(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 770 679**

(51) Int. CI.:

G09C 1/10 (2006.01)
G06F 21/72 (2013.01)
H04L 9/16 (2006.01)
G06F 15/78 (2006.01)
G06F 21/74 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.12.2014 E 14199603 (3)**

(97) Fecha y número de publicación de la concesión europea: **08.01.2020 EP 2889855**

(54) Título: **Procedimiento de diseño de una arquitectura reconfigurable de tratamiento de un conjunto de operaciones multinivel de seguridad**

(30) Prioridad:

26.12.2013 FR 1303087

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.07.2020

(73) Titular/es:

THALES (100.0%)
45, rue de Villiers
92200 Neuilly Sur Seine, FR

(72) Inventor/es:

SALIBA, ERIC;
DICKLIC, LAURENT y
GRISAL, OLIVIER

(74) Agente/Representante:

SALVÀ FERRER, Joan

DESCRIPCIÓN

Procedimiento de diseño de una arquitectura reconfigurable de tratamiento de un conjunto de operaciones multinivel de seguridad

[0001] La presente invención se refiere a un procedimiento de diseño de una arquitectura de tratamiento de un conjunto de operaciones que se efectuarán sobre datos. La presente invención se refiere igualmente a un programa informático adaptado para la implementación de dicho procedimiento y a una arquitectura de tratamiento de un conjunto de operaciones.

[0002] De manera general, la invención se sitúa en el campo del tratamiento de datos seguros que requieren niveles de protección distintos por medio de una arquitectura de tratamiento. Formulada de manera general, la problemática asociada a este campo es garantizar la integridad, la autenticidad, la compartimentación y el dominio de los tratamientos de operaciones aplicadas a datos que requieren niveles de protección diferentes dentro de un mismo sistema.

[0003] Para responder a esta problemática se imponen limitaciones en la arquitectura de los tratamientos de las operaciones aplicadas a los datos. Estas limitaciones varían principalmente en función de la naturaleza de los tratamientos considerados. En concreto, por ejemplo, las operaciones son operaciones de corte, de recurso y de gestión de clave o de parámetros criptográficos. Las limitaciones dependen también del nivel de protección requerido por los datos. Además, las limitaciones dependen también del nivel de protección requerido por las operaciones.

[0004] Por tanto, es deseable que la arquitectura de tratamiento permita garantizar que cuando se efectúa cada operación, el nivel de protección sea suficiente en lo que respecta a las diferentes limitaciones mencionadas anteriormente.

[0005] El documento US-2004/123119-A1 describe procedimientos y aparatos previstos para el desacoplamiento de una interfaz de acelerador de criptografía de núcleo de tratamiento criptográfico. Un recurso compartido alimenta la interfaz de acelerador de criptografía, incluyendo el recurso varios puertos de entrada. Se prevén referencias a los datos en el recurso compartido para permitir el tratamiento y el control de datos con vistas a su tratamiento por núcleos de tratamiento criptográfico sin una cantidad sustancial de memoria intermedia separada en los caminos de datos de tratamiento de criptografía.

[0006] El documento US-6.408.074-B1 describe un dispositivo de cifrado que puede configurarse para ejecutar diferentes tipos de algoritmos criptográficos y efectuar más de un algoritmo simultáneamente. El dispositivo es accionado por una fuente externa y se implementa con una arquitectura de hardware que presenta la eficacia de los dispositivos de cifrado clásicos basados en hardware, así como la flexibilidad de las soluciones basadas en programas de software.

[0007] El documento US-2010/027782-A1 describe un dispositivo de flujo de datos de tratamiento en una unidad de comunicación con dos regiones mutuamente separadas para el tratamiento de la información que suministran al menos dos caminos de mensajes distintos. Los caminos de mensajes están conectados respectivamente a un mensaje emisor y a un receptor de mensajes en el que, para cada camino de mensaje, se prevé un módulo de codificación que está conectado a la vez con la primera región de tratamiento de datos y también con una segunda región de tratamiento de datos. Además, en la segunda región de tratamiento de datos, se prevé una unidad de distribución que está conectada con los caminos de mensaje de la primera región de tratamiento de datos y con todos los módulos de codificación de los caminos de datos correspondientes con el fin de distribuir mensajes dados de manera dirigida.

[0008] El documento US-2012/036.581-A1 describe un equipo de seguridad colocado entre al menos un campo que tiene un nivel de confianza o un nivel de sensibilidad A y al menos un campo que tiene un nivel de confianza o de sensibilidad B, sabiendo que el nivel A es diferente del nivel B. El equipo incluye al menos los elementos siguientes: una capa de software de virtualización V implementada en la capa física H y dispuesta entre dicha capa física H y al menos un conjunto constituido por al menos tres bloques compartimentados diferentes y que presentan niveles de sensibilidad diferentes, BLA, BLB, MDS, de manera que dichos bloques compartimentados se apoyan en la capa física H y la capa de virtualización y dichos bloques están constituidos por al menos uno de los elementos tomados de entre la lista siguiente:

- un bloque de red A, BLA, que incluye el conjunto de funciones de red que permite tratar los datos de nivel de seguridad A,
- un bloque de red B, BLB, que incluye el conjunto de funciones de red que permite tratar los datos de nivel de seguridad B,
- un bloque de módulo de seguridad, MDS, o SAS dispuesto entre al menos un bloque de tipo BLA y al menos un bloque de tipo BLB, estando dicho módulo de seguridad adaptado para controlar los intercambios de datos entre dichos bloques BLA y BLB, incluyendo dicho módulo de seguridad el conjunto de transformaciones de seguridad,

de filtrado o de funciones criptográficas.

