(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 357 472**

(51) Int. Cl.:
H04L 9/00 (2006.01)
H04L 9/32 (2006.01)
A63F 13/10 (2006.01)
A63F 13/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **96921653 .0**
(96) Fecha de presentación : **17.06.1996**
(97) Número de publicación de la solicitud: **0882339**
(97) Fecha de publicación de la solicitud: **09.12.1998**

(54) Título: **Sistema de juego electrónico de casino con mayor capacidad de juego, de autenticación y de seguridad.**

(30) Prioridad: **29.06.1995 US 497662**

(45) Fecha de publicación de la mención BOPI:
26.04.2011

(45) Fecha de la publicación del folleto de la patente:
26.04.2011

(73) Titular/es: **IGT**
9295 Prototype Drive
Reno, Nevada 89511, US

(72) Inventor/es: **Alcorn, Allan, E.;**
Barnett, Michael;
Giacalone, Louis, D., Jr. y
Levinthal, Adam, E.

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

ANTECEDENTES DE LA INVENCIÓN

Campo de la invención

La presente invención se refiere a sistemas de juego basados en microprocesador que se utilizan en los casinos de juego.

Breve Descripción de la Técnica Anterior

Son conocidos los sistemas de juego basados en microprocesador que se utilizan en los casinos de juego para incrementar las tradicionales máquina tragaperras (por ejemplo, juegos individuales de tres carretes o de multilíneas) y juegos de cartas, tales como el póquer y el black jack. En un sistema de juego típico de este tipo, un sistema basado en microprocesador incluye tanto los componentes de hardware como de software para proporcionar las capacidades de juego. Los componentes de hardware incluyen una pantalla de vídeo para visualizar el juego, conmutadores mecánicos para permitir que el jugador seleccione cartas adicionales u opciones de juego, aceptadores y detectores de monedas y los componentes electrónicos que normalmente se encuentran en un sistema basado en microprocesador, tales como memoria de acceso aleatorio (RAM), memoria de sólo lectura (ROM), un procesador y uno o más buses. Los componentes de software incluyen el software de las rutinas de inicialización, de crédito y de pago, la imagen del juego y el conjunto de datos de reglas, y un algoritmo generador de números aleatorios. Con el fin de que sea aceptable para su utilización en un casino, un sistema de juego electrónico debe proporcionar tanto seguridad como autenticación de los componentes de software. Por esta razón, las comisiones de juego hasta el momento han requerido que todos los componentes de software de un sistema de juego electrónico se almacenen en una memoria no modificable, que suele ser una ROM no modificable. Además, una copia de los contenidos de la ROM o un compendio de mensaje de los contenidos (o ambos) se mantienen normalmente en un archivo en un lugar seguro designado por la comisión de juego, de modo que el contenido de una ROM individual retirada de una máquina de juego pueda ser verificado comparándolo con la versión custodiada.

En una disposición típica, un compendio de mensaje del contenido de la ROM se genera inicialmente antes de la instalación de la ROM en la máquina, utilizando un algoritmo conocido normalmente denominado como una función de hash. Una función de hash es un procedimiento de cálculo que produce una cadena de bits de tamaño fijo a partir de una entrada digital de tamaño variable. La cadena de bits de tamaño fijo se denomina valor de hash. Si la función de hash es difícil de invertir – se denomina función de hash unívoca - la función de hash también se denomina función compendio de mensaje, y el resultado se denomina compendio de mensaje. El compendio de mensaje es único para cualquier conjunto de datos de entrada de tamaño variable dado, es decir, el conjunto de datos de juego almacenado en la ROM. Cuando sea necesario autentificar posteriormente la ROM de cualquier máquina dada, la ROM es retirada físicamente de la consola del juego y el compendio de mensaje del contenido de la ROM se calcula directamente desde la ROM usando la función de hash original. El compendio de mensaje calculado se compara con el compendio de mensaje en el archivo en el lugar de custodia designado (por lo general en el mismo casino). Este procedimiento se realiza típicamente si una máquina realiza pagos superiores a un umbral determinado. Si los dos resúmenes de mensaje coinciden, entonces el contenido de la ROM se consideran autenticado (verificado) y se realiza el pago al jugador.

Aunque se ha encontrado que tales sistemas electrónicos de juego de casino son útiles en la promoción de juego de casino, la restricción que requiere que el programa de juego de casino se almacene en una memoria ROM no modificable, conduce a una serie de limitaciones desventajosas. En primer lugar, debido a la capacidad limitada de los medios de almacenamiento ROM que se utilizan tradicionalmente para mantener el programa, el alcance de juego disponible con estos sistemas está muy limitado. En juegos sofisticados que utilizan video de movimiento y elementos multi-media de audio, es necesaria mucha más capacidad de memoria, del orden de cientos de megabytes. Sin embargo, la verificación física de tal gran cantidad de dispositivos físicos no es práctica, y por lo tanto hasta ahora ha sido un impedimento para la creación de juegos sofisticados con más atractivo para los jugadores. En segundo lugar, la verificación de autenticación se realiza únicamente sobre una base limitada (por lo general después de un bote) y otros resultados importantes de ganancias del juego, y el procedimiento de autenticación requieren que el juego sea interrumpido hasta que se compruebe que el contenido de la ROM es auténtico.

