

SUPERINDUSTRIA Y COMERCIO
Radicación : C0047405 C00000001 Folios: 58
Fecha (AMD): 2003-08-25 10:42:32
Trámite : C02 PATENTES D 1 REGISTRO/ 444 REPUESTA
Dependencia: 2020 DIVISION DE NUEVAS CREACIONES

Señores

DIVISION DE NUEVAS CREACIONES

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Santafé de Bogotá, D.C.

RE.: Código 02-01-444

Expediente No. 00 - 47.406

Solicitud de Patente

TELEFONAKTIEBOLAGET LM ERICSSON (publ)

En relación con el Expediente de la referencia y dando cumplimiento a la última providencia recaída sobre este asunto por medio del presente escrito me permito manifestarles lo siguiente:

- 1.- Acompaño una nueva versión de la descripción y las reivindicaciones, debidamente revisada y corregida, junto con un juego de figuras.
- 2.- Adjunto la copia certificada de la solicitud de patente de la cual se reclama prioridad, debidamente traducida.
- 3.- Se anexa el arte final por triplicado.
- 4.- Igualmente se acompañan, debidamente corregidos, el extracto para su publicación y las tarjetas de propietario y archivo temático.

34/27

36

Renuncio al término faltante de traslado, y les solicito ordenar la publicación del extracto.

De Ustedes atentamente,

GERMAN CASTILLO GRAU

T.P. No. 2978 del C.S.J.

35A
37

Dispositivo para procesamiento de datos y el correspondiente método

Campo de la invención

La presente invención se refiere a un dispositivo para el procesamiento de datos y un método para controlar ese dispositivo.

Antecedentes de la invención

El uso de sistemas de procesamiento de datos que comprenden elementos de procesamiento y elementos de memoria se ha difundido en campos muy diversos de la electrónica. En el campo de las comunicaciones, los dispositivos de comunicaciones contienen en su mayoría procesadores que ejecutan programas almacenados en dispositivos de memoria apropiados, para así procesar datos almacenados en los mismos dispositivos de memoria o en alguna otra parte. Un ejemplo típico de un dispositivo de comunicaciones que contiene un procesador (típicamente un microprocesador controlador) y chips de memoria apropiados, es un teléfono móvil.

Uno de los problemas que se encuentran en los sistemas de procesamiento de datos, es el de la seguridad de los datos. Por ejemplo, el teléfono móvil mencionado arriba puede contener diferentes tipos de memorias separadas del procesador central, tales como una memoria *flash* o una EEPROM. Es posible

que una EEPROM sea emulada por una memoria flash, o sea parcialmente una memoria flash. Estas memorias, típicamente, tienen que ser protegidas contra accesos no autorizados, para mantener a salvo la operación normal del teléfono móvil.

Naturalmente, el problema de la seguridad de datos ocurre en cualquier sistema de procesamiento de datos de esa clase, y no sólo en los teléfonos móviles. La solución básica a los problemas de seguridad de datos es la provisión de programa (software) de protección, como por ejemplo un algoritmo para la autenticación de datos sensibles en la EEPROM o EEPROM emulada. No obstante, este tipo de soluciones de programa (software) sufre de una serie de problemas que no pueden ser evitados por el programa (software) mismo, como podría ser la posibilidad de desactivar el algoritmo de autenticación o modificar el algoritmo de autenticación. Algunas veces, también es posible evadir un algoritmo de autenticación usando programa (software) más viejo que no contiene la rutina de autenticación pero aún brinda acceso a los datos sensibles.

Resumen de la invención

El objeto de la presente invención es proveer un dispositivo mejor para el procesamiento de datos, que es bastante simple de implementar y resuelve los problemas señalados arriba.

Este objetivo se alcanza con el dispositivo descrito en la reivindicación 1 y

39 375

el método descrito en la reivindicación 14.

De acuerdo con la presente invención, en un dispositivo de procesamiento de datos que tenga un medio de memoria y un medio de procesamiento, se provee, por un lado, una sección protegida en el medio de memoria del dispositivo de procesamiento de datos y, por otro lado, el medio de procesamiento se dispone para ejecutar necesariamente una rutina de programa almacenada en la parte protegida de la memoria desde el inicio. Debido a esta disposición, pueden ser ejecutados los programas específicos que están, por ejemplo, asociados a la seguridad, pero una persona no autorizada está impedida de efectuar cambios en dichos programas, porque están almacenados en una parte protegida de la memoria. Estos programas de seguridad pueden ser por ejemplo programas que establecen que otros datos no hayan sido manipulados indebidamente, como se explicará en más detalle más adelante.

Un aspecto importante de la presente invención es el hecho de que no es necesaria modificación alguna del procesador. En otras palabras, la solución directa para los problemas mencionados arriba habría consistido en modificar el medio de procesamiento para que contenga mecanismos de seguridad, pero tal modificación de un procesador es típicamente complicada, lleva tiempo y es costosa. En contraste con esto, la presente invención provee una disposición muy simple, en la que solamente es necesaria una memoria modificada, que es con mucho más simple. Especialmente, los procesadores que ya están en uso pueden ser retenidos, en cuyo caso las memorias deben

muestran un dispositivo de memoria preferido a ser usado en el dispositivo de procesamiento de datos de la presente invención;

Fig. 4 muestra un diagrama de flujo de un proceso para el almacenamiento de datos en la parte protegida y seguidamente dichos datos protectores;

Fig. 5 es un diagrama de flujo que explica la operación básica del dispositivo procesador de datos de la presente invención; y

Fig. 6 es un diagrama esquemático de una realización de un medio de memoria.

Descripción detallada de las realizaciones

La Fig. 1 muestra una realización de la presente invención. El numeral de referencia 1 se refiere a un procesador, como podría serlo un controlador microprocesador. El numeral de referencia 11 simboliza las direcciones de inicio en dicho procesador, donde dichas direcciones de inicio son implementadas de tal manera que no pueden ser cambiadas desde afuera. En otras palabras, el procesador 1 se dispone de tal manera que necesariamente llama a las direcciones de inicio almacenadas en sección 11 donde el procesador es iniciado.

El numeral de referencia 2 es un sistema de memoria que comprende una

At 39

primera sección 21, que es una sección protegida, y una segunda sección 22, en la que los datos pueden escribirse libremente. El procesador 1 y la memoria 2 están conectados por las líneas de dirección 3 y las líneas de datos 4, y CLK simboliza que a los circuitos se les suministra una señal de reloj, mientras que U simboliza que a los circuitos se les suministra una tensión de operación.

La protección de la sección protegida consiste en evitar que se escriban datos en ella. Esto se puede lograr de cualquier manera apropiada o deseable para la aplicación en cuestión.

La sección protegida 21 se dispone preferentemente de tal forma que de ninguna manera sea posible escribir datos en dicha sección después haber tenido lugar un almacenamiento inicial en dicha sección. En otras palabras, la memoria debe ser dispuesta de tal manera que se puedan almacenar inicialmente datos específicos o rutinas de programa en la sección protegida 21, y luego deba usarse un mecanismo para asegurar que no sea posible de ahí en más escribir datos en dicha sección protegida. Una de las realizaciones preferidas de una memoria logra esto en la forma que se muestra en la Fig. 4. En este caso, se provee una denominada área de programación única se provee en un dispositivo de memoria *flash*, donde este dispositivo de memoria *flash* incorpora un mecanismo para hacer que una línea de escritura a la sección protegida sea impasable (es decir, destruyendo la línea de escritura quemándola; un así llamado enlace fusible). La destrucción de la línea de escritura es efectuada por la memoria en respuesta a una señal

42 40 X

predeterminada. De esta manera, los programas y datos necesarios pueden ser escritos en la sección protegida (paso S1 en Fig. 4) por el fabricante del aparato en el que el dispositivo de procesamiento de datos de la invención se instalará (por ejemplo el fabricante de teléfonos celulares), después de lo cual se envía la señal predeterminada para así quemar la línea de escritura (enlace fusible). Como consecuencia, no es posible escribir de ahí en más datos en la sección protegida, lo que impide que los datos en dicha sección puedan cambiarse. (Paso S2 en Fig. 4).

Naturalmente, este es sólo un ejemplo preferido, y la presente invención se extiende a todos los tipos de dispositivos de memoria, en los que es posible proteger una parte especificada de la memoria de que a ella acceda escritura. Como un ejemplo, se conocen memorias en las cuales se dispone de cierto número de líneas de entrada, donde una parte predeterminada de la memoria está protegida contra el acceso de escritura en tanto y en cuanto ciertas señales predeterminadas (como podría ser una tensión de masa 0 o una tensión de alimentación) estén presentes en las líneas de entrada.

Otro ejemplo se explicará en relación con Fig. 6, que muestra una memoria con una denominada máquina de estados finitos FS. Las máquinas de estados finitos se conocen en la técnica y, por lo tanto se describirán aquí sólo brevemente. La memoria representada 1A tiene un bus de direcciones 70, un bus de datos 71, línea de acceso de lectura/escritura (R/W) 72, y una línea 73 para conmutar los estados de la máquina de estados finitos (FS). NO simboliza la operación normal, y FSO simboliza la operación de estados

41
42 ~~5~~

finitos. La máquina de estados finitos es básicamente un programa que está cableado en la memoria 1A, de tal manera que no puede ser cambiado desde afuera, cumpliendo de esta manera plenamente los requisitos básicos de seguridad. Este programa cableado es parte de la dirección lógica que procesa las direcciones enviadas a la memoria a través del bus de direcciones.

Como ejemplo, si la línea 73 está alta (es decir, 1), entonces la memoria está en un estado normal de operación y el bus de datos 71 se usa en el modo normal para el transporte de datos. Si la línea 73 está baja (es decir 0), entonces el bus de datos se usa para el control de la máquina de estados finitos FS.

En la aplicación a la presente invención, la máquina de estados finitos tendrá dos estados, a saber: un primer estado en el que se permite escribir datos en una sección predeterminada de la memoria 1A (es decir que esta sección será la sección protegida), y un segundo estado, que es un estado enclavado, en el que la escritura en la sección predeterminada está inhabilitada. La máquina de estados finitos está dispuesta de tal manera que la transición desde el primer estado al segundo estado es irreversible, es decir que una vez que la máquina está enclavada, ya no es posible volver hacia atrás al primer estado, y por lo tanto ya no es posible escribir en la sección protegida. Esto se puede hacer de cualquier forma adecuada con máquinas de estados finitos conocidas, por ejemplo seleccionando el programa de estados finitos de tal forma que el estado enclavado dependa de un valor específico en la sección protegida, de tal manera que en tanto y en cuanto el valor inicial esté en la

44 42 ~~40~~

dirección específica, estará permitido escribir en la sección protegida, mientras que una vez que el valor en la dirección específica haya cambiado (esta es la transición de estado), el programa de estados finitos entrará en un ciclo sin fin o terminará si se hace un intento de escribir una dirección en la sección protegida, y debido a que la dirección específica está en la sección protegida, no puede ser cambiada, y así el estado enclavado es permanente.

Retornando ahora a la Fig. 1, el sistema se dispone de tal manera que las direcciones contenidas en la sección 11 del procesador 1 apunten hacia la sección protegida 21 en la memoria 2. En otras palabras, al iniciarse, el procesador 1 llamará a una o más direcciones en la parte protegida 21 de la memoria 2, y consecuentemente ejecutará los programas contenidos allí. Esto se explica en la parte superior de la Fig. 5, que muestra un diagrama de flujo de la operación de control de acuerdo con la presente invención. En un primer paso S3, la memoria y el procesador CP se inician con el suministro de tensión U y una señal de reloj CLK. Luego, en el paso S4, el procesador CP llama las direcciones de inicio que apuntan a la parte protegida de la memoria. Finalmente, en el paso S5, el procesador CP ejecuta el programa desde la parte protegida.