[0009] Además, los documentos US-A-6.026.490, US-A-6.101.255, US-A-6.845.446, US-A-7.200.229 y US-A-7.444.565 proponen arquitecturas de tratamiento que presentan recursos programables como estructuras de tipo ASIC. Una estructura de tipo ASIC (ASIC es el acrónimo del inglés «Application-Specific Integrated Circuit» o «circuito integrado específico de una aplicación») es un circuito integrado dedicado a una aplicación particular.

[0010] Sin embargo, para cada una de estas arquitecturas propuestas, la reconfigurabilidad asociada es débil.

[0011] Por tanto, existe la necesidad de un procedimiento que permita diseñar una arquitectura de tratamiento propia para tratar datos y que presente una reconfigurabilidad mejorada a la vez que garantiza el nivel de protección requerido para los datos para cuyo tratamiento es adecuada la arquitectura.

[0012] Según la invención, este objeto se consigue por medio de un procedimiento de diseño de una arquitectura de tratamiento de un conjunto de operaciones efectuadas sobre datos, requiriendo algunos datos un nivel de protección, de manera que el conjunto de las operaciones efectuadas sobre datos requiere un nivel de protección superior a un nivel de protección umbral que incluye al menos dos subconjuntos de operaciones que pueden realizarse en paralelo. El procedimiento comprende una etapa de determinación de diferentes subconjuntos de operaciones del conjunto de las operaciones, comprendiendo cada subconjunto operaciones para realizar sobre datos que requieren un nivel de protección superior a un nivel de protección umbral y pudiendo realizarse cada subconjunto de operaciones en paralelo con otros subconjuntos de operaciones. El procedimiento incluye también una etapa de determinación, para cada subconjunto de operaciones, del nivel de protección más elevado requerido por los datos en los que se efectúan las operaciones del subconjunto, y una etapa de generación, para cada subconjunto de operaciones, de un bloque de tratamiento en la arquitectura de tratamiento que se va a diseñar, de manera que el bloque de tratamiento comprende un subbloque de cálculo dedicado únicamente a la ejecución de las operaciones del subconjunto sobre datos que serán tratados por el bloque de tratamiento cuyo nivel de protección depende del nivel de protección determinado para el subconjunto de operaciones considerado y un subbloque de protección capaz de garantizar la protección de los datos que serán tratados por el bloque de tratamiento. El procedimiento comprende igualmente una etapa de generación de al menos un conmutador capaz de encaminar, hacia cada bloque de tratamiento, los datos para tratar, en el que el procedimiento comprende, además, una etapa de:

- determinación de las operaciones para realizar sobre datos cuyo nivel de protección es inferior al nivel de protección umbral, y
- generación, para cada una de las operaciones determinadas, de una unidad de tratamiento de la operación, siendo las unidades de tratamiento distintas de los bloques de tratamiento,
- determinación entre las operaciones efectuadas sobre datos cuyo nivel de protección es inferior al nivel de protección umbral, de las operaciones redundantes, y
- eliminación para las operaciones redundantes determinadas, de una de las dos operaciones redundantes.

[0013] Según realizaciones particulares, el procedimiento comprende una o varias de las características siguientes, tomadas de forma aislada o según todas las combinaciones técnicamente posibles:

- cada bloque de tratamiento es capaz de proteger datos cuyo nivel de protección es igual al nivel de protección determinado para el subconjunto de operaciones para el que se genera el bloque de tratamiento,
- el procedimiento comprende, además, una etapa de determinación de los datos que serán tratados por el bloque de tratamiento que proviene de una unidad de tratamiento,
- cada subbloque de cálculo es capaz de obtener datos tratados por ejecución de las operaciones del subconjunto sobre los datos que serán tratados por el bloque de tratamiento, comprendiendo el procedimiento, además, una etapa de determinación de los datos para encaminamiento hacia una o varias unidades de tratamiento entre los datos tratados por cada subbloque de cálculo y una etapa de generación de al menos un conmutador de datos capaz de encaminar los datos determinados hacia la o las unidades de tratamiento,
- el procedimiento se implementa mediante ordenador.

[0014] La invención se refiere también a un producto de programa informático que incluye instrucciones de código de programación aptas para ser implementadas por un procesador, siendo el procesador capaz de implementar el procedimiento tal como se ha descrito anteriormente.

[0015] Además, la invención se refiere también a una arquitectura de tratamiento obtenida por la implementación del procedimiento tal como se ha descrito anteriormente.

[0016] Otras características y ventajas de la invención se desprenderán de la lectura de la descripción que se ofrece a continuación de realizaciones de la invención, ofrecida únicamente a modo de ejemplo y con referencia a los dibujos, que son:

- figura 1, una vista esquemática de una arquitectura 10 que se va a diseñar,

- figura 2, un diagrama de flujo del ejemplo de procedimiento de diseño según la figura 1, y
- figura 3, una vista esquemática de un ejemplo de arquitectura obtenida por la implementación del procedimiento de la figura 2.

[0017] La figura 1 representa una arquitectura 10 que se va a diseñar que presenta dos componentes elementales 12 también denominados bloques de tratamiento, elementos de entrada 14, 16 y 17 suministrados a los dos componentes elementales, los resultados 18 obtenidos después del uso de cada componente elemental 12, un componente de servicio genérico 19 y conmutadores 20.

[0018] La arquitectura de tratamiento que se va a diseñar es capaz de efectuar operaciones sobre datos. Por ejemplo, la arquitectura de tratamiento es un autómata para operaciones bancarias que permite transacciones financieras o incluso operaciones de cifrado de tipo protección de comunicación o de transmisión en redes.

[0019] A modo de ejemplo, en lo sucesivo se detalla únicamente el primer componente elemental 10, entendiéndose que el segundo componente elemental 10 presenta una estructura análoga al primer componente elemental 10.