El documento norteamericano número 4.727.544 desvela un sistema y un procedimiento para verificar continuamente la integridad de las memorias de un dispositivo de juego controlado por ordenador. El dispositivo de juego incluye una pluralidad de memorias para almacenar software y datos fijos y un procesador para implementar el software para controlar el dispositivo de juego. Una de las memorias almacena un algoritmo de suma de control, de acuerdo con el cual se calculan las sumas de control individuales de cada una de las memorias de la máquina de juego, en el que las sumas de control calculadas se basan en el contenido de las memorias para determinar si ha habido un cambio no autorizado en el contenido de las memorias. Los valores de la suma de control individuales de cada una

de las memorias también se almacenan. El procesador está controlado para implementar periódicamente el algoritmo de suma de control para calcular la suma de control de cada una de los memorias y comparar la suma de control calculada de cada memoria con el valor de la suma de control respectiva almacenada, para determinar si se ha producido un cambio no autorizado. Si se determina que se ha producido un cambio no autorizado en el contenido de las memorias, el procesador bloquea el dispositivo de juego para evitar otra operación del mismo.

En el artículo de Bauspiess F. et al: Requisitos para las funciones de hash criptográficas, Revista Internacional de Ordenadores y Seguridad dedicada al estudio de los aspectos técnicos y financieros de la seguridad informática, Elsevier Science Publishers, Amsterdam, Holanda, vol 11, número 5, 1 de septiembre 1992 (01/09/1992), páginas 427 - 437, XP000296996 ISSN: 0167-4048, proporciona una explicación completa de la estructura y de los requisitos de calidad de las funciones de hash criptográficas.

El documento de Davida G I, Desmedt Y G, Matt B J: "Sistemas de Defensa contra Virus, por medio de Autenticación Criptográfica". 1989 Simposio de la Sociedad de Ordenadores IEEE en Seguridad y Privacidad, Procedimientos. Oakland, California, EE.UU... 1 a 3 de mayo 1989 (01, 03/05/1989). Páginas 312 - 318. XP000041247 desvela la aplicación de la autenticación criptográfica para el control y la defensa de software contra los virus informáticos. Este documento no desvela el uso de funciones de hash o el uso de la autenticación de software en las máquinas de juego.

El Documento GB 2121569 A desvela un procedimiento para autenticar la información de software de un aparato de juego de azar, que comprende las etapas de calcular y de encriptar un primer valor de hash, proporcionar una firma, almacenar la información del software y la firma, calcular un segundo valor de hash, desencriptar la firma almacenada y compara los valores de hash primero y segundo.

El objeto de la presente invención es proporcionar un procedimiento de autenticación de un conjunto de datos o una información de software de un juego visualizable de tipo casino y un sistema de juego electrónico para proporcionar la autenticación de un conjunto de datos de un juego de tipo casino o el software de información que se refiere a un juego de tipo casino, que mejoran en gran medida las capacidades de seguridad y autenticación en los juegos electrónicos de casino, mientras que al mismo tiempo, amplían en gran medida las capacidades de juego de casino.

El objeto anterior se consigue por medio de un procedimiento de autenticación de un conjunto de datos o de un software de información de un juego visualizable de tipo casino, de acuerdo con la reivindicación 1, y un sistema de juegos electrónicos para proporcionar la autenticación de un conjunto de datos de un juego de tipo casino o de información de software relativa a un juego de tipo casino, de acuerdo con la reivindicación 11. Otras características ventajosas se definen en las reivindicaciones dependientes respectivas.

La invención amplía en gran medida la capacidad de juegos del casino y mejora las capacidades de seguridad y autenticación. Más en particular, la invención proporciona un sistema de juegos electrónicos de casino y un procedimiento que tiene una capacidad de almacenamiento masivo ampliado en gran medida para almacenar una multiplicidad de juegos de tipo casino con alta resolución y alta calidad de sonido, y proporciona una autenticación mejorada de la información del programa de juego almacenada con un factor de seguridad elevado.