Puede notarse que no es necesario que se almacenen programas específicos en la parte protegida 21 de la memoria 2, porque en el caso de que el procesador 1 ya haya sido programado, puede ser suficiente que el procesador sólo busque parámetros específicos almacenados en la sección protegida 21, donde estos parámetros son luego procesados por el procesador 1 en las

45 43 +

rutinas preprogramadas.

El correspondiente procesamiento conducido a partir del inicio puede ser seleccionado de acuerdo con los requerimientos y deseos específicos de la aplicación dada. De acuerdo con la realización elegida, las rutinas llevadas a cabo a partir del inicio son rutinas de seguridad, por ejemplo las mostradas en la parte inferior del diagrama de flujo en la Fig. 5. Más específicamente, en el caso de la Fig. 5, la rutina de programa ejecutada a partir del inicio verifica los cambios no autorizados de datos en la sección no protegida 22 de la memoria 2.

Como ejemplo, en el caso de que el dispositivo de procesamiento de datos de la presente invención sea empleado en un teléfono móvil, entonces ciertos parámetros asociados con el usuario específico de dicho teléfono móvil (tales como servicio, prioridades, etc.) pueden ser almacenados en dicha sección no protegida 22, donde es posible que estos parámetros sean cambiados durante el procesamiento de la rutina llevado a cabo por el procesador 1. No obstante, será también posible que un usuario no autorizado acceda a estos datos y los cambie. Una posibilidad de verificar tales accesos no autorizados consiste en almacenar adicionalmente un parámetro que caracterice los datos en dicha sección no protegida 22 junto a los parámetros cambiados. Un ejemplo típico de tal parámetro característico es la suma de verificación (*check sum*). Otro ejemplo es un resultado de una computación de una función criptográfica de comprobación aleatoria (*hash function*). En otras palabras, toda vez que la entidad autorizada (el procesador) cambia datos en la sección 22, entonces

44
46

una correspondiente suma de verificación (*check sum*) cambiada también se almacena. De esta forma, la rutina que verifica si se han efectuado accesos y cambios no autorizados puede consistir en calcular la suma de verificación (*check sum*) y comparar dicha suma de verificación (*check sum*) con el valor almacenado. Si se diere una discrepancia, entonces la rutina determina que ha tenido lugar un cambio de datos no autorizado. Como se muestra en la parte inferior de la Fig. 5, la rutina puede reaccionar a la detección de un cambio no autorizado (SI en paso S6) invocando cualquier tipo de procedimiento de seguridad o emergencia (tal como desconectar el dispositivo) o, si no se detectan cambios, procediendo con la operación normal.

A pesar de que la memoria 2 mostrada en la Fig. 1 aparece como una unidad simple, esto debe ser entendido como una descripción abstracta; dicha memoria puede ser una unidad simple, pero bien puede consistir igualmente en una multiplicidad de dispositivos de memoria separados físicamente, como por ejemplo se muestra en la Fig. 2. La Fig. 2 usa los mismos números de referencia para componentes ya descriptos en relación con la Fig. 1, por lo cual no es necesaria una repetición de la descripción. Como se muestra en la Fig. 2, la memoria 2 comprende una multiplicidad de dispositivos de memoria, como ser chips de memoria individual 201, 202 203 La disposición precisa de los dispositivos de memoria o chips no es de importancia para la presente invención. Por ejemplo, es posible que la sección protegida mostrada como 21 en la Fig. 1 esté formada por el chip completo 201 en la Fig. 2, es decir que este chip 21 esté dispuesto de tal manera que no haya acceso de escritura. Entonces los correspondientes chips 202, 203

47 45 A

pueden ser todos EEPROM convencionales, es decir chips en los que son posibles accesos de escritura normales. Naturalmente, también es igualmente posible, que cada chip 201, 202, 203, tenga una primera sección que esté protegida, y una segunda sección que no esté protegida, donde por ejemplo las direcciones en la sección 11 del procesador 1 apunten a una dirección en la parte protegida del chip 201, y esta parte protegida del chip 201 a su vez apunte a otra parte protegida de los otros chips 202, 203, En el último caso, todas las secciones protegidas de los chips 201, 202, 203, constituirán en su conjunto la parte protegida del medio de memoria descrito en las reivindicaciones.

Se puede notar que, a pesar de que las realizaciones descritas arriba se refieren a un sistema en el que la memoria tiene una parte protegida en la que los datos no pueden ser escritos, aún es posible leer los datos de la sección protegida, incluso para un usuario no autorizado. A fin de hacer esto más difícil para un usuario no autorizado, se muestra una realización preferida de la memoria en el dispositivo de procesamiento de datos de la presente invención en las Figs. 3a y 3b. Las Figs. 3a y 3b muestran un chip de memoria 5 que tiene contactos eléctricos 51 que han de ser soldados o también conectados a terminales eléctricos 61 en una placa de circuito 6. La Fig. 3a muestra los componentes antes del montaje y la Fig. 3b muestra la disposición luego de que el chip de memoria 5 ha sido montado en una placa de circuito 6, donde los contactos eléctricos 51 y los terminales eléctricos 61 han sido unidos a los contactos 71. Se puede notar que la representación de la Fig. 3b está exagerada en el sentido de que en la realidad la distancia entre

48 46 14

el chip de memoria 5 y la placa de circuito 6 serán muy pequeñas, de modo que no hay prácticamente posibilidad de acceder a los contactos 71 mientras el chip 5 esté montado en la placa 6.

Así, como se indica en la Fig. 3, los contactos eléctricos 51 son tales que los contactos resultantes 71 están completamente cubiertos por el chip 5 luego de que dicho chip ha sido montado en la placa de circuito, para así hacer imposible acceder a los contactos eléctricos 51 desde afuera. Por ejemplo, los contacto 51 pueden ser pequeñas semiesferas dispuestas en la denominada matriz rejilla de bolas (ball-grid array).

Al usar la disposición de la Fig. 3, es posible evitar que un usuario no autorizado pueda tomar la señal que pasa a través de los contactos durante la operación del chip de memoria, de tal forma que un monitoreo de las señales entrantes y salientes del chip de memoria 5 durante la operación necesite desmontar el chip de la placa de circuito y luego proveer el correspondiente reemplazo de las conexiones. Este es un procedimiento complicado y tedioso que puede desalentar a cualquier eventual usuario no autorizado para intentar monitorear las señales entre la memoria y el resto de los circuitos. Puede notarse que, aun pensando que es posible leer los datos desde la sección protegida 21 luego de haber desmontado el chip de memoria 5 de la placa de circuito 6, será sin embargo un proceso muy complicado y tedioso remontar el chip en la placa de circuito, porque tales procedimientos de montaje se llevan a cabo con máquinas de alta precisión durante la fabricación, debido a que el espaciado entre contactos es habitualmente muy pequeño.

49-478

Naturalmente, las conexiones entre la memoria y el procesador en la placa de circuito deberían esconderse de una manera apropiada, es decir de tal manera que un intento de acceder a ellos requiera la destrucción de la placa de circuito; y los contactos eléctricos al procesador deberían también ser inaccesibles, por ejemplo con la ayuda de las medidas descriptas arriba en relación con la memoria.

Como ya se mencionó, la presente invención provee una disposición en la que efectivamente puede conseguirse un alto grado de seguridad de los datos de una manera barata. Una aplicación usual del dispositivo de procesamiento de datos de la invención se da en los dispositivos de comunicaciones. Tales dispositivos de comunicaciones pueden ser por ejemplo teléfonos móviles. Una aplicación específicamente elegida del dispositivo de procesamiento de datos es en los dispositivos de comunicaciones que se adhieren a la denominada tecnología Bluetooth. La tecnología Bluetooth está diseñada con el propósito de habilitar a los usuarios para conectar sus computadoras móviles, teléfonos celulares digitales, dispositivos manuales, puntos de acceso a red y otros dispositivos móviles por medio de enlaces inalámbricos de radio de corto alcance sin impedimentos de restricciones de línea visual. Al eliminar la necesidad de cables propietarios o comunicaciones de línea visual por enlaces IR para conectar dispositivos, la tecnología Bluetooth incrementa la facilidad y el alcance de la conectividad inalámbrica. Bluetooth opera en la "banda libre" ISM de 2.45 GHz. Los detalles de esta tecnología pueden encontrarse por ejemplo en <http://www.bluetooth.com>.

50 48 10

La presente invención ha sido descripta por medio de ejemplos, pero se entenderá que estos ejemplos sólo sirven para presentar claramente la invención a personas entendidas y no intentan restringir el alcance de la invención de manera alguna. Más aún, el alcance de la invención está determinado por las reivindicaciones adjuntas.

SA 49

Reivindicaciones

1. Dispositivo para procesamiento de datos, que comprende:

medio de procesamiento (1) para la ejecución de rutinas de programa,
y

medio de memoria (2) para almacenar rutinas de programa a ser
ejecutadas por dicho medio de procesamiento (1), donde

al menos una parte de dicho medio de memoria (2) está dispuesto como
una parte protegida (21) desde la que los datos pueden ser leídos pero
que está protegido contra escritura, y

dicho medio de procesamiento (1) está dispuesto para necesariamente
ejecutar una rutina de programa almacenada en dicha parte protegida
de dicho medio de memoria desde el inicio.

- 2.- Dispositivo según la reivindicación 1, donde dicho medio de
procesamiento (1) almacena direcciones de inicio permanentes (11) que
necesariamente se llaman al inicio de dicho medio de procesamiento (1),
donde al menos una de dichas direcciones de inicio apuntan a dicha parte
protegida (21) de dicho medio de memoria (2).

- 3.- Dispositivo según una de las reivindicaciones 1 o 2, donde dicha parte

52 50A

protegida (21) de dicho medio de memoria (2) es una primera parte, y dicho medio de memoria comprende además una segunda parte (22) en la que pueden ser escritos datos, donde la rutina de programa de dicha parte protegida (21) ejecutada por dicho medio de procesamiento (1) a partir del inicio comprende la verificación de cambios en al menos una parte de los datos contenidos en dicha segunda parte (22).

4.- Dispositivo según la reivindicación 3, donde dicha rutina de programa de dicha parte protegida (21) ejecutada por dicho medio de procesamiento (1) a partir del inicio comprende el cálculo de un parámetro característico para que se verifiquen cambios en los datos, y comparar dichos parámetros característicos con un valor almacenado en dicha segunda parte (22) de dicho medio de memoria (2) en el momento de escribir dichos datos a los que se les está verificando cambios en la dicha segunda parte (22) de dicho medio de memoria (2).

5.- Dispositivo según la reivindicación 4, donde dicho parámetro característico es una suma de verificación (*check sum*).

6.- Dispositivo según una de las reivindicaciones 1 a 5, donde dicho medio de memoria (2) comprende una multiplicidad de dispositivos de memoria (201, 202, 203), uno (201) de los cuales comprende dicha parte protegida, y el resto (202, 203) de los cuales están dispuestos de tal manera que en ellos pueden escribirse datos.

SF 51 A

7.- Dispositivos según una de las reivindicaciones precedentes, donde dicha área protegida (21) está dispuesta de tal manera que un mecanismo está provisto de tal modo que luego de que los datos son inicialmente almacenados en dicha parte protegida (21), cualquier escritura siguiente de datos en dicha parte protegida (21) se bloquea.

8.- Dispositivo según la reivindicación 7, donde dicha área protegida (21) está dispuesta de tal manera que el proceso de almacenar datos en ellos comprende:

escritura (S1) de datos en dicha parte protegida (21) por medio de una línea de escritura, y

envío (S2) de una señal a dicha parte protegida, en respuesta a la cual dicha línea de escritura es permanentemente interrumpida.

9.- Dispositivo según la reivindicación 8, donde dicha línea de escritura es un enlace fusible.

10.- Dispositivo según una de las reivindicaciones 1 a 7, donde dicho medio de memoria (1) comprende una máquina de estados finitos, definiendo dicha máquina de estados finitos un estado que protege dicha parte protegida de que se escriba en ella.