[0020] El primer componente elemental 10 incluye un subbloque de cálculo 21 y un subbloque de protección local 22. A modo de ejemplo, el subbloque de cálculo 21 es una parte de un FPGA, de un ASIC o de una arquitectura programable.

[0021] El subbloque de cálculo 21 corresponde normalmente a una implementación que asegura tratamientos criptográficos en los datos de entrada. Los elementos de entrada del subbloque de cálculo 21 corresponden por una parte a los datos tratados en los que el subbloque de cálculo 21 realiza operaciones y elementos correspondientes a datos y parámetros que permiten la configuración de las operaciones que realiza el subbloque de cálculo 21.

[0022] El subbloque de cálculo 21 asegura operaciones sobre los datos tratados y sobre los datos y parámetros de configuración de entrada con o sin resultado 18 y con o sin llamada al componente de servicios genéricos 19 por medio del subbloque de protección local 22.

[0023] Los primeros elementos de entradas 14 son los datos que serán tratados por el subbloque de cálculo 21. Las operaciones realizadas por el subbloque de cálculo 21 se dirigen prioritariamente a los primeros elementos de entrada 14.

[0024] Los datos requieren un nivel de protección diferente según los datos considerados. Normalmente, algunos datos son datos que requieren un nivel de protección débil o incluso nulo mientras que otros datos son datos críticos que requieren un nivel de protección muy elevado. A modo de ejemplo, los importes de una transacción bancaria y la verificación de los códigos de identificación del portador son datos que implican un nivel de protección no nulo.

[0025] De manera general, el nivel de protección de un dato depende de las limitaciones relacionadas con los campos de aplicación que definen reglas en función de los niveles de las sensibilidades pretendidas (por ejemplo, marco regulador para los usos de defensa o gubernamentales, limitaciones bancarias, ...).

[0026] En lo sucesivo, para simplificar, el nivel de protección se representará mediante un número, de manera que un número más alto corresponde a un nivel de protección más elevado.

[0027] Los segundos elementos de entradas 16 son datos de tratamiento como claves criptográficas o valores de referencia (contraseña o código) que permiten la configuración de las diferentes operaciones que pueden efectuarse sobre los datos de entrada. Por ejemplo, en el caso del autómata para operaciones bancarias, las operaciones son el cifrado, la verificación de integridad o de autenticidad del importe de una transacción o de una compensación bancaria. Algunas operaciones se efectúan de manera sistemática mientras que otras operaciones dependen de las preferencias del usuario del autómata.

[0028] Los terceros elementos de entradas 17 son la totalidad o una parte de la implementación de las operaciones del bloque de tratamiento 12. Estos elementos corresponden por ejemplo a la máscara, al flujo de bits FPGA o al archivo de configuración del bloque de tratamiento 12 que contiene el conjunto o una parte de las operaciones que realiza el bloque.

[0029] El componente elemental 10 asegura la protección de la integridad y la confidencialidad del conjunto de las operaciones que realiza el subbloque de cálculo 21. El componente elemental 10 asegura la protección del conjunto de elementos de entrada desde su introducción hasta su borrado. El componente elemental 10 asegura igualmente la compartimentación de los tratamientos y los datos con respecto a otros componentes elementales de nivel diferentes.

[0030] El subbloque de protección local 22 del primer componente elemental 10 asegura una desensibilización

de los datos tratados antes de su envío hacia el componente de servicios genéricos 19.

[0031] El componente de servicios genéricos 19 puede ser distribuido solidariamente para un conjunto de componentes elementales 10 de niveles de sensibilidad diferentes conectados por medio de protección local. Estos servicios genéricos manipulan datos no sensibles (por ejemplo, del nivel de seguridad más bajo) y corresponden por ejemplo a un servicio de almacenamiento.

[0032] Cada componente elemental 10 es así capaz de exportar o importar datos 'no sensibles' obtenidos del componente de servicios genéricos 19 (por ejemplo, por memorización) por medio de su subbloque de protección local 22.

[0033] El subbloque de protección local 22 implementa así un conjunto de operaciones llamadas de 'protección local' que garantizan la protección por el bloque de tratamiento 12 en cuanto a integridad y confidencialidad de los elementos de entrada.

[0034] Esta protección local es del nivel apropiado y puede configurarse por medio de los elementos de entrada 16 y 17.

[0035] A partir de los elementos de entradas 14, 16 y 17, el componente elemental 10 es capaz de efectuar sobre los datos operaciones con el nivel de protección apropiado. El componente elemental 10 es así capaz de obtener los datos que se deben calcular con el nivel de protección apropiado. El conjunto de estos datos es el resultado 18.

[0036] Para diseñar la arquitectura de tratamiento en su totalidad se incluyen varios componentes elementales 10.

[0037] Por tanto, conviene usar los conmutadores 20 para encaminar los datos de entradas hacia los bloques de tratamientos 12 pero también los datos calculados por los bloques de tratamiento 12 hacia un usuario de la arquitectura de tratamiento.

[0038] Preferentemente, se usa asimismo un componente de servicios genéricos 19 (que comparten los componentes elementales 10) con la reserva de que se garantice la protección de los datos transmitidos por medio de un subbloque de protección local 22 que garantiza así una compartimentación por la cifra de estos datos antes del tratamiento por el componente de servicios genéricos. En este caso, conviene asimismo garantizar el encaminamiento de cada dato desde interfaces externas no representadas en la figura 1 y entre los componentes elementales 10 y el componente de servicios genéricos 19 hacia los bloques de tratamiento 12 apropiados. Para ello se propone usar igualmente los conmutadores 20 adecuados para encaminar los datos hacia los componentes elementales 10 y el componente de servicios genéricos 19.

[0039] Para obtener dicha arquitectura 10, se propone implementar un procedimiento de diseño de arquitectura de tratamiento 10, por ejemplo, como el procedimiento ilustrado por la figura 2.