De acuerdo con un primer aspecto de la invención, la autenticación de un conjunto de datos de un juego de casino se realiza en la consola de juego de casino mediante un programa de autenticación almacenado en una memoria ROM no modificable situada físicamente en la consola de juego de casino. El conjunto de datos de juego de casino y una única firma se almacenan en un dispositivo de almacenamiento masivo, que puede comprender una unidad de sólo lectura o una unidad de lectura / escritura y que se puede encontrarse físicamente, ya sea en la consola de juego de casino, o remotamente localizada y enlazada con la consola de juego de casino por una red adecuada. El programa de autenticación almacenado en la ROM no modificable realiza una verificación de autenticación del conjunto de datos de juego de casino en momentos apropiados, tales como antes del comienzo del juego, a intervalos periódicos o sobre demanda. En las ocasiones adecuadas, el contenido de la ROM no modificable puede ser verificado mediante el cálculo del compendio de mensaje de los contenidos de la ROM no modificable y la comparación de este resumen de mensaje calculado con una copia del compendio de mensaje calculado almacenada de manera segura, a partir del contenido de la ROM antes de la instalación en la consola de juego de casino.

Desde un punto de vista del proceso, este aspecto de la invención comprende un procedimiento de autenticación de un conjunto de datos de un juego de estilo casino que consta de dos fases: una fase de preparación del conjunto de datos de juego y una fase de verificación del conjunto de datos de juego. En la fase de preparación del conjunto de datos de juego, el procedimiento procede a proporcionar un conjunto de datos para un juego de casino, calcular una primera cadena de bits abreviada única para el conjunto de datos de juego de casino, encriptar la primera cadena de bits abreviada para proporcionar una firma encriptada del conjunto de datos de juego de casino y almacenar el conjunto de datos de juego

de casino y la firma en un dispositivo de almacenamiento masivo. La primera cadena de bits abreviada es calculada preferentemente utilizando una función de hash para producir un compendio de mensaje del conjunto de datos de juego de casino. La firma se encripta entonces en el compendio de mensaje. Después del almacenamiento del conjunto de datos de juego y de la firma única, esta información se instala en una consola de juego de casino. La fase de verificación del conjunto de datos de juego de casino continua calculando una segunda cadena de bits abreviada del conjunto de datos de juego de casino utilizando la misma función de hash, desencripta la firma almacenada encriptada para recuperar la primera cadena de bits abreviada, y compara las cadenas de bits abreviadas primera y segunda para determinar si las dos cadenas son iguales. Si se produce una coincidencia, el conjunto de datos de juego de casino se considera auténtico; si no hay ninguna coincidencia, la autenticación es denegada y el juego se prohíbe.

El proceso de encriptado / desencriptado se realiza preferiblemente utilizando una técnica de clave privada / clave pública en la que la primera cadena de bits abreviada es encriptada por el fabricante del juego utilizando una clave privada de encriptado mantenida bajo la custodia del fabricante del juego. El desencriptado de la firma se realiza usando una clave pública que está contenida en un elemento de la memoria no modificable de solo lectura que está situada en la consola del juego, junto con el conjunto de datos de juego de casino. El conjunto de datos de juego de casino se almacena preferiblemente en un dispositivo de almacenamiento masivo, tal como una unidad de disco magnético o CD-ROM o una unidad de archivos de red, teniendo la unidad seleccionada una capacidad relativamente grande. El tamaño real del dispositivo de almacenamiento masivo dependerá de los requisitos de almacenamiento de juego de casino y se puede adaptar a cualquier aplicación específica.

Cada vez que un conjunto de datos de juego de casino es transferido desde el dispositivo de almacenamiento masivo a la memoria principal del sistema, se ejecuta la rutina de autenticación. La rutina de autenticación también puede ser un medio de conmutador de operador montado en la consola del juego o de forma remota a través de una red. Como consecuencia, la autenticidad del conjunto de datos puede ser verificada automáticamente cada vez que se produce la transferencia y en otros momentos oportunos.

Con el fin de detectar los intentos de manipulación del contenido del elemento de memoria no modificable de solo lectura que está situada en la consola del juego, un compendio de mensaje calculado para el programa de autenticación almacenado en la misma se almacena de forma segura en una ubicación diferente que la consola del juego, tal como las instalaciones de seguridad del operador del casino o las instalaciones de una comisión de juego (o en ambas). La autenticidad del elemento de memoria no modificable de sólo lectura se verifica de la misma forma que hasta ahora se realiza en dispositivos de la técnica anterior: a saber, calcular el compendio de mensaje directamente desde el dispositivo memoria no modificable de solo lectura, y comparar el compendio de mensaje calculado con la versión custodiada.