11.- Dispositivo según una de las reivindicaciones precedentes, donde dicho medio de memoria (2) comprende una o más de una EEPROM, un dispositivo de memoria *flash*, y un dispositivo de memoria *flash* que emula una

54

52

EEPROM.

12.- Dispositivo según una de las reivindicaciones precedentes, donde dicho medio de memoria (2) comprende un chip de memoria (5) que tiene contactos eléctricos (51) para ser conectado con una placa de circuito (6) que está dispuesta de tal manera que dichos contactos eléctricos (51) estén cubiertos por dicho chip de memoria (5) cuando dicho chip de memoria (5) esté montado en dicha placa de circuito (6).

13.- Dispositivo según la reivindicación 12, donde dichos contactos eléctricos (51) están provistos en una matriz rejilla de bolas (*ball-grid array*).

14.- Dispositivo de comunicaciones que comprende un dispositivo para el procesamiento de datos según una de las reivindicaciones 1 a 13.

15.- Dispositivo de comunicaciones según la reivindicación 14, donde dicho dispositivo de comunicaciones es un teléfono móvil.

16.- Dispositivo de comunicaciones según la reivindicación 14, donde dicho dispositivo de comunicaciones es un dispositivo de comunicaciones *bluetooth*.

Método para co 17.- Método para controlar un dispositivo de procesamiento de datos que tenga un medio de procesamiento (1) para ejecutar rutinas de programa y medio de memoria (2) para almacenar rutinas de programa a ser ejecutadas

~~S4~~ S3

por dicho medio de procesamiento (1), donde al menos una parte de dicho medio de memoria (2) está dispuesto como una parte protegida (21) desde la cual los datos pueden ser leídos pero que está protegida contra la posibilidad de que se escriba en ella, que comprende:

permitir (S4) a dicho medio de procesamiento (1) ejecutar necesariamente una rutina de programa almacenada en dicha parte protegida de memoria de dicho medio de memoria a partir del inicio (S3).

18.- Método según la reivindicación 17, donde dicho medio de procesamiento almacena direcciones permanentes de inicio que son necesariamente llamadas a partir del inicio de dicho medio de procesamiento, donde al menos una de dichas direcciones de inicio apunten a dicha parte protegida de dicho medio de memoria.

19.- Método según una de las reivindicaciones 17 o 18, donde dicha parte protegida de dicho medio de memoria es una primera parte, y dicho medio de memoria además comprende una segunda parte en la que los datos pueden ser escritos, donde la rutina de programa de dicha parte protegida ejecutada por dicho medio de procesamiento desde el inicio comprende la verificación de cambios en al menos una parte de los datos contenidos en dicha segunda parte.

20.- Método según reivindicación 19, donde dicha rutina de programa de dicha parte protegida ejecutada por dicho medio de procesamiento desde el inicio comprende el cálculo de un parámetro característico de los datos a los

que se les están verificando cambios, y comparar dicho parámetro característico con un valor almacenado en dicha segunda parte de dicho medio de memoria en el momento en que se escriben dichos datos a los que se les están verificando cambios en dicha segunda parte de dicho medio de memoria.

21.- Método según reivindicación 20, donde dicho parámetro característico es una suma de verificación (*check sum*).

Método según 22.- Método de acuerdo con una de las reivindicaciones 17 a 21, donde dicho medio de memoria comprende una multiplicidad de dispositivos de memoria, uno de los cuales comprende dicha parte protegida, y el resto del mismo están dispuestos de tal manera que los datos pueden ser escritos en ellos.

23.- Método según una de las reivindicaciones 17 a 22, donde dicha área protegida está dispuesta de tal manera que se provee un mecanismo tal que luego de que los datos son inicialmente almacenados en dicha parte protegida, cualquier intento subsiguiente de escritura de datos en dicha parte protegida puede ser bloqueado.

24.- Método según la reivindicación 23, donde dicha área protegida se dispone de tal manera que el proceso para almacenar datos comprende:

escribir datos en la parte protegida por medio de una línea de escritura,

y

SA 55 27

enviar una señal a dicha parte protegida en respuesta a lo cual dicha línea de escritura es interrumpida permanentemente.

25.- Método según la reivindicación 24, donde dicha línea de escritura es un enlace fusible.

26.- Método según una de las reivindicaciones 17 a 23, donde dicho medio de memoria (1) comprende una máquina de estados finitos, definiendo dicha máquina de estados finitos un estado que protege dicha parte protegida de que se escriba en ella.

27.- Método según una de las reivindicaciones 17 a 26, donde dicho medio de memoria comprende una o más EEPROM, un dispositivo de memoria *flash*, y un dispositivo de memoria *flash* que emula una EEPROM.

28.- Método según una de las reivindicaciones 17 a 27, donde dicho medio de memoria comprende un chip de memoria que tenga contactos eléctricos para ser conectado con una placa de circuito que está dispuesta de tal manera que dichos contactos eléctricos están cubiertos por dicho chip de memoria cuando dicho chip de memoria está montado en dicha placa de circuito.

29.- Método según la reivindicación 28, donde dichos contactos eléctricos están provistos en una matriz rejilla de bolas (*ball-grid array*).

58 56 24

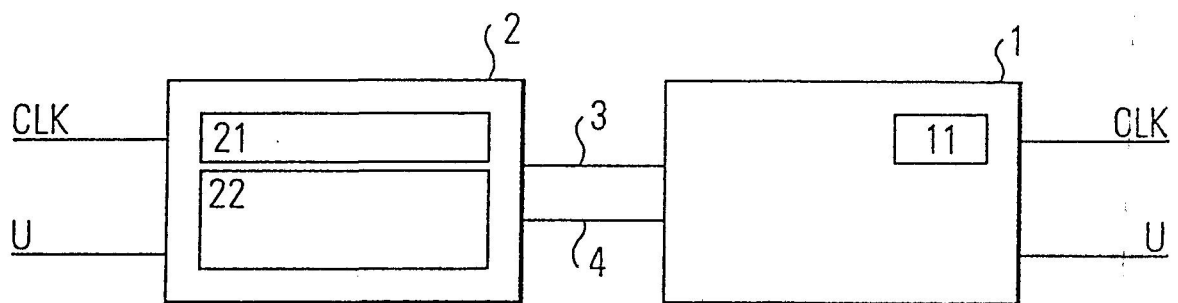
Resumen

Dispositivo para procesamiento de datos, que comprende medios de procesamiento (1) para la ejecución de rutinas de programa, y medios de memoria (2) con el fin de almacenar rutinas de programa que han de ser ejecutadas por dicho medio de procesamiento (1), donde al menos una parte de dicho medio de memoria (2) está dispuesta como una parte protegida (21) desde la cual pueden leerse datos pero que está protegida contra la posibilidad de que se escriba en ella, y dicho medio de procesamiento (1) está dispuesto para ejecutar necesariamente una rutina de programa almacenada en dicha parte protegida de dicho medio de memoria a partir del inicio.