[0040] El procedimiento incluye una etapa 100 de determinación de los diferentes subconjuntos de operaciones que tienen dos propiedades acumulativas.

[0041] Por una parte, las operaciones de los subconjuntos de operaciones se aplican sobre datos que requieren un nivel de protección superior a un umbral dado. Con tal de que se elija un umbral suficientemente elevado, esto permite seleccionar solo las operaciones que manipulan datos considerados sensibles para la aplicación pretendida. Esto permite aplicar la etapa 100 de determinación solo a los datos sensibles, implementándose la determinación de manera automatizada.

[0042] Por otra parte, los subconjuntos se aplican a operaciones que pueden realizarse en paralelo. Esto permite acelerar el cálculo de las diferentes operaciones por medio de la arquitectura de tratamiento que se va a diseñar.

[0043] El procedimiento de diseño incluye igualmente una etapa 102 de determinación para cada subconjunto de operaciones del nivel de protección más elevado requerido por los datos en los que se efectúan las operaciones del subconjunto.

[0044] Por ejemplo, si un subconjunto incluye tres operaciones sucesivas efectuadas respectivamente en un dato que requiere una protección de nivel dos, un dato que requiere una protección de nivel tres y un dato que requiere una protección de nivel cinco, el nivel de protección más elevado determinado es el nivel de protección cinco.

[0045] El procedimiento de diseño incluye entonces una etapa 104 de generación para cada subconjunto de operaciones de un bloque de tratamiento 12 en la arquitectura 10 de tratamiento para diseñar.

[0046] Cada bloque de tratamiento 12 incluye una entrada y una salida y así es adecuado para realizar operaciones sobre los datos de entrada con el fin de obtener datos de salida.

[0047] Para ello, cada bloque de tratamiento 12 incluye un subbloque de cálculo 21 y un subbloque de protección local 22, de manera que estos dos subbloques 21, 22 pueden confundirse según la arquitectura 10 deseada.

[0048] Más en concreto, cada subbloque de cálculo 21 está dedicado a la ejecución de las operaciones del subconjunto para el que se genera el bloque de tratamiento 12. Esto significa que, en funcionamiento, el subbloque de cálculo 21 es capaz de efectuar únicamente las operaciones del subconjunto de tratamiento para el que se genera el bloque de tratamiento 12. Sin embargo, como se indica anteriormente, en ciertas realizaciones, en funcionamiento, el subbloque de cálculo 21 solo efectúa algunas de las operaciones del subconjunto de tratamiento para el que se genera el bloque de tratamiento 12.

[0049] Además, cada subbloque de protección 21 es capaz de proteger datos cuyo nivel de protección depende del nivel de protección determinado para el subconjunto de operaciones consideradas. En lo que sigue de la descripción, el nivel de protección del bloque de tratamiento designa el nivel de protección de los datos que el subbloque de protección y por tanto el bloque de tratamiento es capaz de proteger.

[0050] A modo de ejemplo, la dependencia entre el nivel de protección del bloque de tratamiento y el nivel de protección máximo determinado es una relación lineal.

[0051] Así, según una realización, para dos subconjuntos de operaciones cuyo nivel de protección máximo es respectivamente dos y cinco, los niveles de protección de los bloques de tratamiento generados son, por ejemplo, tres y seis. Esta regla de dependencia permite adaptar el nivel de protección del bloque de tratamiento al nivel máximo a la vez que se prevé un margen de protección, que garantiza un buen nivel de protección. Además, la arquitectura 10 de tratamiento diseñada permite tratar cada dato con el nivel de protección requerido.

[0052] Según otra realización, la dependencia es una igualdad. Para el ejemplo anterior en el que para dos subconjuntos de operaciones el nivel de protección máximo es dos y cinco, los niveles de protección de los bloques de tratamiento 12 suministrados son entonces dos y cinco. Esto permite dimensionar la protección de los bloques de tratamiento 12 al valor más exacto con respecto a los datos tratados. También en esta realización, la arquitectura 10 de tratamiento diseñada permite asimismo tratar cada dato con el nivel de protección requerido.

[0053] Como salida de la etapa 104 de generación de bloques de tratamiento, se conocen todos los componentes elementales 10. Así pues, conviene estudiar la manera de ensamblar los bloques de tratamientos para formar la arquitectura de tratamiento. Preferentemente, para esto, como se ha explicado para el caso particular de la figura 1, conviene conectar los bloques de tratamientos con ayuda de conmutadores y distribuir solidariamente las operaciones no efectuadas por los componentes elementales 10. Las operaciones no efectuadas son normalmente operaciones menos críticas desde el punto de vista de la seguridad.

[0054] El procedimiento de diseño comprende igualmente una etapa 106 de determinación de las operaciones para realizar sobre datos cuyo nivel de protección es inferior al nivel de protección umbral. Los datos cuyo nivel de protección es inferior al nivel de protección umbral son considerados datos desensibilizados. En consecuencia, las operaciones determinadas en la etapa sensible de determinación son operaciones denominadas no seguras.

[0055] De manera opcional, el procedimiento de diseño incluye, cuando las operaciones no seguras son redundantes, una etapa 108 de determinación entre las operaciones efectuadas sobre datos cuyo nivel de protección es inferior al nivel de protección umbral de las operaciones de la misma naturaleza.

[0056] Esta etapa de determinación 108 se sigue de una etapa 110 de eliminación de las operaciones no seguras redundantes. Las operaciones no seguras son redundantes si efectúan la misma operación sobre datos idénticos o diferentes. Por ejemplo, si una primera operación consiste en sumar veinte y treinta y una segunda operación en sumar treinta y cuarenta, solo se conserva una operación no segura de las sumas de los dos números. Esto permite distribuir solidariamente las operaciones no efectuadas por los componentes elementales 10 y definir el componente de servicios genéricos 19 presentado en la figura 1.