Desde el punto de vista del aparato, el primer aspecto de la invención comprende un sistema de juego electrónico de casino que tiene los medios para proporcionar la autenticación de un conjunto de datos de un tipo de juego de casino antes de permitir el juego, incluyendo el sistema un primer medio para almacenar un conjunto de datos de juego de casino y una firma del conjunto de datos de juego de casino, comprendiendo la firma una versión encriptada de una única primera cadena de bits abreviada calculada a partir del conjunto de datos de juego de casino; un segundo medio para almacenar un programa de autenticación que puede calcular una segunda cadena de bits abreviada del conjunto de datos de juego de casino almacenado en el primer medio de almacenamiento y que puede desencriptar la firma encriptada almacenada en el primer medio de almacenamiento para recuperar la primera cadena de bits abreviada; un medio de proceso para permitir que el programa de autenticación calcule una cadena de bits abreviada del conjunto de datos de juego de casino almacenado en el primer medio de almacenamiento y para permitir que el programa de autenticación desencripte la firma encriptada; y un medio para comparar la segunda cadena de bits abreviada calculada con la cadena de bits abreviada desencriptada para determinar si hay una coincidencia. El primer medio de almacenamiento comprende preferentemente un dispositivo de almacenamiento masivo, tal como una unidad de disco duro, una unidad de CD-ROM o una unidad de almacenamiento en red. El segundo medio de almacenamiento comprende preferentemente una memoria no modificable de sólo lectura en la que se almacena el programa de autenticación.

De acuerdo con un segundo aspecto de la invención, el programa de autenticación almacenado en la ROM no modificable localizada en la consola de juego de casino, se utiliza para probar la autenticidad de todos los otros programas y datos almacenados en dispositivos de memoria fijos en el sistema de juego electrónico de casino, tal como una ROM de arranque del sistema, dispositivos de memoria que contienen el programa del sistema operativo, controladores del sistema y programas ejecutivos / cargadores y otros dispositivos de memoria incorporados en la arquitectura del sistema de juego electrónico de casino. El contenido de cada dispositivo de memoria de este tipo, ya sea información de programa o datos fijos, incluyen las firmas encriptado de compendios de mensaje calculados utilizando una función de hash a partir de la información del programa original o del conjunto de datos fijos. Tras la

inicialización del sistema, el programa de autenticación en la ROM no modificable es utilizado para autenticar el contenido del dispositivo de memoria individual esencialmente de la misma manera que la utilizada para autenticar el conjunto de datos de juego de casino. Más específicamente, el compendio de mensaje para el programa o para el conjunto de datos fijos se calcula utilizando la misma función de hash originalmente utilizada para producir el compendio del mensaje para ese programa o conjunto de datos fijos. La firma encriptada se desencripta utilizando el programa de desencriptado correcto y la clave de desencriptado para recuperar el compendio de mensaje. Las dos versiones del compendio de mensaje se comparan y, si se considera que coinciden, el programa en cuestión o conjunto de datos fijos se considera auténtico y se permite que sean utilizados por el sistema. Una vez que todos los programas en cuestión y los conjuntos de datos fijos han sido autenticados, el procedimiento de autenticación del conjunto de datos de juego de casino se ejecuta, después de lo cual se permite el juego (siempre que se produzca una coincidencia).

Desde un punto de vista del proceso, este segundo aspecto de la invención comprende un procedimiento de autenticación de un programa o conjunto de datos de un juego de estilo casino que consiste en dos fases: una fase de preparación del programa o conjunto de datos fijos, y una fase de verificación del programa o del conjunto de datos fijos. En la fase de preparación del programa o del conjunto de datos fijos, el procedimiento procede a proporcionar un programa o conjunto de datos fijos para un juego de casino, calcular una primera cadena de bits abreviada única para el programa o conjunto de datos fijos, encriptar la primera cadena de bits abreviada para proporcionar una firma encriptada del programa o conjunto de datos fijos, y almacenar el programa o el conjunto de datos fijos y la firma en un dispositivo de memoria. La primera cadena de bits abreviada es calculada preferentemente utilizando una función de hash para producir un compendio de mensaje del programa o conjunto de datos fijos. La firma se encripta entonces en el compendio de mensaje. Después de almacenar el programa o conjunto de datos fijos y la firma única en el dispositivo de memoria, el dispositivo de memoria se instala en una consola de juego de casino. El programa de juego de casino o la fase de verificación del conjunto de datos fijos continua calculando una segunda cadena de bits abreviada desde el programa del casino de juego almacenado o el conjunto de datos fijos almacenado en el dispositivo de memoria, utilizando la misma función de hash, desencriptando la firma encriptada almacenada en el dispositivo de memoria para recuperar la primera cadena de bits abreviada, y comparando las cadenas de bits abreviadas primera y segunda para determinar si ambas cadenas coinciden. Si se produce una coincidencia, el programa de juego de casino o el conjunto de datos fijos se consideran auténticos; si no hay ninguna coincidencia, la autenticación se deniega y el uso de ese programa de juego de casino o conjunto de datos fijos se prohíbe.

