el primer identificador 132 se accede a continuación al bloque de datos 133 en la memoria caché, en el caso de que este bloque de datos 133 ya se haya archivado en la memoria caché.

Para proteger los datos frente a ataques de canal lateral, se modifica el parámetro de ofuscación después de por ejemplo 500 aciertos caché (en inglés cache hits) y se sustituye por nuevos números aleatorios. Mediante esta modificación ha de reorganizarse primeramente la memoria caché, ya que una asociación de direcciones de bloque caché modificadas, por ejemplo la primera dirección de bloque caché modificada, y las correspondientes direcciones de bloque caché, por ejemplo la primera dirección de bloque caché, ya no es correcta.

Mediante la modificación del parámetro de ofuscación se logra que en una reorganización de la memoria caché los datos que hasta ahora habían sido tamponados como copias en la primera línea caché del primer bloque caché, se reproduzcan en una nueva memoria de una copia sobre una segunda línea caché de un segundo bloque caché. Adicionalmente se reproducen entonces copias de otros datos que se tamponaron en otras líneas caché del primer bloque caché, ahora como nuevas copias, total o parcialmente en otras líneas caché de otros bloques caché.

En otras palabras, se fuerza por ejemplo después de 500 aciertos caché la reorganización de la memoria caché. Tras esta reorganización de la memoria caché, ya no son accesibles las copias de los datos o bloques de datos en la memoria caché y se produce un fallo de caché. Entonces se escriben con el procedimiento correspondiente a la invención de nuevo copias de los datos en la memoria caché y en consecuencia se construye de nuevo la memoria caché.

La ventaja es que las zonas de direcciones cuya dirección de memoria se diferencia sólo en un múltiplo de la longitud de una línea caché, ya no se reproducen en una línea caché en el mismo bloque caché.

Al reorganizarse una y otra vez la memoria caché, ya no es posible deducir mediante la vigilancia de la memoria caché conclusiones relativas a los datos relevantes para la seguridad que se utilizan en un proceso.

En los citados ejemplos de ejecución no se diferencia en cuanto a los datos que se tamponan en la memoria caché entre si se trata al respecto de datos relevantes para la seguridad o datos no críticos. Se presupone que básicamente todos los datos son datos relevantes para la seguridad.

En una variante de los citados ejemplos de ejecución, puede formarse para el acceso a un bloque de datos en la memoria caché la primera dirección caché modificada en un acceso mediante la función de generación, el primer identificador y el parámetro de ofuscación también directamente a partir de la primera dirección de bloque caché. Entonces se renuncia a la tabla, para por ejemplo ahorrar espacio de memoria en un procesador.

En otra variante de los citados ejemplos de ejecución se modifican los parámetros de ofuscación después de una cantidad predefinida de accesos con acierto a la memoria caché. Esto puede realizarse mediante un sencillo contador, que puede configurar un administrador mediante una interfaz del sistema, para tener en cuenta distintas exigencias de seguridad. No obstante una tal configuración podría realizarse por ejemplo también mediante una actualización del programa, por ejemplo como actualización (update) del firmware.

En otra variante más de los ejemplos de ejecución citados se modifican los parámetros de ofuscación mediante una solicitud de interrupción. Un sistema operativo puede ejecutar una pluralidad de medidas cuando detecta un ataque, para conducir a un estado seguro. Entre ellas se encuentra también provocar una reorganización o una modificación del parámetro de ofuscación activamente por parte del sistema operativo mediante una solicitud de interrupción.

En otra variante más de los ejemplos de ejecución citados se modifican los parámetros de ofuscación dentro de un intervalo de tiempo predeterminado. Esto puede realizarse por ejemplo mediante un sencillo reloj interno. En otra variante más puede configurar el administrador el reloj mediante una interfaz del sistema, para tener en cuenta distintas exigencias de seguridad. Una tal configuración podría realizarse por ejemplo también mediante una actualización del programa, por ejemplo como actualización (update) del firmware. Aún cuando la invención se ha ilustrado y descrito más en detalle mediante los ejemplos de ejecución, la invención no queda limitada por los ejemplos dados a conocer y el especialista puede deducir otras variaciones a partir de aquí. El ámbito de protección de la invención viene determinado por las reivindicaciones independientes 1 y 11.