[0057] El procedimiento de diseño comprende a continuación una etapa 112 de generación para cada una de las operaciones determinadas en la etapa de determinación 106, de una unidad de tratamiento de las operaciones determinadas, siendo la unidad de tratamiento distinta de cada uno de los bloques de tratamiento generados en la etapa 104.

[0058] En el caso en que las operaciones redundantes se hayan eliminado, esto permite disminuir el número de unidades de tratamiento a la vez que se conserva la misma precisión en los cálculos.

[0059] El procedimiento incluye igualmente una etapa 114 de determinación de los datos de entrada de los

bloques de tratamiento 12 y de las unidades de tratamiento de las que provienen los datos determinados. Asimismo, el procedimiento comprende también la determinación de los datos en salida de los bloques de tratamiento 12 y de las unidades de tratamiento que usan los datos obtenidos de los bloques.

[0060] El procedimiento incluye también una etapa 116 de generación de al menos un primer conmutador 20 capaz de encaminar hacia cada bloque de tratamiento 12 los datos para tratar y de al menos un segundo conmutador 20 capaz de encaminar los datos tratados hacia el o las unidades de tratamiento.

[0061] Más exactamente, el al menos un primer conmutador 20 es capaz de encaminar los datos determinados hacia la entrada de los bloques de tratamiento 12 apropiada mientras que el al menos un segundo conmutador 20 es capaz de encaminar los datos determinados obtenidos en salida de los bloques de tratamiento 12 hacia la o las unidades de tratamiento apropiadas.

[0062] El procedimiento incluye finalmente una etapa 118 de generación de la arquitectura 10 de tratamiento completa que retoma los bloques de tratamiento 12, las unidades de tratamiento y los conmutadores 20 y en su caso añade uniones entre estos diferentes elementos.

[0063] Esto permite obtener una arquitectura 10 de tratamiento que presenta un nivel de protección adaptado a los datos tratados en particular. Así, al contrario de lo indicado en el estado de la técnica en el que el nivel de protección de cada una de las operaciones para su realización por la arquitectura de tratamiento es el del dato que tiene un nivel de protección máximo, el nivel de protección de cada una de las operaciones para su realización está adaptado al nivel de protección de los datos tratados. Esto permite reducir las limitaciones de seguridad aplicadas a algunas de las operaciones.

[0064] Además, dicha arquitectura 10 de tratamiento se implementa de manera reconfigurable, de forma que es posible implementar el procedimiento para optimizar arquitecturas de tratamiento existentes.

[0065] Además, este procedimiento se aplica a diferentes tipos de soportes. Así, según los casos, la arquitectura diseñada se implementa con ayuda de un FPGA, de una arquitectura programable o de ASIC.

[0066] La figura 3 ilustra un ejemplo de arquitectura de tratamiento 200 obtenida con ayuda del procedimiento de diseño. La arquitectura de tratamiento 200 es capaz de efectuar operaciones sobre un flujo de datos. Las operaciones permiten convertir datos sensibles en datos no sensibles y al contrario, mientras que otras operaciones se aplican en datos sensibles para obtener otros datos sensibles y otras operaciones sobre datos no sensibles para obtener otros datos no sensibles. Por ejemplo, se usan operaciones de cifrado y de descifrado. En lo que sigue de la descripción, se asocia un color a los datos en función de su carácter sensible en relación con la seguridad de la arquitectura de tratamiento 200. Los datos rojos son los datos llamados sensibles, como claves, contraseñas o números de cuenta, mientras que los datos negros son los datos no sensibles. Formulado en otros términos, esto significa que el nivel de protección requerido por los datos rojos es estrictamente superior al nivel de protección requerido por los datos negros.

[0067] La arquitectura de tratamiento 200 incluye un conjunto de interfaces de usuario para los datos rojos 202, un primer nivel de conmutadores 204, un conjunto de bloques de tratamiento 206, un segundo nivel de conmutadores 208 y un conjunto de interfaces de usuario para los datos negros 210.

[0068] El conjunto de interfaces de usuario para los datos rojos 202 permite el acceso a los servicios de corte o de recurso accesibles a los datos rojos.

[0069] El conjunto de interfaces de usuario para datos rojos 202 incluye una unidad de tratamiento de servicio externo de administración 212, una unidad de tratamiento de servicios externos de corte o de recurso 214, una unidad de tratamiento de servicios externos de inyección local 216, una unidad de administración general 218, una unidad de tratamiento de borrado de urgencia 220 y una unidad de protección local de administración 222.

[0070] La unidad de tratamiento de servicios externos de administración 212 permite el acceso a servicios de administración.

[0071] En el caso de la figura 3, los servicios de administración accesibles a la unidad de tratamiento de servicios externos de administración 212 son el borrado de urgencia, el acceso a una interfaz hombre-máquina (a menudo designada con el acrónimo IHM) y la autenticación. Para esto, la unidad de tratamiento de servicios externos de administración 212 está en interacción con una subunidad IHM 224 apropiada para suministrar una interfaz hombre-máquina, una subunidad de borrado de urgencia 226 apropiada para proceder a un borrado de urgencia y una subunidad de autenticación 228 apropiada para obtener una autenticación de la persona. Cada una de estas interacciones se muestra en la figura 3 por una flecha doble.

[0072] Además, la unidad de servicios externos de administración 212 está también conectada con la unidad de administración general 218 y la unidad de tratamiento del borrado de urgencia 222.

[0073] La unidad de tratamiento de servicios externos de corte o de recurso 214 permite el acceso a los servicios de corte por medio de una subunidad de servicio de corte 230 (inserción de datos externos) y una subunidad de servicio de recurso 232 (solicitud de datos hacia un servidor) con las que la unidad de tratamiento de servicios externos de corte o de recurso 214 es capaz de interaccionar. Esta capacidad de interacción se muestra mediante flechas dobles en la figura 3.