59

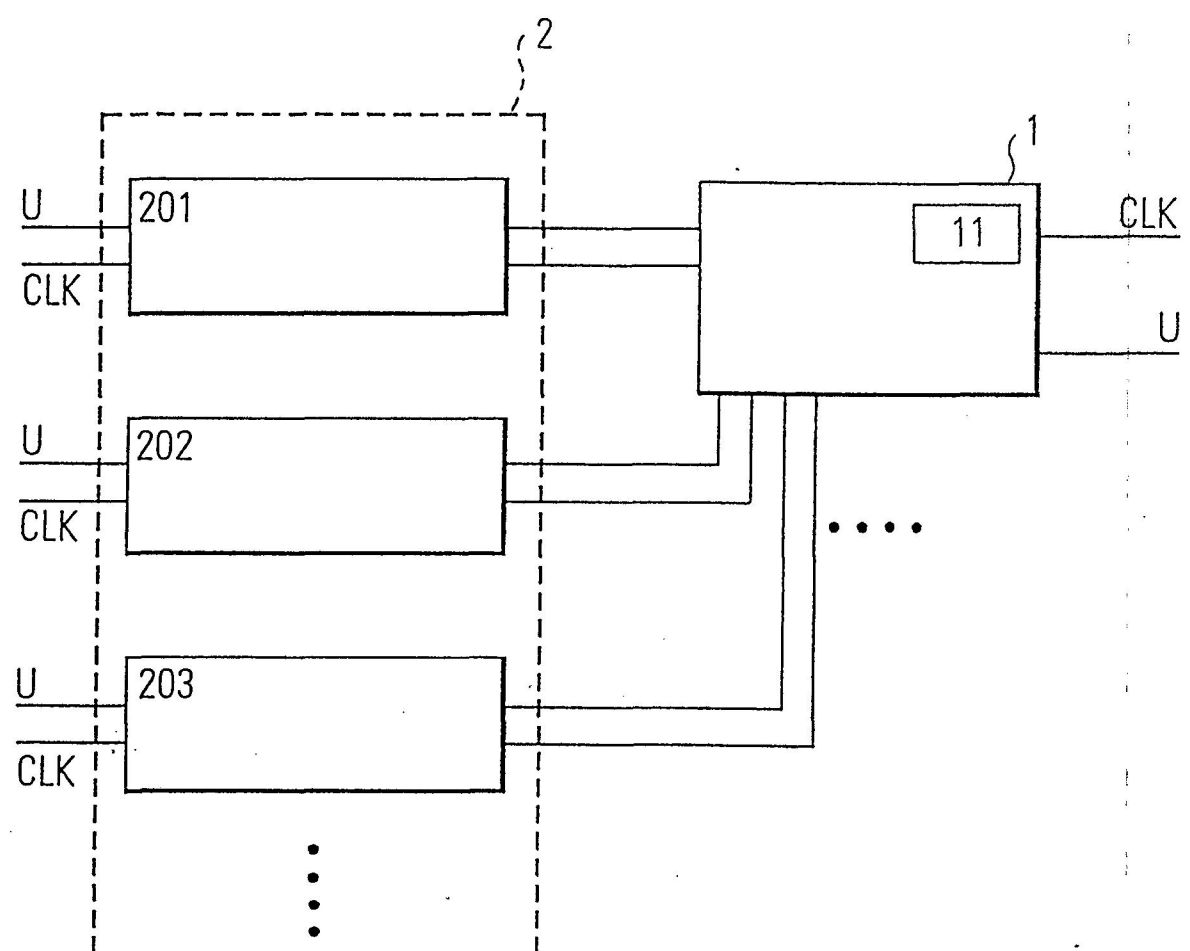
57

FIG.1



6058

FIG.2



6A 5A 2A

FIG.3a

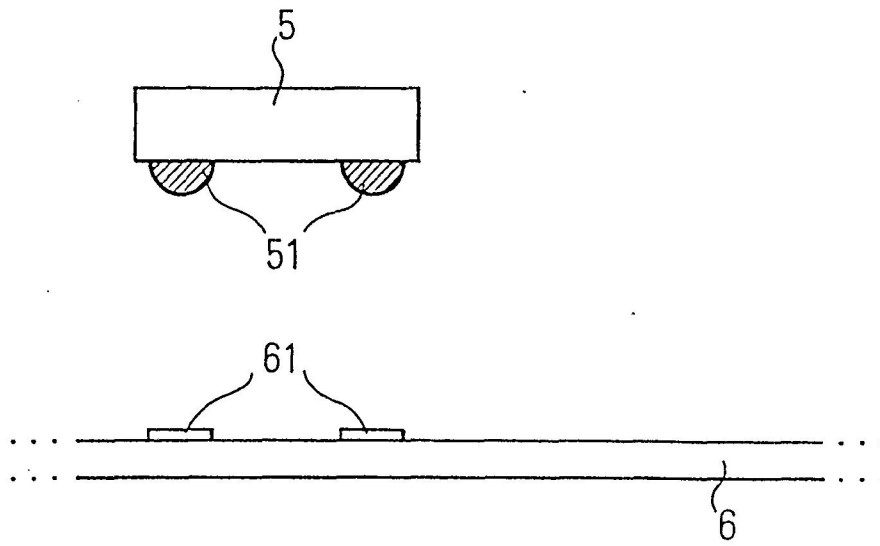
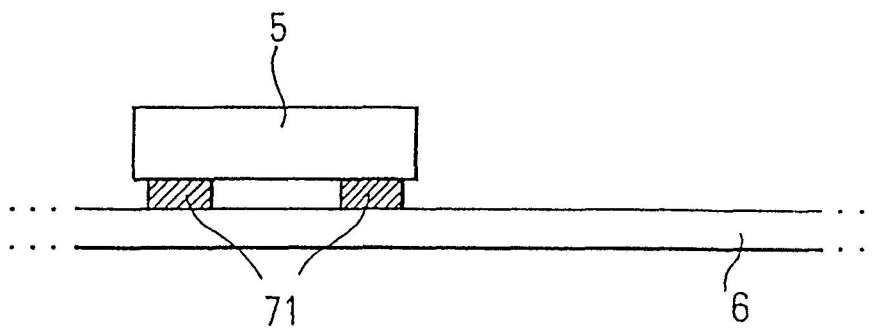
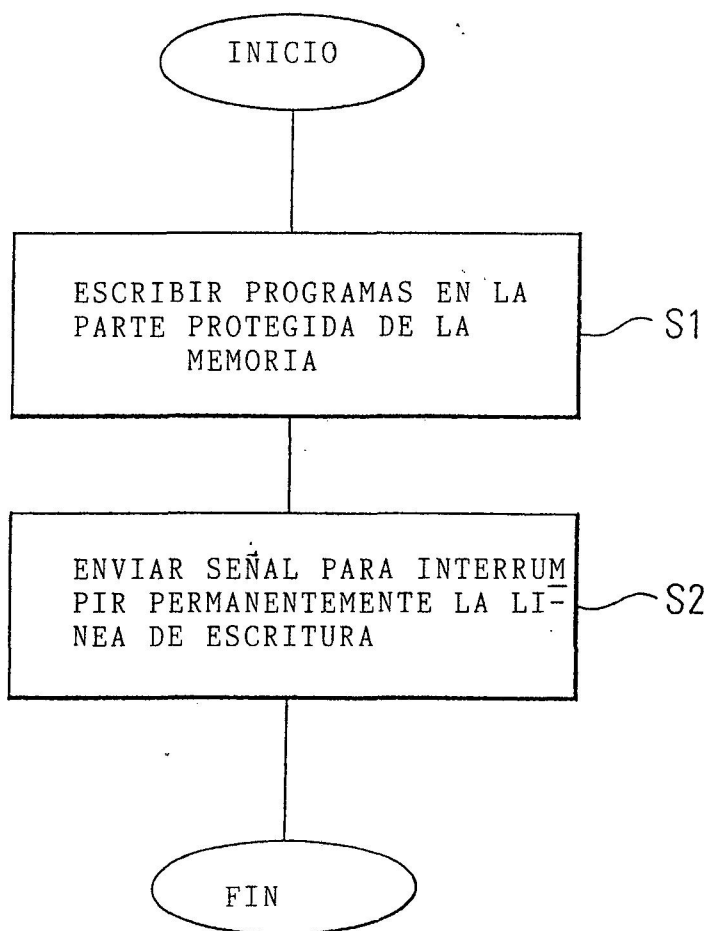


FIG.3b

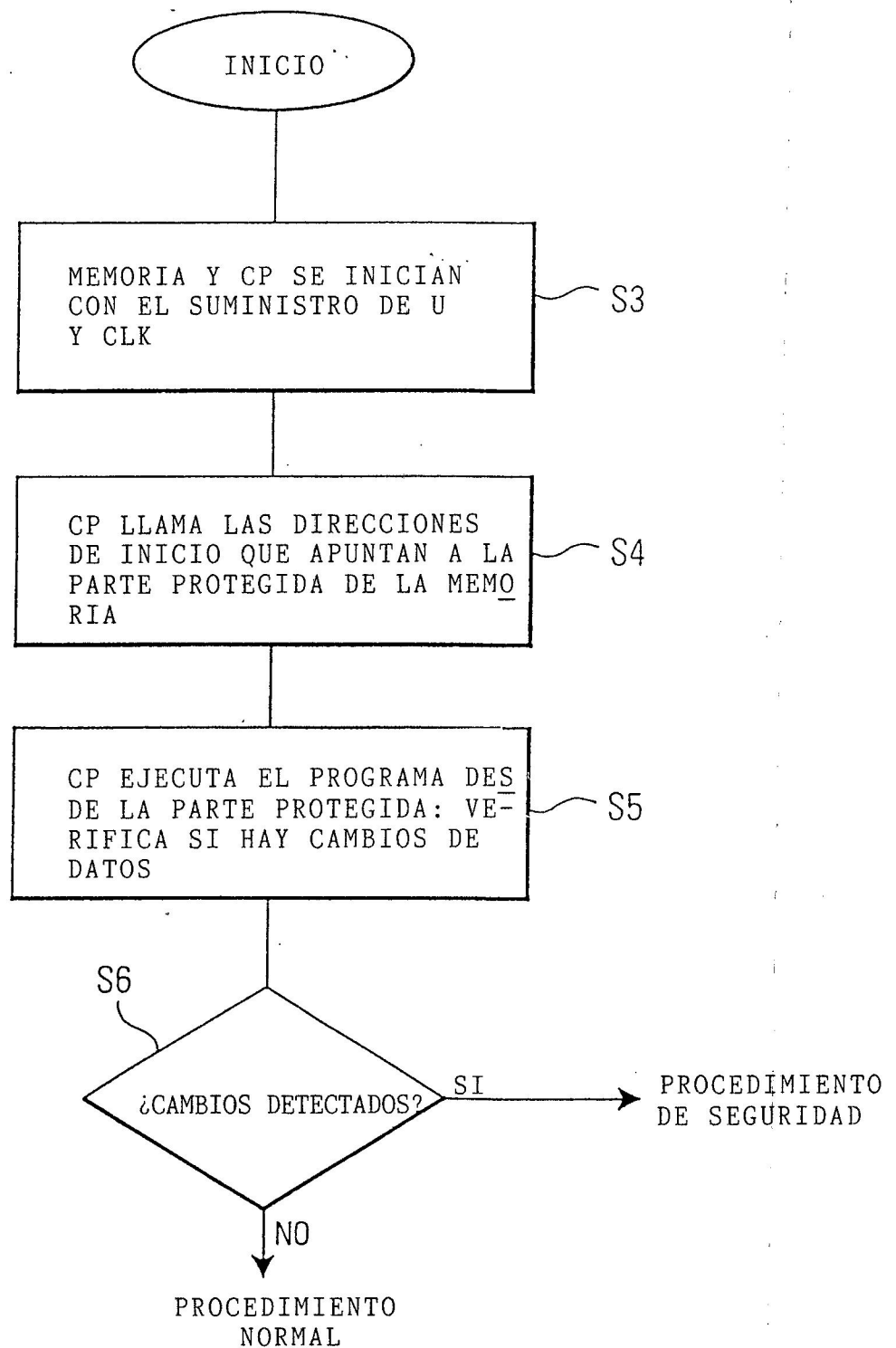


62 60 ~~60~~

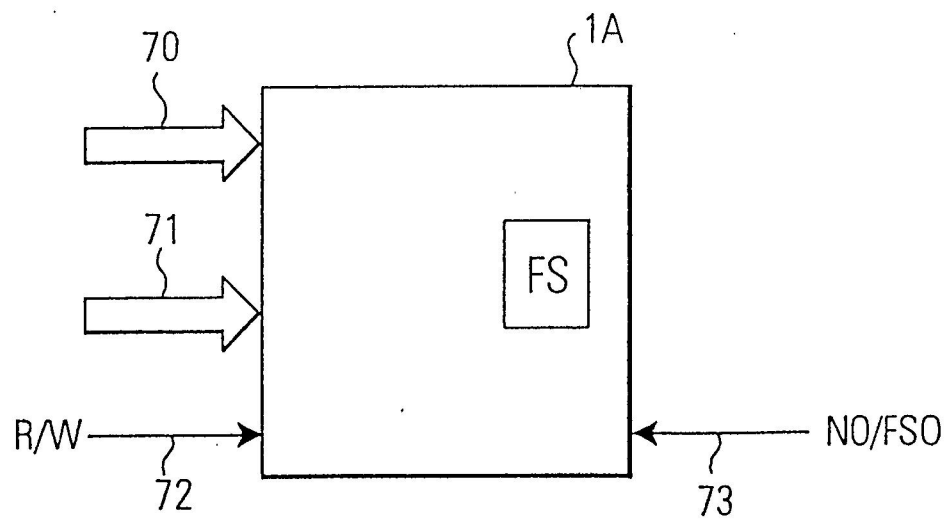
FIG.4



6/2 6/10

FIG.5

62

FIG. 6



Europäisches
Patentamt

European
Patent Office

Office européen
des brevets

63

65

Bescheinigung

Certificate

Attestation

Die angehefteten Unterla-
gen stimmen mit der
ursprünglich eingereichten
Fassung der auf dem näch-
sten Blatt bezeichneten
europäischen Patentanmel-
dung überein.

The attached documents
are exact copies of the
European patent application
described on the following
page, as originally filed.

Les documents fixés à
cette attestation sont
conformes à la version
initialement déposée de
la demande de brevet
européen spécifiée à la
page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

99111962.9

Der Präsident des Europäischen Patentamts:
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

I.L.C. HATTEN-HECKMAN

DEN HAAG, DEN
THE HAGUE, 16/06/00
LA HAYE, LE



Europäisches
Patentamt

European
Patent Office

Office européen
des brevets

64/21
66

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.:
Demande n°: 99111962.9

Anmeldetag:
Date of filing:
Date de dépôt: 25/06/99

Anmelder:
Applicant(s):
Demandeur(s):
TELEFONAKTIEBOLAGET L M ERICSSON (publ)
126 25 Stockholm
SWEDEN

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Device for processing data and corresponding method

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat:	Tag:	Aktenzeichen:
State:	Date:	File no.
Pays:	Date:	Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
G06F9/445, G06F1/00

Am Anmeldetag benannte Vertragsstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE
Etats contractants désignés lors du dépôt:

Bemerkungen:
Remarks:
Remarques:

EPO-Munich
53

25. Juni 1999

78626 q/q8

Device for processing data and corresponding methodField of the invention

The present invention relates to a device for processing data and a method for controlling such a device.

Background of the invention

The use of data processing systems comprising processing elements and memory elements have become widespread in very different fields of electronics. In the field of communication, most communication devices contain processors that execute programs stored in appropriate memory devices, to thereby process data stored in the same memory devices or somewhere else. A typical example of a communication device containing a processor (typically a microprocessor controller) and appropriate memory chips is a mobile telephone.

One of the problems encountered with data processing systems is that of data security. For example, the above-mentioned mobile phone may contain different types of memories separated from the central processor, such as a flash memory or an EEPROM. It is possible that an EEPROM is emulated by a flash memory or is partly a flash memory. Such memories typically have to be protected against unauthorized access, in order to safeguard the normal operation of the mobile telephone.

Naturally, the problem of data security occurs in any such data processing system, not only in mobile phones. The basic solution to problems of data security is the provision of protection software, e.g. an algorithm for the authentication

of sensitive data in the EEPROM or emulated EEPROM. However, such software solutions suffer from a number of problems that cannot be overcome by software itself, such as the possibility of switching off the authentication algorithm or modifying the authentication algorithm. Sometimes, it is also possible to circumvent an authentication algorithm by using older software that did not contain the authentication routine but still provides access to the sensitive data.

Summary of the invention

The object of the present invention is to provide a better device for data processing, which is fairly simple to implement and solves the above problems.