REIVINDICACIONES

1. Procedimiento (200) para proteger datos relevantes para la seguridad en una memoria caché, archivándose una copia de los datos relevantes para la seguridad de una memoria general en la memoria caché, que presenta:
   - fijación (210) de parámetros de ofuscación;
   - determinación (220) de una primera dirección de bloque caché (112) de una dirección de memoria (110) de la memoria general, en la que están archivados los datos relevantes para la seguridad (133);
   - generación (230) de una primera dirección de bloque caché modificada (431) para un primer bloque caché (430) con una función de generación, utilizando el parámetro de ofuscación y la primera dirección de bloque caché (112) y
   - memorización (240) de la copia de los datos relevantes para la seguridad (132) utilizando la primera dirección de bloque caché modificada (431) en una primera línea caché (131) del primer bloque caché (430) y

   en el que los parámetros de ofuscación se modifican mediante una solicitud de interrupción.

2. Procedimiento (200) según la reivindicación 1,
   en el que se determina una dirección de bloque (111) a partir de la dirección de memoria (110), formándose un primer identificador (132) de la dirección de bloque (111) y
   en el que la función de generación utiliza adicionalmente la dirección de bloque (111) o el primer identificador (132) para generar la primera dirección de bloque caché modificada (431).

3. Procedimiento (200) según la reivindicación 2,
   en el que un acceso a los datos relevantes para la seguridad (133) en la memoria caché se realiza mediante el primer identificador (132), la primera dirección de bloque caché (112) y la función de generación y
   en el que la función de generación utiliza el parámetro de ofuscación, la primera dirección de bloque caché y el primer identificador (132) para generar la primera dirección de bloque caché modificada (431).

4. Procedimiento (200) según una de las reivindicaciones precedentes,
   en el que se realiza una modificación de los parámetros de ofuscación según reglas predeterminadas y
   en el que mediante la modificación de los parámetros de ofuscación se realiza una reorganización de la memoria caché.

5. Procedimiento (200) según la reivindicación 4,
   en el que en la reorganización se reproducen los datos de la primera línea caché (131) del primer bloque caché (430) en una segunda línea caché (141) de un segundo bloque caché (440) y
   en el que se reproducen otros datos de otras líneas caché del primer bloque caché (430) total o parcialmente en otras líneas caché de otros bloques caché.

6. Procedimiento (200) según una de las reivindicaciones precedentes,
   en el que la función de generación es una función que genera la primera dirección de bloque caché modificada mediante una permutación de la primera dirección de bloque caché (112) utilizando los parámetros de ofuscación y/o el primer identificador (132).

7. Procedimiento (200) según una de las reivindicaciones precedentes,
   en el que los parámetros de ofuscación se modifican tras una cantidad previamente definida de accesos con acierto a la memoria caché.

8. Procedimiento (200) según una de las reivindicaciones 1 - 6,
   en el que los parámetros de ofuscación se modifican dentro de un intervalo de tiempo predeterminado.

9. Procedimiento (200) según una de las reivindicaciones precedentes,
   en el que los parámetros de ofuscación contienen un número aleatorio, que con preferencia se forma de nuevo cuando tiene lugar un rearranque del sistema.

10. Procedimiento (200) según una de las reivindicaciones precedentes,
    en el que los parámetros de ofuscación contienen un identificador de hardware inequívoco.

11. Sistema (400) para proteger datos relevantes para la seguridad en una memoria caché, archivándose una copia de los datos relevantes para la seguridad de una memoria general en la memoria caché, que presenta:
    - un equipo de fijación (330), que está constituido para fijar parámetros de ofuscación;

- un primer equipo de determinación (310), que está constituido para determinar una primera dirección de bloque caché (112) de una dirección de memoria (110) de la memoria general en la que están archivados los datos relevantes para la seguridad (133);
- un primer equipo de generación (340), que está constituido para generar una primera dirección de bloque caché modificada (431) para un primer bloque caché (430) con un equipo de generación utilizando los parámetros de ofuscación y la primera dirección de bloque caché (112);
- un equipo de memoria (350), que está constituido para memorizar la copia de los datos relevantes para la seguridad (133) utilizando la primera dirección de bloque caché modificada (431) en una primera línea caché (131) del primer bloque caché (430) y

en el que los parámetros de ofuscación se modifican mediante una solicitud de interrupción.

12. Sistema (400) según la reivindicación 11,
tal que el sistema presenta un segundo equipo de determinación (320), que está constituido para determinar una dirección de bloque (111) a partir de la dirección de memoria (110),
formándose un primer identificador (132) de la dirección de bloque (111) y utilizando el equipo de generación adicionalmente la dirección de bloque (111) o el primer identificador (132) para generar la primera dirección de bloque caché modificada (431).