[0074] La unidad de tratamiento de servicios externos de inyección local 216 permite la carga de datos criptográficos directamente hacia un conjunto 206 de bloque de tratamiento. Los datos criptográficos se obtienen de varias subunidades. Así, la unidad de tratamiento de servicios externos de inyección local 216 está en interacción con una subunidad de criptografía 234, una subunidad de inserción de datos rojos 236 y una subunidad de inserción de datos negros 238. Cada una de estas interacciones se muestra en la figura 3 por una flecha doble. La subunidad de criptografía 234 permite convertir datos negros en datos rojos.

[0075] De manera general la unidad de administración general 218 permite garantizar la configuración estática o dinámica de los niveles de conmutadores 204, 208 y permite el inicio de las diferentes interfaces e interconexiones de la arquitectura de tratamiento 200.

[0076] Más exactamente, en el caso concreto de la figura 3, la unidad de administración general 218 está en interacción con una unidad de tratamiento de servicios externos de administración 212 como se menciona anteriormente. Además, la unidad de administración general 218 está asimismo en interacción con la unidad de tratamiento de protección local administrativa 222 y la unidad de tratamiento de gestión del borrado de urgencia 220.

[0077] La unidad de tratamiento del borrado de urgencia 220 puede garantizar el borrado de datos rojos bajo el control de la unidad de administración general 218. Las condiciones que llevan al borrado de datos dependen de la política de borrado definida para el diseño de la arquitectura 200.

[0078] La unidad de tratamiento de protección local administrativa 222 asegura la protección de la unidad de administración general 218.

[0079] El primer nivel de conmutación 204 es capaz de llevar datos desde el conjunto de interfaces de usuario para datos rojos 202 hacia el bloque de tratamiento 206 o datos rojos obtenidos después del tratamiento del bloque de tratamiento 206 hacia el conjunto de interfaces de usuario para datos rojos 202.

[0080] El primer nivel de conmutación 204 incluye dos conmutadores 240 y 242, de manera que el primer conmutador 240 asegura la reconfiguración estática y dinámica para todos los datos rojos y el segundo conmutador 242 asegura la reconfiguración estática y dinámica de los servicios de administración local. Debido a ello, el primer conmutador 240 está principalmente en interacción con la unidad de tratamiento de servicios externos de corte o de recurso 214 mientras que el segundo conmutador 242 está en interacción con la unidad de tratamiento de servicios externos de inyección local 216.

[0081] El bloque de tratamiento 206 incluye tres bloques de tratamiento 244, 246, 248.

[0082] El primer bloque de tratamiento 244 incluye un subbloque de protección local 250 en interacción con un subbloque de tratamiento de datos sensibles 252.

[0083] El segundo bloque de tratamiento 246 incluye un subbloque de protección local 254 en interacción con un subbloque de tratamiento de datos sensibles 256.

[0084] El tercer bloque de tratamiento 248 incluye un subbloque de protección local 258 en interacción con un subbloque de tratamiento de datos sensibles 260.

[0085] Cada subbloque de tratamiento de datos sensibles 252, 256 y 260 es capaz de efectuar operaciones sobre datos. Por ejemplo, las operaciones son operaciones criptográficas, operaciones de filtrado u operaciones asociadas a servicios. A modo de ilustración, los servicios permiten recuperar mensajes de gestión, suministrar una hora de confianza para los datos calculados o memorizar datos determinados.

[0086] Cada uno de los bloques de tratamiento 244, 246 y 248 tiene un nivel de protección diferente. Por ejemplo, el nivel de protección del primer bloque de tratamiento 244 es el nivel de protección tres, el nivel de protección del segundo bloque de tratamiento 246 es el nivel cuatro y el nivel de protección del tercer bloque es el nivel de protección cinco.

[0087] Cada subbloque de protección local 250, 254 y 258 es capaz de proteger los datos tratados por el bloque de tratamiento 244, 246 y 248 al que está asociado. A modo de ejemplo, los servicios son la memorización de las claves de protección local o el descifrado y la verificación de la autenticidad y la integridad de los datos usados en el

bloque de tratamiento 244, 246 y 248 considerado.

[0088] El segundo nivel de conmutación 208 es capaz de llevar datos desde el conjunto de interfaces de usuario para datos negros 210 hacia el bloque de tratamiento 206 o datos negros obtenidos después del tratamiento del bloque de tratamiento 206 hacia el conjunto de interfaces de usuario para datos rojos 202. Para esto, en el caso concreto de la figura 3, el segundo nivel de conmutación 208 incluye dos conmutadores 260 y 262.

[0089] El conjunto de interfaces de usuario para datos negros 210 permite el acceso a los servicios de corte o de recurso accesibles para los datos negros.

[0090] En el caso particular de la figura 3, el conjunto de interfaces de usuario para datos negros 210 incluye una unidad de tratamiento de datos negros de recurso o de corte 264 y una unidad de tratamiento de servicios comunes externos 266.

[0091] La unidad de tratamiento de servicios externos de corte o de recurso 264 permite el acceso a los servicios de corte por medio de una subunidad de servicio de corte 268 (inserción de datos externos) y una subunidad de servicio de recurso 270 (solicitud de datos hacia un servidor) con las que la unidad de tratamiento de servicios externos de corte o de recurso 264 es capaz de interaccionar. Esta capacidad de interacción se muestra mediante flechas dobles en la figura 3.

[0092] La unidad de tratamiento de servicios comunes externos 266 asegura servicios externos. En el caso presentado, esta unidad de tratamiento de servicios comunes externos 266 está en interacción con una subunidad de memorización 272, una subunidad de generación de número aleatorio 274 y una subunidad de comunicación 276. Así, la unidad de tratamiento de servicios comunes externos 266 es adecuada principalmente para la memorización de datos y para la comunicación entre varios aparatos.