This object is achieved by the device described in claim 1 and the method described in claim 14.

In accordance with the present invention, in a data processing device having a memory means and a processing means, there is provided on the one hand a protected section in the memory means of a data processing device, and on the other hand the processing means in is arranged to necessarily execute a program routine stored in the protected part of the memory upon start-up. Due to this arrangement, specific programs that are e.g. associated with security can be executed, where an unauthorized person is prevented from performing changes in said programs, because they are stored in a protected part of the memory. Such security programs can e.g. be programs that establish that other data has not been tampered with, as shall be explained in more detail further on.

An important aspect of the present invention is the fact that no modification of the processor is necessary. In other words, the straightforward solution to the above-mentioned problems would have consisted in modifying the processing

means to thereby contain security mechanisms, but such a modification of a processor is typically complicated, time consuming and costly. In contrast thereto, the present invention provides a very simple arrangement, in which only a modified memory is necessary, which is far simpler.

Especially, processors already in use may be retained, in which case the memories have to be arranged in such a way that the addresses fixed in said processors for start-up (so-called start addresses) point to the protected section of the memory devices. As an alternative, a slight modification of the processors could be performed, namely changing the start addresses. Although this is a modification of the processor, it is fairly simple and not costly.

Preferred embodiments of the invention are described in the dependent claims.

Brief description of drawings

The various advantages and features of the present invention will become more apparent by studying the following detailed description of embodiments of the invention, where said description makes reference to the figures, in which:

Fig. 1 shows a basic arrangement of an embodiment of the present invention;

Fig. 2 shows an arrangement of another embodiment of the present invention;

Figs. 3a and 3b

show a preferred memory device to be used in the data processing device of the present invention;

Fig. 4 shows a flow-chart of a process for storing data in the protected part and subsequently protecting said data;

Fig. 5 is a flow-chart explaining the basic operation of the data processing device of the present invention; and

Fig. 6 is a schematic diagram of an embodiment of a memory means.

Detailed description of embodiments

Fig. 1 shows an embodiment of the present invention. Reference numeral 1 refers to a processor, such as a microprocessor controller. Reference numeral 11 symbolizes start addresses in said processor, where said start addresses are implemented in such a way that they cannot be changed from the outside. In other words, the processor 1 is arranged in such a way that it necessarily calls the start-addresses stored in section 11 when the processor is started.

Reference numeral 2 is a memory system comprising a first section 21, which is a protected section, and a second section 22, in which data may freely be written. The processor 1 and memory 2 are connected by address lines 3 and data lines 4, and CLK symbolizes that the circuits are supplied with a clock signal, while U symbolizes that the circuits are supplied with an operating voltage.

The protected section is protected against data being written into it. This may be accomplished in any way suitable or desirable for the application at hand.

The protected section 21 is preferably arranged in such a way that it is not at all possible to write data into said section after an initial storing of data in said section has taken place. In other words, the memory must be arranged in such a way that specific data or program routines can be stored in the protected section 21 initially, and then a

mechanism must be used for ensuring that no subsequent writing of data into said section is possible. One preferred embodiment of a memory accomplishes this in a way shown in Fig. 4. In this case, a so-called one-time programming area is provided in a flash memory device, where this flash memory device incorporates a mechanism for making a write line to the protected section impassable (e.g. destroying the write line by burning it through, so-called fusable link). The destruction of the write line is performed by the memory in response to a predetermined signal. In this way, the necessary programs and data can be written into the protected section (step S1 in Fig. 4) by the manufacturer of the apparatus into which the data processing device of the invention is to be built-in (i.e. the manufacturer of mobile telephones), after which the predetermined signal is sent to thereby burn-through the write line (fusable link). As a consequence, no subsequent writing of data into the protected section is possible, such that the data in said section cannot be changed. (Step S2 in Fig. 4).

Naturally, this is only a preferred example, and the present invention extends to any type of memory device, in which it is possible to protect a specified part of the memory from write access. As an example, memories are known, in which a certain number of input lines are given, where a predetermined part of the memory is protected from write access as long as certain predetermined signals (such as a ground voltage 0 or a supply voltage) are present on the input lines.

Another example will be explained in connection with Fig. 6, which shows a memory with a so-called finite state machine FS. Finite state machines are known in the art, and will therefore only briefly be described here. The depicted memory 1A has an address bus 70, a data bus 71, read/write (R/W) access line 72, and a line 73 for switching the states of the finite state machine (FS). NO symbolizes normal operation,

and FSO symbolizes finite state operation. The finite state machine is basically a program that is hard-wired into the memory 1A, such that it cannot be changed from the outside, thereby fulfilling basic security requirements. This hard-wired program is part of the address logic that processes the addresses sent to the memory over the address bus.

As an example, if line 73 is high (i.e. 1), then the memory is in a normal state of operation and the data bus 71 is used in the normal fashion for transporting data. If line 73 is low (i.e. 0), then the data bus is used for controlling the finite state machine FS.

In the application to the present invention, the finite state machine will have two states, namely a first state in which it is allowed to write data into a predetermined section of the memory 1A (i.e. this section will be the protected section), and a second state, which is a locked state, in which writing into the predetermined section is disabled. The finite state machine is arranged such that the transition from the first state to the second state is irreversible, i.e. once the machine is locked, it is no longer possible to switch back to the first state, and therefore it is no longer possible to write into the protected section. This can be done in any suitable way with known finite state machines, for example by selecting the finite state program such that the locked state depends on a specific value in the protected section, such that as long as the initial value is at the specific address a writing into the protected section is allowed, whereas once the value at the specific address has changed (this is the state transition), the finite state program will go into an endless loop or terminate if an attempt is made to write into an address in the protected section, and because the specific address is in the protected section, it may not be changed, so that the locked state is permanent.

Returning now to Fig. 1, the system is arranged in such a way that the addresses contained in section 11 of processor 1 point towards the protected section 21 in memory 2. In other words, upon start-up, the processor 1 will call one or more addresses in the protected part 21 of memory 2, and consequently execute the programs contained therein. This is explained in the top-part of Fig. 5, which shows a flow chart of the control operation in accordance with the present invention. In a first step S3, the memory and processor CP are started by supplying voltage U and a clock signal CLK. Then, in step S4, the processor CP calls the start addresses that point to the protected part of the memory. Finally, in step S5, the processor CP executes the programs from the protected part.

It may be noted that it is not necessary for specific programs to be stored in the protected part 21 of memory 2, because in the event of the processor 1 already being programmed, it may be sufficient that the processor only calls up specific parameters stored in the protected section 21, where these parameters are then processed by the processor 1 in the preprogrammed routines.

The precise processing conducted upon start-up can be selected in accordance with the specific requirements and desires of the given application. In accordance with a preferred embodiment, the routines carried-out upon start-up are security routines, for example shown in the bottom part of the flow-chart in Fig. 5. More specifically, in the case of Fig. 5, the program routine executed upon start-up checks for unauthorized changes of data in the unprotected section 22 of memory 2.

As an example, in the event that the data processing device of the present invention is employed in a mobile telephone, then certain parameters associated with the specific user of said mobile telephone (such as service, priorities, etc.) can

be stored in said unprotected section 22, where it is possible that these parameters are changed during the routine processing performed by processor 1. However, it will also be possible that an unauthorized user will access these data and change them. One possibility of checking for such an unauthorized access consists in additionally storing a characterizing parameter for the data in said unprotected section 22 together with any changed parameters. A typical example of such a characterizing parameter is the check sum. Another example is a result of a computation of a cryptographic hash function. In other words, every time that the authorized entity (the processor) changes data in section 22, then an accordingly changed check sum is also stored. In this way, the routine for checking if unauthorized access and changes have been performed can consist in calculating the check sum and comparing said check sum to the stored value. If a discrepancy occurs, then the routine determines that an unauthorized change of data has taken place. As shown in the bottom part of Fig. 5, the routine can react to the detection of an unauthorized change (yes in step S6) by invoking any sort of desired security or emergency procedure (such as shutting-off the device), or if no changes are detected, proceeding with normal operation.

Although the memory 2 shown in Fig. 1 appears as a single unit, this is to be understood as an abstract description, as said memory may be a single unit, but can equally well consist of a plurality of physically separate memory-devices, as e.g. shown in Fig. 2. Fig. 2 uses the same reference numerals for components already described in connection with Fig. 1, so that a repeated description is not necessary. As shown in Fig. 2, memory 2 comprises a plurality of memory devices, such as individual memory chips 201, 202, 203 The precise arrangement of the memory devices or chips is of no importance to the present invention. For example, it is possible that the protective section shown as 21 in fig. 1 is formed by the entire chip 201 in fig. 2, i.e. this chip 201

is arranged in such a way that there is no write access. Then the remaining chips 202, 203.... could all be conventional EEPROMs, i.e. chips into which normal write access is possible. Naturally, it is equally well possible, that each chip 201, 202, 203,has a first section that is protected, and a second section, that is not protected, where for example the addresses in section 11 of processor 1 point to an address in the protected part of chip 201, and this protected part of chip 201 in turn points to other protected parts of the other chips 202, 203, In the latter case, all of the protected sections of the chips 210, 202, 203,.... would together constitute the protected part of the memory means described in the claims.

It may be noted, that although the above-described embodiments relate to a system in which the memory has a protected part into which data cannot be written, it is still possible to read out the data in the protected section, even for an unauthorized user. In order to make this more difficult for an unauthorized user, a preferred embodiment of the memory in the data processing device of the present invention is shown in Figs. 3a and 3b. Figs. 3a and 3b show a memory chip 5 having electrical contacts 51 that are to be soldered or otherwise connected to electrical leads 61 on a circuit board 6. Fig. 3a shows the components before mounting and Fig. 3b shows the arrangement after the memory chip 5 has been mounted onto circuit board 6, where the electrical contacts 51 and electrical leads 61 have been unified into contacts 71. It may be noted that the representation of Fig. 3b is exaggerated in the sense that in reality the distance between memory chip 5 and circuit board 6 will be very small, such that there is practically no possibility of accessing the contacts 71 while the chip 5 is mounted on the board 6.

Therefore, as indicated in Fig. 3, the electrical contacts 51 are such that the resulting contacts 71 are completely covered by the chip 5 after said chip has been mounted on the

circuit board, to thereby make it impossible to access the electrical contacts 51 from the outside. For example, the contacts 51 can be small semi-spheres arranged in so-called ball-grid array.

By using the arrangement of Fig. 3, it is possible to avoid that an unauthorized user can pick up the signal passing through the contacts during the operation of the memory chip, such that a monitoring of the signals going in and coming out of the memory chip 5 during operation necessitates dismantling the chip from the circuit board and then providing corresponding replacement connections. This is a complicated and tedious procedure that may be expected to let any prospective unauthorized user shy away from attempting to monitor the signals between the memory and the remaining circuits. It may be noted that even though it is possible to read out data from protected section 21 after having dismantled the memory chip 5 from the circuit board 6, it will nonetheless be a very complicated and tedious procedure to re-mount the chip onto the circuit board, because such mounting procedures are performed by high-precision machines during manufacturing, i.e. the spacing between contacts is typically very small.

Naturally, the connections between the memory and the processor on the circuit board should also be hidden in an appropriate fashion, e.g. in such a way that an attempt to access them requires destroying the circuit board, and the electrical contacts to the processor should also be inaccessible, e.g. with the help of the measures described above in connection with the memory.

As already mentioned, the present invention provides an arrangement in which a fairly high amount of data security can be achieved in an inexpensive way. A preferred application of the data processing device of the invention is in communications devices. Such communications devices can

12 70
AP

e.g. be mobile telephones. A specifically preferred application of the data processing device is to communication devices adhering to the so-called Bluetooth technology. Bluetooth technology is designed to enable users to connect their mobile computers, digital cellular phones, handheld devices, network access points and other mobile devices via wireless short-range radio links unimpeded by line-of-sight restrictions. Eliminating the need for proprietary cables or for line-of-sight communication via IR-links to connect devices, Bluetooth technology increases the ease and breadth of wireless connectivity. Bluetooth operates in the 2.45 GHz ISM "free band". Details on this technology may be found e.g. at <http://www.bluetooth.com>.