La rutina de autenticación se ejecuta cada vez que un programa de casino de juego determinado o conjunto de datos fijos debe ser invocado o usado. La rutina de autenticación también se puede ejecutar de forma automática en una base periódica, o sobre demanda - ya sea a nivel local por medio de un conmutador de operador montado en la consola de juego de casino o de forma remota a través de una red. En consecuencia, la autenticidad del programa de juego de casino o del conjunto de datos fijos puede ser verificada automáticamente cada vez que se requiera el uso de ese programa o conjunto de datos fijos y en otros momentos apropiados, tales como en el curso de una auditoría de la comisión de juego.

Desde un punto de vista del aparato, este segundo aspecto de la invención comprende un sistema de juego electrónico de casino para proporcionar la autenticación de un programa de juego de casino o del conjunto de datos fijos antes de permitir el uso del sistema de ese programa de juego de casino o del conjunto de datos fijos, incluyendo el sistema un primer medio para almacenar un programa de juego de casino o del conjunto de datos fijos y una firma del programa de juego de casino o del conjunto de datos fijos; comprendiendo la firma una versión encriptada de una única primera cadena de bits abreviada calculada a partir del programa de juego de casino o del conjunto de datos fijos; un segundo medio para almacenar un programa de autenticación que puede calcular una segunda cadena de bits abreviada del programa de juego de casino o del conjunto de datos fijos establecido en el primer y un medio de almacenamiento que puede desencriptar la firma encriptada almacenada en el primer medio de almacenamiento para recuperar la primera cadena de bits abreviada; un medio de proceso para permitir que el programa de autenticación calcule una cadena de bits abreviada del programa de juego de casino o del conjunto de datos fijos almacenados en el primer medio de almacenamiento y para permitir que el programa de autenticación desencripte la firma encriptada, y un medio para comparar la segunda cadena de bits abreviada calculada con la cadena de bits abreviada desencriptada para determinar si se presenta una coincidencia. El primer medio de almacenamiento comprende preferentemente un dispositivo de memoria, tal como una memoria de sólo lectura o una memoria de acceso aleatorio. El segundo medio de almacenamiento comprende preferentemente una memoria no modificable de sólo lectura en la que se almacena el programa de autenticación.

Los sistemas de juego electrónicos de casino que incorporan la invención proporcionan una capacidad expandida en gran medida para juego de estilo casino más sofisticados y atractivos, mientras que al mismo tiempo mejoran la autenticación de los juegos sin comprometer la seguridad. Además, los sistemas de juego de casino que incorporan la invención proporcionan una gran flexibilidad para cambiar el juego de casino, ya que los conjuntos de datos de juegos del casino que representan los diferentes

juegos se pueden almacenar en un medio modificable en lugar de unidades de memoria de solo lectura, como ocurre en los actuales sistemas de juego de casino.

Al separar el proceso de autenticación del almacenamiento del conjunto de datos de juego de casino, la invención permite la distribución segura y la ejecución del código de programa y de los datos, con independencia de la distribución particular o de la técnica de almacenamiento empleada. Más específicamente, la invención permite que el conjunto de datos de juego de casino resida en cualquier tipo de medio de almacenamiento secundario, tales como el almacenamiento tradicional en ROM, discos duros y unidades de disco magnético CD-ROM, o los sistemas de archivos en red. Siempre que el procedimiento de autenticación realizado en el conjunto de datos de juego se realice usando el programa de autenticación almacenado en una ROM no modificable, y siempre que la ROM se pueda verificar de forma fiable, el conjunto de datos de juego se puede cargar desde cualquier fuente y puede ser verificado por el sistema en cualquier momento: ya sea antes de su uso, durante el tiempo de ejecución, periódicamente durante el tiempo de ejecución o bajo demanda. Las grandes cantidades de almacenamiento que pueden estar disponibles de forma segura utilizando la invención facilitan la creación de sistemas de juego de casino que ofrecen una mayor diversidad de juego así como juegos individuales de calidad superior. Además, la autenticación de todos los programa de juego de casino y el software de datos fijos asegura la integridad de todo el software del sistema, tanto antes del juego y, posteriormente, en intervalos periódicos o aleatorios.

Para una comprensión más completa de la naturaleza y de las ventajas de la invención, se debe hacer referencia a la descripción detallada que sigue, tomada en conjunto con los dibujos que se acompañan.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1 es un diagrama de bloques de un sistema que incorpora la invención;

la figura 2 es un diagrama esquemático que ilustra el contenido de la memoria de sólo lectura y el dispositivo de almacenamiento masivo;

la figura 3 es una vista esquemática más detallada del programa de autentificación almacenado en la ROM y los datos de juego almacenados en la unidad de almacenamiento masivo;

la figura 4 es un diagrama que ilustra la preparación del conjunto de datos de juego;

la figura 5 es un diagrama que ilustra el procedimiento de autenticación del conjunto de datos de juego, y

la figura 6 es un diagrama que ilustra un enfoque alternativo para la carga segura de software en el sistema.