[0093] En funcionamiento, dicha arquitectura 200 permite así tratar a la vez datos negros y datos rojos. Estos tratamientos están optimizados con respecto al nivel de protección que se aportará a los diferentes datos tratados, sabiendo que pese a todo la integridad de los datos es segura.

[0094] Así, la arquitectura 200 asegura una compartimentación de los datos negros (sin codificar) con respecto a los datos rojos (cifrados). La arquitectura 200 permite igualmente separar los datos criptográficos rojos de otros datos rojos y negros. Además, la arquitectura 200 asegura la compartimentación entre datos rojos que requieren un nivel de protección distinto.

REIVINDICACIONES

1. Procedimiento de diseño de una arquitectura (10, 200) de tratamiento de un conjunto de operaciones efectuadas sobre datos, en el que algunos datos requieren un nivel de protección, requiriendo el conjunto de las operaciones efectuadas sobre datos un nivel de protección superior a un nivel de protección umbral que incluye al menos dos subconjuntos de operaciones que pueden realizarse en paralelo, **caracterizado porque** el procedimiento comprende una etapa de:

- determinación de los diferentes subconjuntos de operaciones del conjunto de las operaciones, comprendiendo cada subconjunto operaciones para realizar sobre datos que requieren un nivel de protección superior a un nivel de protección umbral y pudiendo cada subconjunto de operaciones realizarse en paralelo a otros subconjuntos de operaciones,
- determinación, para cada subconjunto de operaciones, del nivel de protección más elevado requerido por los datos en los que se efectúan las operaciones del subconjunto, y
- generación, para cada subconjunto de operaciones, de un bloque de tratamiento (12, 206) en la arquitectura (10, 200) de tratamiento para diseño, comprendiendo el bloque de tratamiento (12, 206) un subbloque de cálculo (21, 244, 246, 248) dedicado únicamente a la ejecución de las operaciones del subconjunto sobre datos para su tratamiento por el bloque de tratamiento (12, 206) cuyo nivel de protección depende del nivel de protección determinado para el subconjunto de operaciones considerado y un subbloque de protección (22, 250 , 254, 258) capaz de garantizar la protección de los datos que serán tratados por el bloque de tratamiento (12, 206), y
- generación de al menos un conmutador (20, 204) capaz de encaminar, hacia cada bloque de tratamiento (12, 206), los datos para tratar,

en el que el procedimiento está **caracterizado por** las etapas de:

- determinación de las operaciones para realizar sobre datos cuyo nivel de protección es inferior al nivel de protección umbral, y
- generación, para cada una de las operaciones determinadas, de una unidad de tratamiento de la operación, siendo las unidades de tratamiento distintas de los bloques de tratamiento (12, 206),
- determinación entre las operaciones efectuadas sobre datos cuyo nivel de protección es inferior al nivel de protección umbral, de las operaciones redundantes, y
- eliminación para las operaciones redundantes determinadas, de una de las dos operaciones redundantes.

2. Procedimiento según la reivindicación 1, en el que cada bloque de tratamiento (12, 206) es capaz de proteger datos cuyo nivel de protección es igual al nivel de protección determinado para el subconjunto de operaciones para el que se genera el bloque de tratamiento (12, 206).

3. Procedimiento según la reivindicación 1, en el que el procedimiento comprende, además, una etapa de determinación de los datos que serán tratados por el bloque de tratamiento (12, 206) provenientes de una unidad de tratamiento (12).

4. Procedimiento según cualquiera de las reivindicaciones 1 a 3, en el que cada subbloque de cálculo (21, 244, 246, 248) es capaz de obtener datos tratados por ejecución de las operaciones del subconjunto sobre los datos que serán tratados por el bloque de tratamiento (12, 206), comprendiendo el procedimiento, además, una etapa de:

- determinación de los datos para encaminamiento hacia una o varias unidades de tratamiento entre los datos tratados por cada subbloque de cálculo (21, 244, 246, 248), y
- generación de al menos un conmutador (20) de datos capaz de encaminar los datos determinados hacia la o las unidades de tratamiento (12).

5. Procedimiento según cualquiera de las reivindicaciones 1 a 4, en el que el procedimiento es implementado mediante ordenador.

6. Producto de programa informático que incluye instrucciones de código de programación aptas para ser implementadas por un procesador, siendo el procesador capaz de implementar el procedimiento según cualquiera de las reivindicaciones 1 a 5.

7. Arquitectura de tratamiento (10, 200) obtenida por la implementación del procedimiento según cualquiera de las reivindicaciones 1 a 5.

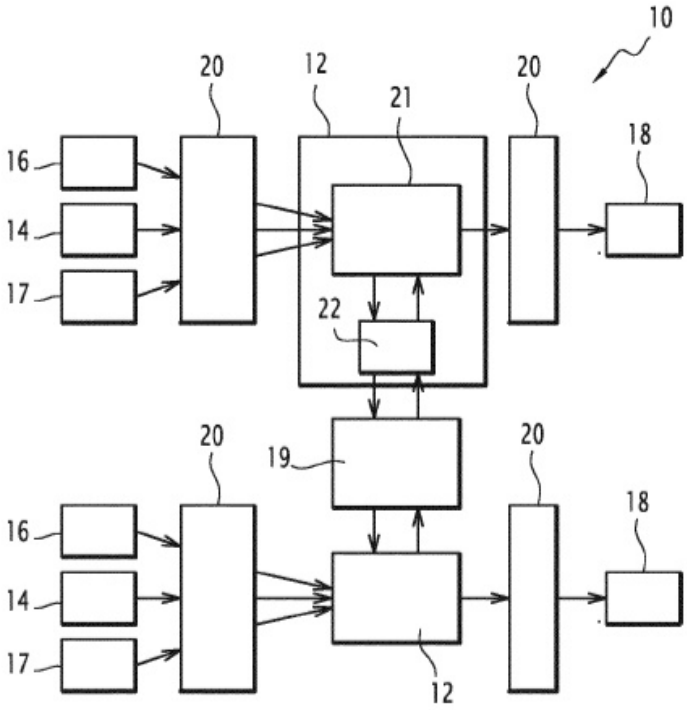
10
20
12
21
20
18
16
14
17
22
20
19
20
18
16
14
17
12