13. Sistema (400) según la reivindicación 12,
tal que el sistema presenta un equipo de acceso, que está constituido para acceder a los datos relevantes para la seguridad (133) en la memoria caché mediante el primer identificador (132), la primera dirección de bloque caché (112) y el equipo de generación, utilizando el equipo de generación el parámetro de ofuscación, la primera dirección de bloque caché y el primer identificador (132) para generar la primera dirección de bloque caché modificada (431) para el acceso en la memoria caché.

14. Sistema (400) según una de las reivindicaciones precedentes,
en el que está constituido un equipo de modificación para modificar los parámetros de ofuscación según reglas predeterminadas y en el que se realiza mediante la modificación de los parámetros de ofuscación una reorganización de la memoria caché.

15. Sistema (400) según una de las reivindicaciones precedentes,
en el que el equipo de generación es un equipo de permutación, que genera la primera dirección de bloque caché modificada (431) mediante una permutación de la primera dirección de bloque caché (112) utilizando los parámetros de ofuscación y el primer identificador (132).

16. Sistema (400) según una de las reivindicaciones precedentes,
en el que el primer equipo de determinación y el segundo equipo de determinación están constituidos como un equipo de determinación integral.

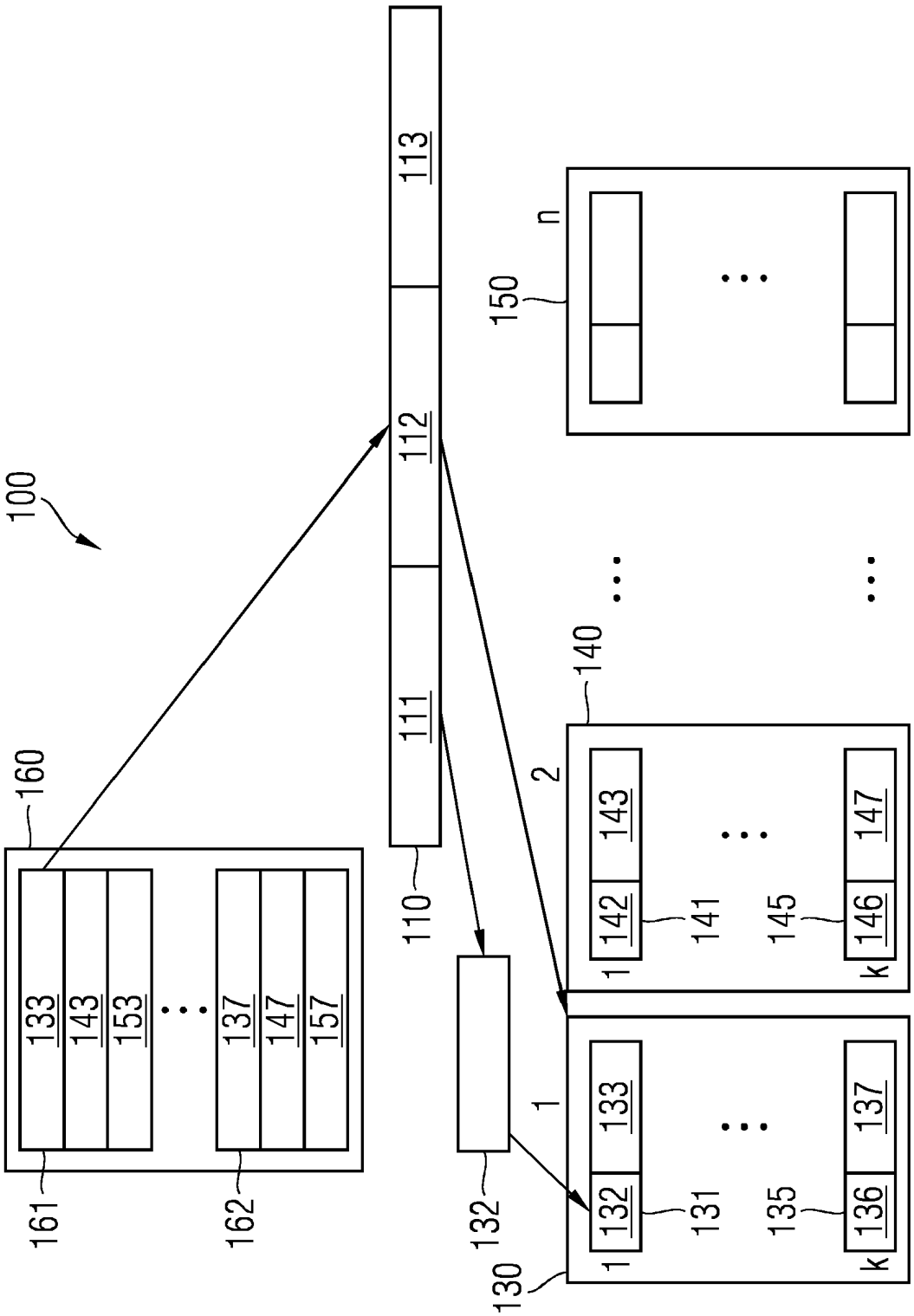

100
160
161
162
133
143
153
137
147
157
110
111
112
113
132
130
131
135
140
141
145
142
146
150
n
1
2
k

FIG 1

FIG 2

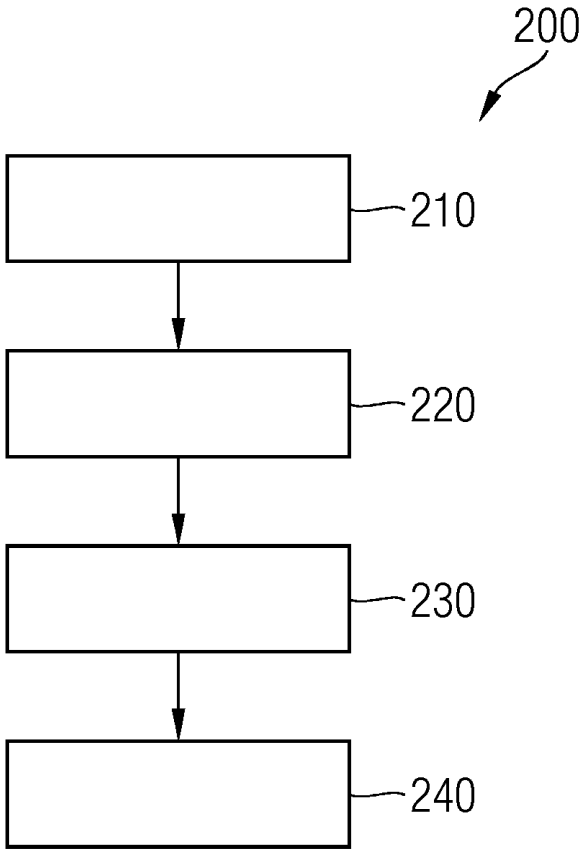
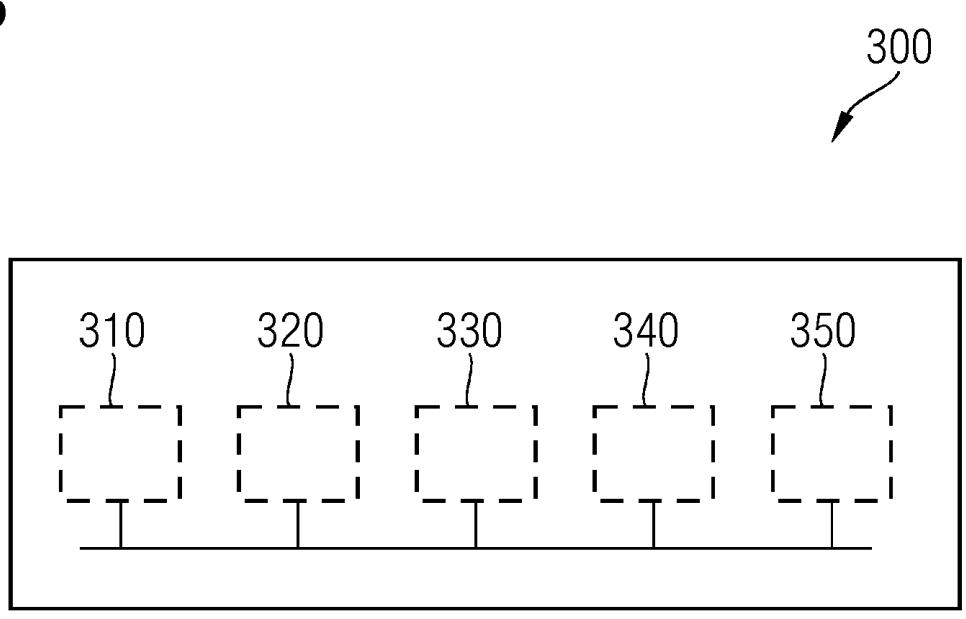