The present invention has been described by way of examples, but it shall be understood that these examples only serve to clearly present the invention to a skilled person and do not intend to restrict the scope of the invention in any way. Much rather, the scope of the invention is determined by the appended claims.

7271
EPO-Munich
53

25. Juni 1999

12

Claims

1. Device for processing data, comprising:

processing means (1) for executing program routines, and

memory means (2) for storing program routines to be executed by said processing means (1), where

at least a part of said memory means (2) is arranged as a protected part (21) from which data can be read but which is protected against being written into, and

said processing means (1) is arranged to necessarily execute a program routine stored in said protected part of said memory means upon start-up.
2. Device according to claim 1, wherein said processing means (1) stores permanent start addresses (11) that are necessarily called upon start-up of said processing means (1), where at least one of said start addresses points to said protected part (21) of said memory means (2).
3. Device according to one of claims 1 or 2, wherein said protected part (21) of said memory means (2) is a first part, and said memory means further comprises a second part (22) into which data can be written, where the program routine from said protected part (21) executed by said processing means (1) upon start-up comprises checking for changes in at least a part of the data contained in said second part (22).
4. Device according to claim 3, wherein said program routine from said protected part (21) executed by said processing means (1) upon start-up comprises calculating a characteristic parameter for data being checked for

changes, and comparing said characteristic parameter with a value stored in said second part (22) of said memory means (2) at the time of writing said data being checked for changes into said second part (22) of said memory means (2).

5. Device according to claim 4, wherein said characteristic parameter is a check sum.
6. Device according to one of claims 1 to 5, wherein said memory means (2) comprises a plurality of memory devices (201, 202, 203), one (201) of which comprises said protected part, and the rest (202, 203) of which are arranged such that data may be written into them.
7. Device according to one of the preceding claims, wherein said protected area (21) is arranged such that a mechanism is provided such that after data is initially stored in said protected part (21), any subsequent writing of data into said protected part (21) is blocked.
8. Device according to claim 7, wherein said protected area (21) is arranged such that the process for storing data therein comprises:
writing (S1) data into said protected part (21) via a write line, and
sending (S2) a signal to said protected part in response to which said write line is permanently interrupted.
9. Device according to claim 8, wherein said write line is a fusible link.
10. Device according to one of claims 1 to 7, wherein said memory means (1) comprises a finite state machine, said finite state machine defining a state which protects said protected part from being written into.

11. Device according to one of the preceding claims, wherein said memory means (2) comprise one or more of an EEPROM, a flash memory device, and a flash memory device emulating an EEPROM.
12. Device according to one of the preceding claims, wherein said memory means (2) comprises a memory chip (5) having electrical contacts (51) for being connected with a circuit board (6) that are arranged such that said electrical contacts (51) are covered by said memory chip (5) when said memory chip (5) is mounted on said circuit board (6).
13. Device according to claim 12, wherein said electrical contacts (51) are provided in a ball-grid-array.
14. Communication device comprising a device for processing data according to one of claims 1 to 13.
15. Communication device according to claim 14, wherein said communication device is a mobile telephone.
16. Communication device according to claim 14, wherein said communication device is a bluetooth communication device.
17. Method for controlling a data processing device having processing means (1) for executing program routines and memory means (2) for storing program routines to be executed by said processing means (1), where at least a part of said memory means (2) is arranged as a protected part (21) from which data can be read but which is protected against being written into, comprising:
letting (S4) said processing means (1) necessarily execute a program routine stored in said protected part of said memory means upon start-up (S3).

18. Method according to claim 17, wherein said processing means stores permanent start addresses that are necessarily called upon start-up of said processing means, where at least one of said start addresses points to said protected part of said memory means.
19. Method according to one of claims 17 or 18, wherein said protected part of said memory means is a first part, and said memory means further comprises a second part into which data can be written, where the program routine from said protected part executed by said processing means upon start-up comprises checking for changes in at least a part of the data contained in said second part.
20. Method according to claim 19, wherein said program routine from said protected part executed by said processing means upon start-up comprises calculating a characteristic parameter for data being checked for changes, and comparing said characteristic parameter with a value stored in said second part of said memory means at the time of writing said data being checked for changes into said second part of said memory means.
21. Method according to claim 20, wherein said characteristic parameter is a check sum.
22. Method according to one of claims 17 to 21, wherein said memory means comprises a plurality of memory devices, one of which comprises said protected part, and the rest of which are arranged such that data may be written into them.
23. Method according to one of claims 17 to 22, wherein said protected area is arranged such that a mechanism is provided such that after data is initially stored in

said protected part, any subsequent writing of data into said protected part may be blocked.

24. Method according to claim 23, wherein said protected area is arranged such that the process for storing data therein comprises:
writing data into said protected part via a write line,
and
sending a signal to said protected part in response to which said write line is permanently interrupted.
25. Method according to claim 24, wherein said write line is a fusible link.
26. Method according to one of claims 17 to 23, wherein said memory means (1) comprises a finite state machine, said finite state machine defining a state which protects said protected part from being written into.
27. Method according to one of claims 17 to 26, wherein said memory means comprise one or more of an EEPROM, a flash memory device, and a flash memory device emulating an EEPROM.
28. Method according to one of claims 17 to 27, wherein said memory means comprises a memory chip having electrical contacts for being connected with a circuit board that are arranged such that said electrical contacts are covered by said memory chip when said memory chip is mounted on said circuit board.
29. Method according to claim 28, wherein said electrical contacts are provided in a ball-grid-array.

HOFFMANN · EITLE
PATENT- UND RECHTSANWALTE

79626

1/6

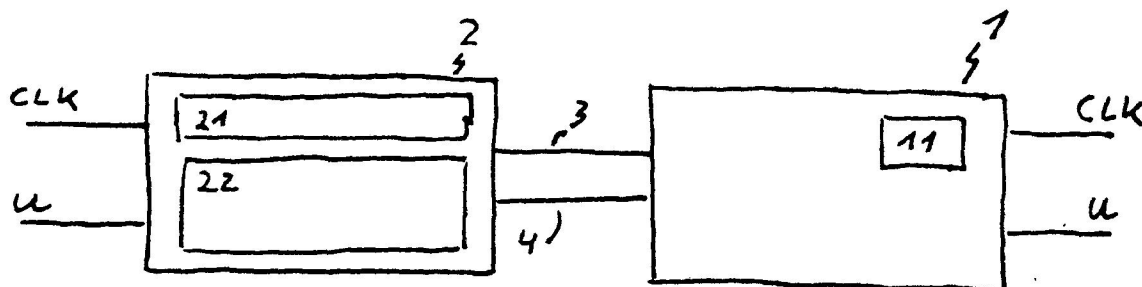


Fig. 1

HOFFMANN · EITLE
PATENT- UND RECHTSANWÄLTE

2/6

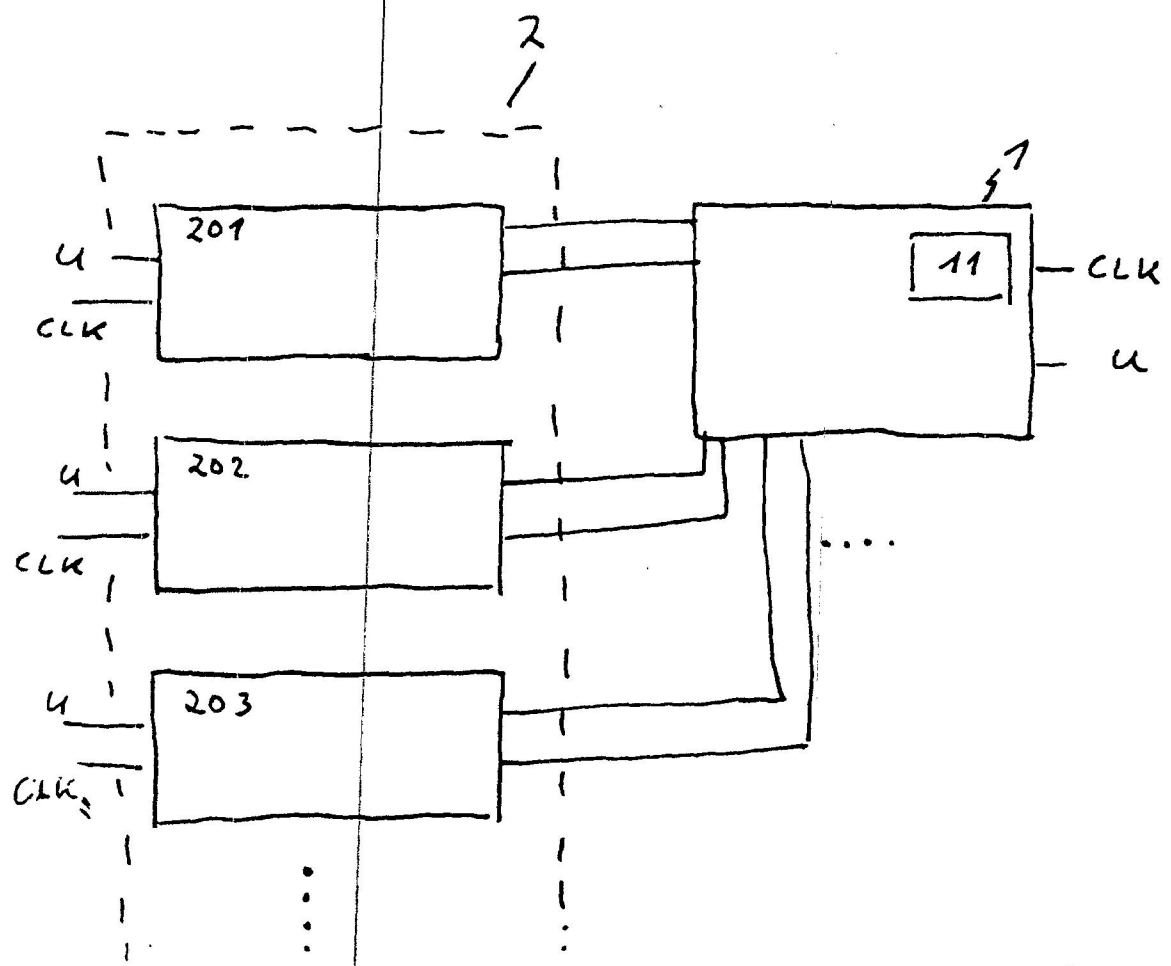


Fig. 2

HOFFMANN · EITLE
PATENT- UND RECHTSANWÄLTE

3/6

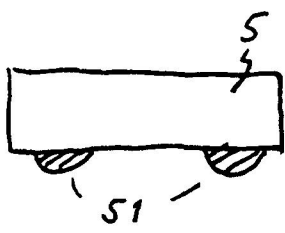


Fig. 3a

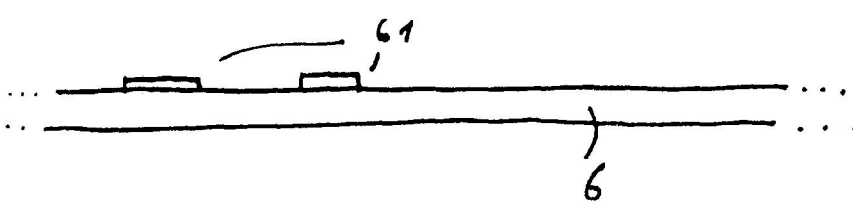
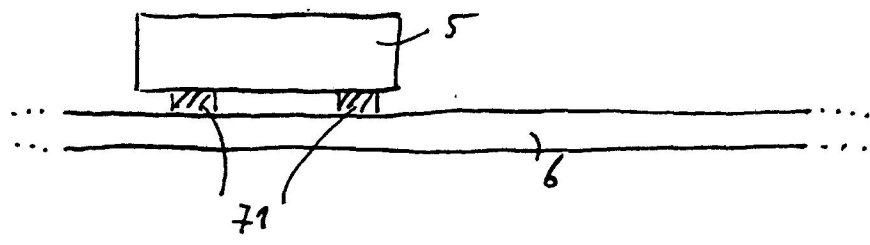