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES PREFERIDAS

Volviendo a continuación a los dibujos, la figura 1 es un diagrama de bloques de un sistema de juego electrónico de casino que incorpora la invención. Como se ve en esta figura, el sistema consta de varios componentes de sistema bajo control de software. Estos componentes de sistema incluyen un microprocesador 12, que puede comprender cualquier microprocesador de propósito general, tal como un microprocesador Pentium de Intel Corporation. Se proporciona una unidad de memoria principal 13, que típicamente es una memoria de acceso aleatorio que tiene una capacidad de entre 32 y 64 megabytes, para almacenar la mayoría de los programas y elementos gráficos durante el juego. Una memoria ROM 14 de arranque del sistema proporciona el software de inicialización necesario cuando se activa el sistema por primera vez. La ROM 14 contiene programas adicionales en forma de sólo lectura, incluyendo el sistema operativo, los controladores relacionados y el software de autenticación que se describen en detalle a continuación. La memoria RAM no volátil 17 es una RAM estática con respaldo de batería que puede mantener su contenido a lo largo de ciclos de activación. La RAM NV 17 almacena una información significativa sobre el juego, tal como el número de créditos del jugador, el resultado del juego anterior y cierta información de diagnosis y de errores que no es crítica para la comprensión de la invención.

Una unidad de almacenamiento masivo implementado en el sistema de la figura 1 como una unidad de disco duro 18 se acopla a, y está controlada por, un subsistema de disco 19 de diseño y operación convencionales. La unidad de disco 18 proporciona almacenamiento para el conjunto de datos de juego específicos, que incluye tanto los datos del programa como los datos de imagen que especifican las reglas de los diferentes juegos del casino o de variaciones de un único juego de casino, y los tipos de imágenes y las secuencias de imágenes que se deben mostrar a los jugadores del juego. El tamaño de la unidad de disco 18 es una función del número de juego y de las variaciones de juego que se proporciona a un sistema dado, así como de la cantidad de datos necesarios para cada juego específico. En general, cuanto más movimiento tenga el vídeo diseñado para un juego de casino en particular, más almacenamiento será requerido por el software de juego de casino. Una unidad de disco 18 con una

capacidad de 4 gigabytes suele proporcionar suficiente capacidad de almacenamiento. El subsistema de disco 19 comprende un controlador de disco conectada a un bus PCI 20 para controlar la unidad de disco 18. El controlador 19 soporta preferiblemente SCSI-2, con opciones de velocidad y de anchura. Se debe hacer notar que un número de diferentes tipos de unidades de disco basadas localmente puede ser utilizado en el sistema de la figura 1, incluyendo una unidad de almacenamiento de CD-ROM. Además, la unidad de almacenamiento masivo no tiene por qué estar ubicada físicamente en la consola de juego, junto con los demás elementos representados en la figura 1: la unidad de almacenamiento masivo pueden estar situada de forma remota de la consola de juego y acoplada a la misma por medio de una red adecuada, tal como Ethernet, un enlace R5232, o algún otro enlace de red cableado o inalámbrico. Esta última disposición alternativa se indica por medio de la inclusión de un subsistema 21 de red de la configuración y características funcionales apropiadas, que pueden tener Ethernet, R5232 serie, u otra compatibilidad de red.

Un subsistema de vídeo 22 se acopla al bus PCI y proporciona la capacidad de mostrar imágenes fijas a todo color y películas MPEG con una velocidad relativamente alta (por ejemplo, 30 imágenes por segundo) en un monitor apropiado (no mostrado). El mapeo de textura 3D opcional se puede agregar a este sistema, así se desea.

Un subsistema de sonido 23 que tiene una capacidad de reproducción de sonido estéreo de hasta 16 bits de sonido con calidad de CD, se acopla a un bus ISA 24. Una unidad de entrada / salida 25 de propósito general proporciona interfaces a los dispositivos de juego mecánicos (no ilustrados), tales como conmutadores actuables manualmente y luces de pantalla. Un primer circuito puente 27 proporciona una interfaz entre el microprocesador 12, la ROM 14, la memoria principal 13 y el bus PCI 20. El circuito puente 27 preferentemente es un conjunto de chips TRITON disponible en Intel Corporation. Un segundo circuito puente 28 proporciona una interfaz entre el bus PCI 20 y el bus ISA 24. El circuito puente 28 preferiblemente es un tipo de chip 82373 disponible en Intel Corporation.