FIG.1

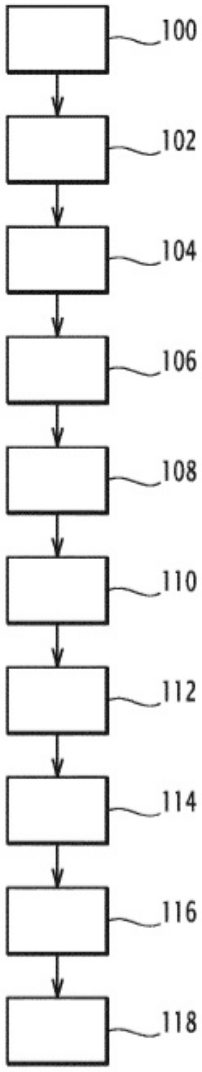
100
102
104
106
108
110
112
114
116
118

FIG.2

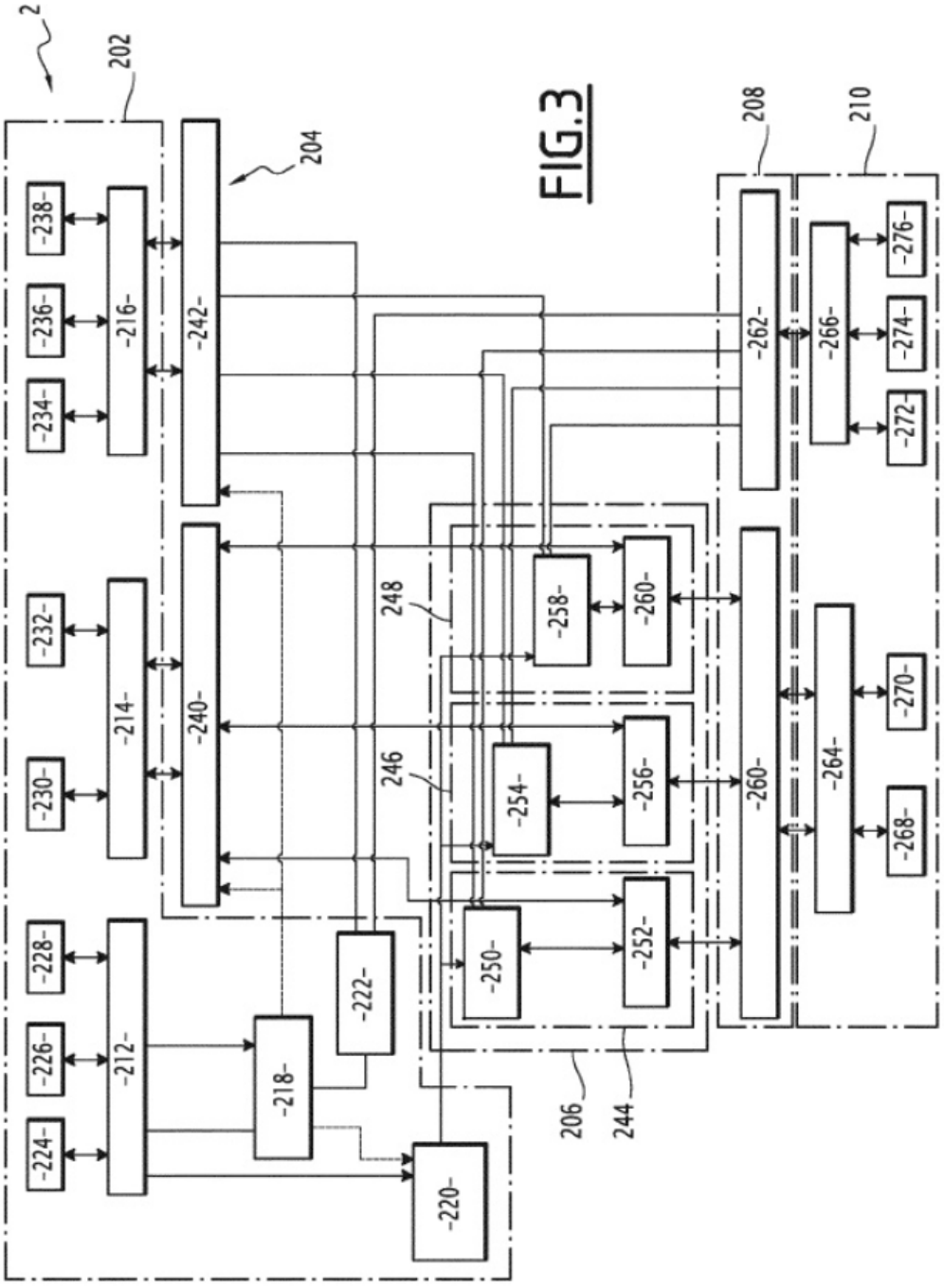
2
202
204
208
210
206
244
248
246
-212-
-214-
-216-
-218-
-220-
-222-
-224-
-226-
-228-
-230-
-232-
-234-
-236-
-238-
-240-
-242-
-250-
-252-
-254-
-256-
-258-
-260-
-262-
-264-
-266-
-268-
-270-
-272-
-274-
-276-

FIG.3