FIG 3



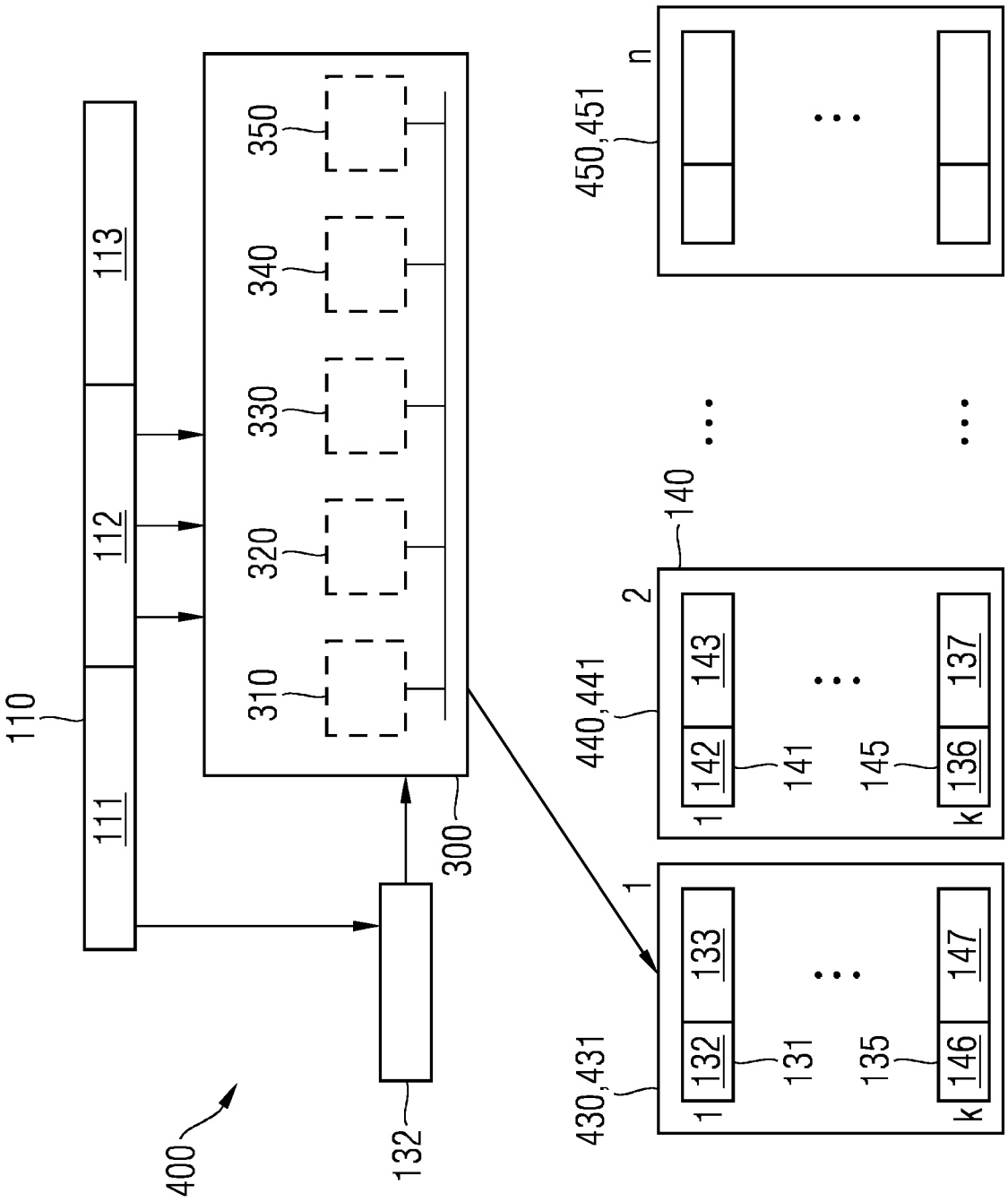

110
111
112
113
310
320
330
340
350
300
400
132
430,431
440,441
450,451
140
1
2
n
131
135
141
145
146
147
142
143
136
137
133

FIG 4