La figura 2 ilustra los tipos de información, almacenados en el sistema ROM 14 y en la unidad de almacenamiento masivo. Como se observa en la figura 2, la unidad ROM 14 que se utiliza en el sistema de la figura 1 comprende dos elementos separados ROM: la ROM 29 y la ROM 30. La ROM 29 debe ser un dispositivo no modificable, tal como una ROM de máscara programada de 512K x 8 bits de tipo C53400 de Toshiba. La ROM 30 preferiblemente es un dispositivo tal como la ROM 29, pero puede comprender un tipo diferente de ROM, tal como una ROM flash programable en el campo tipo 29FO40, disponible en lntel Corp. La ROM 29 contiene el sistema de inicialización o código de arranque, un programa de autenticación, un programa generador de números aleatorios y una porción inicial del programa ejecutivo / cargador. La ROM 30 contiene el programa del sistema operativo, los controladores del sistema y el resto de de los programas ejecutivos / cargador que se señalan a continuación. La unidad de almacenamiento masivo contiene las aplicaciones, que incluyen los datos de imagen y sonido del juego, las reglas de juego y similares, y la firma asociada a cada juego de casino en particular.

La figura 3 ilustra la autenticación y la información de programa de aplicación con más detalles. Como se ve en esta figura, el programa de autenticación almacenado en la memoria ROM no modificable 29, comprende un componente de algoritmo 32 de compendio de mensaje, un componente de algoritmo 33 de desencriptado, y un componente de clave de desencriptado 34. El componente de algoritmo 32 de compendio de mensaje almacenado en la ROM 29 comprende una copia exacta de una rutina del programa de la función de hash utilizada para calcular inicialmente un compendio de mensaje a partir del conjunto de datos de juego 36 cargable en la forma que se describe más abajo. El componente de algoritmo 33 de desencriptado almacenado en la ROM 29 comprende el algoritmo requerido para desencriptar cualquier firma de conjunto de datos de juego de casino encriptada utilizando el componente de clave de desencriptado 34.

El componente de clave de desencriptado 34 comprende la clave de desencriptado que se necesita para desencriptar cualquiera de las firmas encriptadas 37, de la manera que se describirá más adelante durante la rutina de autenticación

La figura 4 ilustra la manera en la que se genera una firma encriptada 37 del conjunto de datos. Un conjunto 36 de datos de juego de casino cargable es procesado utilizando una función de hash 41 para generar un compendio de mensaje 42 que es único para el conjunto 36 de datos de juego cargables. La función de hash empleada puede ser una de un número de funciones de hash conocidas, tal como las funciones de hash MD2, MD4, y MD5 y la función de hash SHS; o cualquier otra función de hash adecuada que pueda producir una cadena única de bits abreviada a partir de unos datos de entrada de tamaño variable. Para obtener más información acerca de estas funciones de hash, se debe hacer referencia a la publicación titulada "Respuestas a Preguntas Frecuentes sobre la Criptografía Actual", revisión 2.0, 5 de octubre de 1993, publicada por RSA Laboratories, Redwood City, California, y las publicaciones que se indican en la sección de referencias de la misma. Después de la generación, el compendio de mensaje 42 se encripta con un algoritmo de encriptado 43 utilizando una clave privada de encriptado 44 para generar una firma 37 del compendio de mensaje. En la realización preferida, se utiliza la técnica de codificación de dos claves (claves privada / pública), desarrollada por RSA Data Security,

Inc., de Redwood City, California, Esta técnica se divulga y se describe en las patentes norteamericanas números 4.200.770, 4.218.582 y 4.405.829. La firma 37 del compendio de mensaje 42 se almacena en la unidad de almacenamiento masivo, junto con el conjunto 36 de datos cargables.

La figura 5 ilustra la rutina de autenticación realizada de acuerdo con la invención. Cuando se invoca la rutina de autenticación (véase más adelante), el conjunto de datos de juego de casino cargables 36 es transferido desde la unidad de almacenamiento masivo a la memoria principal 13 (a menos que ya esté ahí), y el compendio de mensaje del conjunto de datos de juego de casino 36 se calcula utilizando un algoritmo 32 de compendio de mensaje. El algoritmo 32 de compendio de mensaje utiliza la misma función de hash 41 que ha sido utilizada por el fabricante para preparar el compendio de mensaje original 42. El resultado es una versión sin encriptar 46 del compendio de mensaje calculado a partir del conjunto de datos de juego de casino 36 actualmente presentes en la unidad de almacenamiento masivo. La firma 37 encriptada del conjunto de datos es desencriptada con la clave de desencriptado pública 34 que coincide con la clave privada 44 utilizada para encriptar originalmente el compendio de mensaje 42 del conjunto de datos de juego de casino 36. El compendio de mensaje 47 desencriptado con la clave de desencriptado 34 se compara entonces con el compendio de mensaje 46 calculado a partir del conjunto de datos de juego de casino 36. Si los dos compendios de mensajes coinciden, entonces el conjunto de datos de juego de casino 36 se considera auténtico y el juego puede continuar. Si no hay ninguna coincidencia, se considera que, ya sea el conjunto de datos de juego de casino 36 o la firma 37, están corruptos y no son auténticos. El juego se prohíbe y se pueden tomar las medidas adecuadas: por ejemplo, alertar a un empleado de seguridad utilizando un sistema de mensajería adecuado (una alarma acústica, luces intermitentes, o un mensaje de red desde la consola del juego a un área de seguridad central).