Fig. 3b



HOFFMANN · EITLE
PATENT- UND RECHTSANWÄLTE

4/6

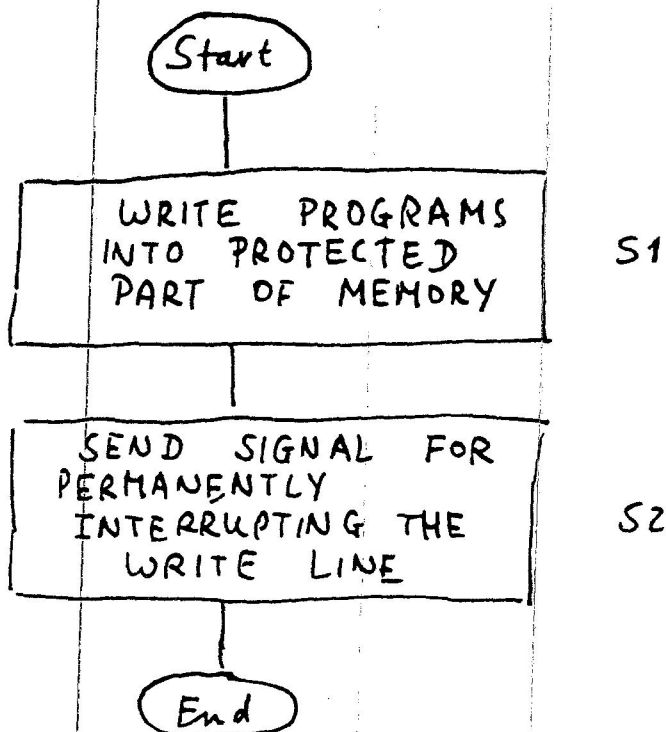


Fig. 4

HOFFMANN · EITLÉ
PATENT- UND RECHTSANWÄLTE

5/6

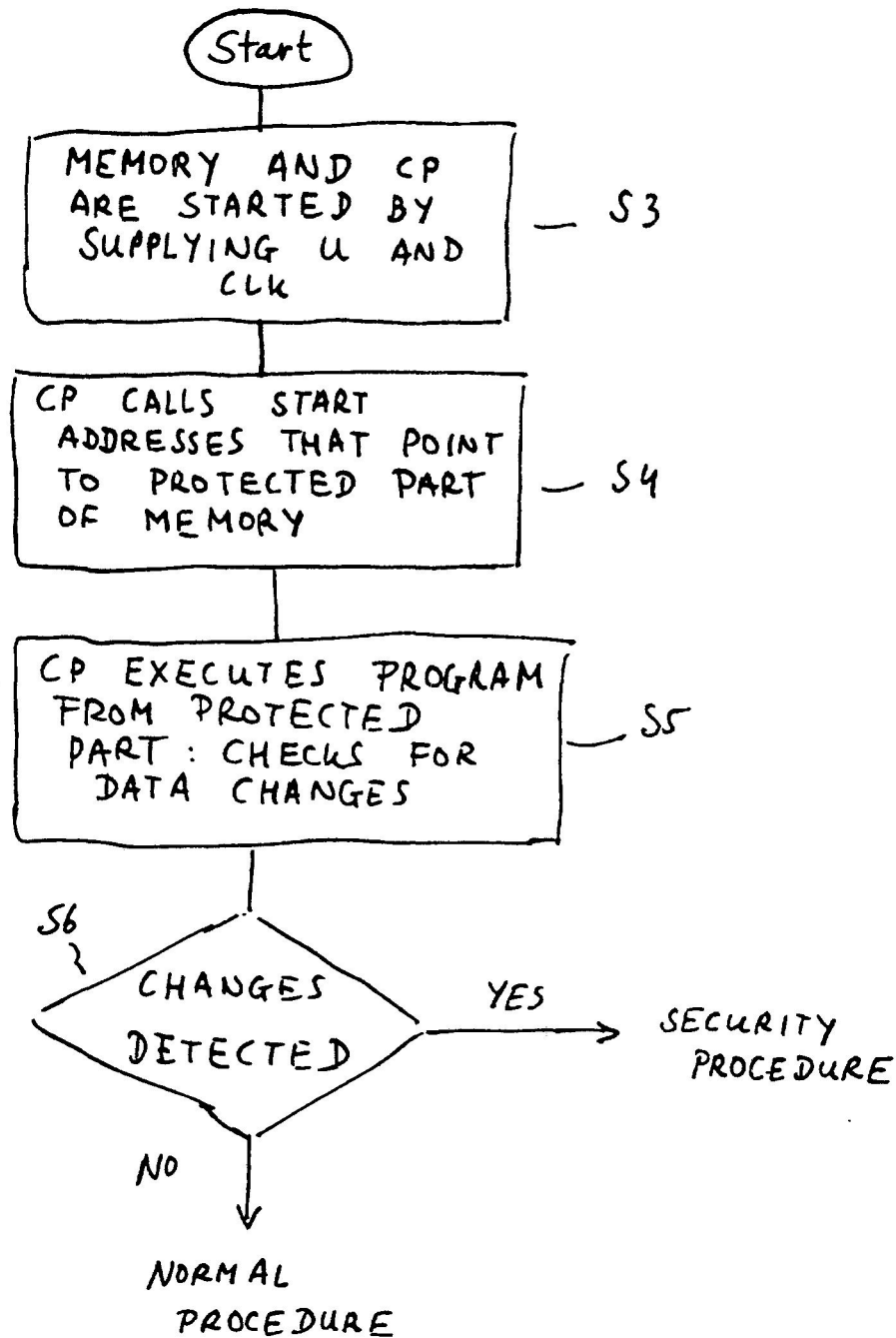


Fig. 5

HOFFMANN · EITLE
PATENT- UND RECHTSANWÄLTE

6/6

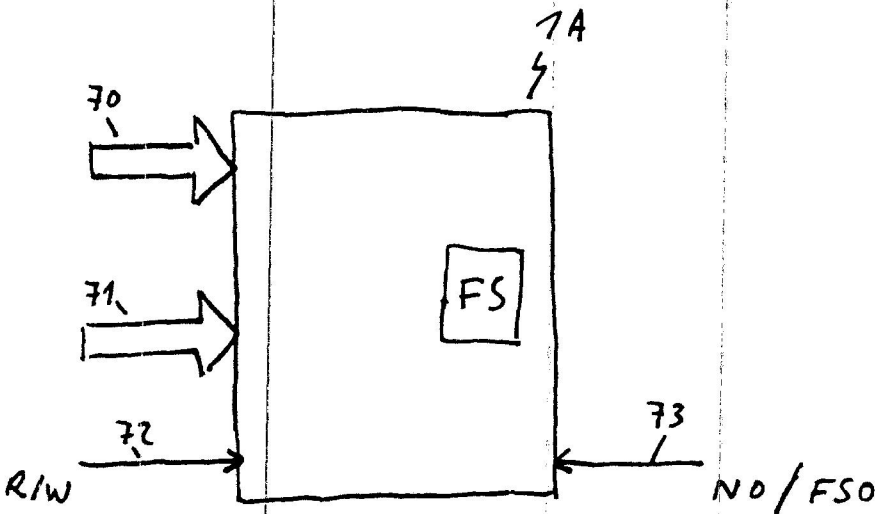


Fig. 6

EPO-Munich
53

25. Juni 1999

17

Abstract

Device for processing data, comprising processing means (1) for executing program routines, and memory means (2) for storing program routines to be executed by said processing means (1), where at least a part of said memory means (2) is arranged as a protected part (21) from which data can be read but which is protected against being written into, and said processing means (1) is arranged to necessarily execute a program routine stored in said protected part of said memory means upon start-up.

Fig. 1

OFICINA DE PATENTES EUROPEA

CERTIFICADO

Los documentos adjuntos son copias exactas de la solicitud de patente europea descrita a continuación, tal como fue radicada en su forma original.

Solicitud de Patente No. 99111962.9

Por el Presidente de la Oficina de Patentes Europea

(FIRMA) I.L.C. HATTEN-HECKMAN

LA HAYA 16/06/00

PAGINA 2 DEL CERTIFICADO

Solicitud No. 99111962.9 Fecha: 25/06/99

Solicitante: **TELEFONAKTIEBOLAGET L M (ERICSSON)**
126 25 Estocolmo
SUECIA

Título de la invención

DISPOSITIVO PARA PROCESAR DATOS Y SU CORRESPONDIENTE METODO

Fecha de radicación: 08/06/00

Clasificación internacional: G06F9/445, G06F1/00

Países contratantes designados en la fecha de radicación:

AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE

81 157-79

**DISPOSITIVO PARA PROCESAR DATOS Y SU MÉTODO
CORRESPONDIENTE**

REIVINDICACIONES:

1. Un dispositivo para procesar datos, que comprende:

medio de procesamiento (1) para ejecutar rutinas de programa, y

medio de memoria (2) para almacenar rutinas de programa para ser ejecutadas por dicho medio de procesamiento (1), donde

al menos una parte de dicho medio de memoria (2) es arreglado como una parte protegida (21) de la cual se pueden leer datos, pero protegida para que no se le pueda escribir, y

dicho medio de procesamiento (1) arreglado para ejecutar necesariamente una rutina de programa almacenada en dicha parte protegida de dicho medio de memoria cuando se de arranque.
2. El dispositivo según la reivindicación 1, en el cual dicho medio de procesamiento (1) almacena direcciones de inicio permanentes (11) que son llamadas necesariamente en el momento de arranque de dicho medio de procesamiento (1), donde al menos una de dicha direcciones de inicio señala dicha parte protegida (21) de dicho medio de memoria (2).
3. El dispositivo según una de las reivindicaciones 1 o 2, en el cual dicha parte protegida (21) de dicho medio de memoria (2) es una primera parte, y dicho medio de memoria comprende además una segunda parte (22) en la que se pueden escribir datos, donde la rutina de programa de dicha parte

82 88

protegida (21) ejecutada por dicho medio de procesamiento (1) en el momento del arranque consiste en revisar cambios en al menos una parte de los datos contenidos en dicha segunda parte (22).

4. El dispositivo según la reivindicación 3, en donde dicha rutina de programa de dicha parte protegida (21) ejecutada por dicho medio de procesamiento (1) en el momento del arranque consiste en calcular un parámetro para los datos donde se estén verificando cambios, y comparar dicho parámetro característico con un valor almacenado en dicha segunda parte (22) de dicho medio de memoria (2) en el momento de escribir dichos datos a los que se les estén comprobando cambios en dicha segunda parte (22) de dicho medio de memoria (2).
5. El dispositivo según la reivindicación 4, en donde dicho parámetro característico es una suma de comprobación.
6. El dispositivo según cualquiera de las reivindicaciones 1 a 5, en el cual dicho medio de memoria (2) comprende una pluralidad de dispositivos de memoria (201, 202, 203), uno (201) de los cuales comprende dicha parte protegida, y el resto (202, 203) de los cuales está dispuesto de manera tal que se pueda escribir datos en ellos.
7. El dispositivo según cualquiera de las reivindicaciones anteriores, en el cual dicha área protegida (21) está dispuesta de forma tal que se provee un mecanismo con el fin de que luego de que los datos sean almacenados inicialmente en dicha parte protegida (21) se bloquee cualquier escritura posterior de datos en dicha parte protegida (21).
8. El dispositivo según la reivindicación 7, en el cual dicha área protegida (21) está dispuesta de tal manera que el proceso para almacenar datos allí consista en:

83

81

escribir (S1) datos en dicha parte protegida (21) vía una línea de escritura,
y

enviar (S2) una señal a dicha parte protegida en respuesta a lo cual dicha
línea de escritura es interrumpida permanentemente.

9. El dispositivo según la reivindicación 8, en el cual dicha línea de escritura es un enlace fusible.
10. El dispositivo según cualquiera de las reivindicaciones 1 a 7, en el cual dicho medio de memoria (1) comprende una máquina de estado finito; dicha máquina de estado finito define un estado que protege dicha parte protegida contra escritura.
11. El dispositivo según cualquiera de las reivindicaciones anteriores, en el cual dicho medio de memoria (2) comprende uno o más de un EEPROM, un dispositivo de memoria instantánea, y un dispositivo de memoria instantánea que emula un EEPROM.
12. El dispositivo según cualquiera de las reivindicaciones anteriores, en el cual dicho medio de memoria (2) comprende un chip de memoria (5) que tiene contactos eléctricos (51) para ser conectados a una tarjeta de circuitos (6) y dispuestos de tal modo que dichos contactos eléctricos (51) sean cubiertos por dicho chip de memoria (5) cuando dicho chip de memoria (5) está montada sobre dicha tarjeta de circuitos.
13. El dispositivo según la reivindicación 12, en el cual dichos contactos eléctricos (51) están provistos en un arreglo esfera-rejilla.
14. El dispositivo de comunicaciones que comprende un dispositivo para procesar datos según cualquiera de las reivindicaciones 1 a 13.

8A 03

15. El dispositivo de comunicaciones según la reivindicación 14, en el cual dicho dispositivo de comunicaciones es un teléfono móvil.
16. El dispositivo de comunicaciones según la reivindicación 14, en el cual dicho dispositivo de comunicaciones es un dispositivo de comunicaciones.
17. Un método para controlar un dispositivo de procesamiento de datos que tiene medio de procesamiento (1) para ejecutar rutinas de programa y medio de memoria (2) para almacenar rutinas de programa para ser ejecutadas por dicho medio de procesamiento (1), donde al menos una parte de dicho medio de memoria (2) está dispuesta como una parte protegida (21) de la cual se pueden leer datos pero protegida contra escritura, que consiste en: dejar (S4) que dicho medio de procesamiento (1) ejecute necesariamente una rutina de programa almacenada en dicha parte protegida de dicho medio de memoria cuando se de arranque (S3).
18. El método según la reivindicación 17, en el cual dicho medio de procesamiento almacena direcciones de inicio permanentes que son necesariamente llamadas cuando arranca a dicho medio de procesamiento, donde al menos una de dichas direcciones de inicio señala a dicha parte protegida de dicho medio de memoria.
19. El método según cualquiera de las reivindicaciones 17 o 18, en el cual dicha parte protegida de dicho medio de memoria es una primer parte, y dicho medio de memoria comprende además una segunda parte donde se pueden escribir datos, donde la rutina de programa de dicha parte protegida ejecutada por dicho medio de procesamiento en el momento de arranque consiste en verificar cambios en al menos una parte de los datos contenidos en dicha segunda parte.

85

83

20. El método según la reivindicación 19, en el cual dicha rutina de programa de dicha parte protegida ejecutada por dicho medio de procesamiento en el momento del arranque consiste en calcular un parámetro característico para los datos a los que se les comprueba cambios, y comparar dicho parámetro característico con un valor almacenado en dicha segunda parte de dicho medio de memoria en el momento de escribir dicho datos a los que se les está comprobando cambios en dicha segunda parte de dicho medio de memoria.
21. El método según la reivindicación 20, en el cual dicho parámetro característico es una suma de verificación.
22. El método según cualquiera de las reivindicaciones 17 a 21, en el cual dicho medio de memoria comprende una pluralidad de dispositivos de memoria, uno de los cuales comprende dicha parte protegida, y el resto de los cuales está dispuesto de tal manera que se les pueda escribir datos.
23. El método según cualquiera de las reivindicaciones 17 a 22, en el cual dicha área protegida está dispuesta de manera tal que se provee un mecanismo luego de que los datos son almacenados inicialmente en dicha parte protegida, se bloquee cualquier escritura posterior de datos en dicha parte protegida.
24. El método según la reivindicación 23, en el cual dicha área protegida (21) está dispuesta de tal manera que el proceso para almacenar datos allí consista en:

escribir datos en dicha parte protegida vía una línea de escritura, y

enviar una señal a dicha parte protegida en respuesta a lo cual dicha línea de escritura es interrumpida permanentemente.

86 2784

25. El método según la reivindicación 24, en el cual dicha línea de escritura es un enlace fusionable.
26. El método según cualquiera de las reivindicaciones 17 a 23, en el cual dicho medio de memoria (1) comprende una máquina de estado finito; dicha máquina de estado finito define un estado que protege dicha parte protegida contra escritura.
27. El método según cualquiera de las reivindicaciones 17 a 26, en el cual dicho medio de memoria comprende uno o más de un EEPROM, un dispositivo de memoria instantánea, y un dispositivo de memoria instantánea que emula un EEPROM.
28. El método según cualquiera de las reivindicaciones 17 a 27, en el cual dicho medio de memoria comprende un chip de memoria que tiene contactos eléctricos para ser conectados a una tarjeta de circuitos y dispuestos de tal modo que dichos contactos eléctricos sean cubiertos por dicho chip de memoria cuando dicho chip de memoria está montado sobre dicha tarjeta de circuitos.
29. El método según la reivindicación 28, en el cual dichos contactos eléctricos están provistos en un arreglo esfera-rejilla.

2do. EXAMEN DE FORMA PATENTE DE INVENCION

Folio

93

Radicación no 00-47406

Concepto Técnico no . 206

Clasificación Internacional de Patentes: C06F13/00

Practicado el examen de acuerdo a lo establecido en el Art. 38 de la Decisión 486 se determinó que esta solicitud de **Patente de Invención**:

- | | | |
|--|--|--|
| SI [☒] | NO [☐] | Contiene un resumen de la invención (Art.26-e). |
| SI [☒] | NO [☐] | Contiene el título de la invención (Art.27-a). |
| SI [☒] | NO [☐] | Contiene la descripción de la invención (Art.26-b). |
| SI [☒] | NO [☐] | NO ES APLICABLE [☐] Contiene los dibujos necesarios para comprender la invención (Art.26-d). |
| SI [☒] | NO [☐] | Contiene una reivindicación (Art.26-c). |
| SI [☐] | NO [☐] | NO ES APLICABLE [☒] Han sido desarrollados los productos y/o procedimientos a partir de recursos genéticos o de sus productos derivados de los que cualquiera de los Países Miembros es país de origen. (Art.26-f-h). |
| SI [☐] | NO [☐] | NO ES APLICABLE [☒] Los productos y/o procedimientos han sido obtenidos o desarrollados por los miembros tradicionales de las comunidades indígenas, afroamericanas o nativas de un país miembro, de acuerdo a lo establecido en la Decisión 391 y sus modificaciones y reglamentaciones vigentes.(Art.26-i). |
| SI [☐] | NO [☒] | La invención se refiere a un producto relativo a un material biológico. (Art.26-j). |
| SI [☒] | NO [☐] | La prioridad se basa en la solicitud anterior. |
| SI [☒] | NO [☐] | CUMPLE LOS REQUISITOS TÉCNICOS |

OBSERVACIONES Y OTROS: (ver anexos)

EXAMINADOR TÉCNICO
202044

Bogotá D. C. Febrero 12 de 2003.

Folio 94

Concepto técnico no. 206

OBSERVACIONES

- ▣ Envía el documento mediante el cual reivindica la prioridad. Folios 65-79
- ▣ Anexa la traducción del documento de prioridad. Folios 80-86.
- ▣ Anexa el documento de poder. Folios 87-90.
- ▣ Anexa un nuevo capítulo reivindicatorio. Folio 51-57.
- ▣ Anexa un capítulo descriptivo de la invención. Folios 40-50.
- ▣ Anexa los dibujos alucivos a la invención. Folios 59-64
- ▣ Anexa el extracto de publicación. Folios 87-90
- ▣ Envía el arte final. Folio 88.
- ▣ Anexa las tarjetas de archivo temático y de propietarios. Folios 91 y 92.

EXAMINADOR TECNICO

202044

Bogotá, Febrero 12 de 2003.

Folio 95

2020
Bogotá DC

Doctor(a)
GERMAN CASTILLO GRAU
Apoderado(a)

REFERENCIA:	Radicación No.	00-47406
	Trámite	002
	Evento	001
	Actuación	416
	Oficio No.	212
	Folios	001

Teniendo en cuenta que la solicitud de privilegio de patente que se tramita bajo el expediente indicado en la referencia, reúne los requisitos de forma establecidos en los artículos 26 y 27 de la Decisión 486 de la Comisión de la Comunidad Andina, y en las demás disposiciones vigentes sobre la materia, se envía el extracto de la solicitud a la Oficina de Comunicaciones para efecto de su publicación en la Gaceta de Propiedad Industrial, conforme lo establece el artículo 40 de la misma Decisión.

Cúmplase

Dado en Bogotá DC, a los

17 8 FEB 2003

ALIX CARMENZA CESPEDES DE VERGEL
Jefe de la División de Nuevas Creaciones

202044

DIVISION DE NUEVAS CREACIONES

RADICACIÓN EXPEDIENTE No. **00-047406**

EL EXTRACTO DE LA PRESENTE SOLICITUD DE **PATENTE DE INVENCION**
FUE PUBLICADO EN LA GACETA DE PROPIEDAD INDUSTRIAL No **529**, DE
FECHA **27 DE JUNIO DE 2003**, EL TERMINO HABIL SEÑALADO POR LA LEY
EXPIRA EL **24 DE SEPTIEMBRE DE 2003**.

NOTA: Dentro del plazo de los seis (6) meses siguientes a partir de la fecha de publicación en la gaceta de Propiedad Industrial, deberá solicitar y cancelar el examen de patentabilidad so pena de que la solicitud caiga en abandono, de acuerdo con lo establecido en el Artículo 44 de la Decisión 486/2000.

SE PRESENTARON OPOSICIONES POR PARTE DE TERCEROS.

SI _____ NO **X**

Bogotá D.C., Diciembre de 2003

89

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RADICACIÓN: 0-47406

EDICTO No. 1292

LA SECRETARÍA GENERAL AD-HOC HACE SABER:

Que esta Superintendencia profirió **Resolución No. 37126 de 30-DIC-2003**. Que el contenido de la parte resolutive es como sigue: E Superintendente de Industria y Comercio.

RESUELVE

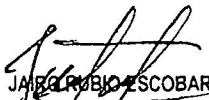
ARTICULO PRIMERO: Declarar abandonada la solicitud de privilegio de patente de invención contenida en el expediente de la referencia.

ARTICULO SEGUNDO: Notificar personalmente el contenido de la presente resolución al doctor Germán Castillo Grau, o a quien haga sus veces, quien actúa como apoderado de Telefonaktiebolaget LM Ericsson (publ), entregándole copia de la misma, advirtiéndole que contra ella procede el recurso de reposición interpuesto ante el Superintendente de Industria y Comercio, al momento de la notificación o dentro de los 5 días hábiles siguientes a ella.

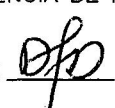
NOTIFÍQUESE Y CUMPLASE

Dada en Bogotá, D.C., a los **30 DIC. 2003**

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO,


JAIME RUBIO ESCOBAR

Para notificar a los interesados, se fija el presente EDICTO en lugar visible al público en la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO, por el término de (10) diez días hábiles contados a partir de las 8:30 a.m. de hoy.

Secretaría General Ad-Hoc **22-ENE-2004**  Este edicto se desfija hoy **04-FEB-2004** a las cinco (5:00 p.m.) 
Secretaría General Ad-Hoc
EDICTO No. 1292