Con el fin de garantizar que la rutina de autenticación no puede ser derivada por la manipulación del programa cargador almacenado en la ROM 30, una parte inicial del programa cargador está incorporado en la ROM 29 no modificable. Esta parte inicial del programa cargador requiere que el programa de autenticación se invoque antes del inicio de cualquier juego de casino. Puesto que esta porción inicial del programa cargador se encuentra en la ROM 29 no modificable, y puesto que no se pueden jugar juegos de casino hasta que el conjunto de datos de aplicación de juego de casino particular 36 se haya cargado en la memoria principal 13, el procedimiento de autenticación no pueden ser derivado por la manipulación del software almacenado en la memoria ROM 30.

Puesto que la autenticación del conjunto de datos fijos 36 y de la firma 37 se confía a los contenidos de la ROM 29, se debe proporcionar un procedimiento para verificar los contenidos de la ROM 29. Con este fin, se calcula un compendio de mensaje para el programa de autenticación almacenado en la ROM 29, y este compendio de mensaje es almacenado de forma segura con el operador de casinos de juego o la comisión (o ambos) junto con la función de hash utilizada para producir el compendio de mensaje. Esta función de hash puede ser la misma función de hash utilizada para calcular el compendio 42 de mensaje del conjunto de datos de juego de casino o una función de hash diferente. De esta manera, la autenticidad de la ROM 29 puede ser fácilmente comprobada en la misma forma que la que se realiza hasta ahora en dispositivos de la técnica anterior: a saber, calcular el compendio de mensaje directamente desde la ROM 29 y comparar el compendio de mensaje calculado con la versión custodiada del compendio de mensaje. Si es requerido por una comisión de juego determinada o es considerado conveniente por un operador de casino, el sistema también puede mostrar el compendio de mensaje 42 de cada conjunto de datos particular 36 o la versión de firma encriptada 37 con fines de auditoría. Además, el sistema puede transmitir esta información a través de subsistemas de redes 21 en el lugar o fuera del lugar en una localización remota (tal como la oficina de la comisión de juego). El compendio de mensaje mostrado o transmitido puede comprender la versión desencriptada o la versión calculada (o ambas).

El procedimiento de autenticación realizado por medio del programa 32 de compendio de mensaje, programa 33 de desencriptado y claves de desencriptado 34 almacenados en la memoria ROM no modificable 29 de la manera que se ha descrito con anterioridad, también se utiliza para autenticar el contenido de todos los dispositivos de memoria en el sistema de la figura 1, tales como los contenidos de la ROM 30 (véase la figura 2), las porciones de datos fijos y los componentes de programa almacenados en la memoria RAM NV 17 y los contenidos de programa y de los datos fijos de cualquier dispositivo de memoria almacenado en el subsistema de red 21, subsistema de vídeo 22, subsistema de sonido 23, interfaz PCI-ISA 24, y unidad de GPIO 25. Cada programa o conjunto de datos fijos almacenados en cualquier dispositivo de memoria en cualquiera de estas unidades tiene una firma asociada, que está encriptada desde un compendio de mensaje del programa original o el conjunto de datos fijos mediante una función de hash, que es preferentemente es la misma función de hash que se utilizó para preparar el compendio de mensaje del conjunto de datos de juego de casino. Antes de autorizar cualquier programa o conjunto de datos fijos de este tipo para participar en la operación del sistema, ese programa o conjunto de datos fijos se somete al procedimiento de autorización para garantizar que el compendio de mensaje calculado a partir de la versión actual del programa o del conjunto de datos fijos coincide con el compendio de mensaje desencriptado desde la firma encriptada asociada al programa o conjunto de datos fijos. Además, el procedimiento de autenticación se puede ejecutar en cada uno de tales programas o conjunto de datos fijos a intervalos periódicos o aleatorios (bajo demanda) de una manera

esencialmente idéntica a la que se ha descrito con anterioridad con respecto al procedimiento de autenticación del conjunto de datos de juego de casino. Como consecuencia, la integridad de todo el software en el sistema se comprueba antes de la utilización del citado software particular con el fin de revelar cualquier cambio no autorizado en la porción de software del sistema de juego de casino.

Un enfoque alternativo para la carga segura de software en el sistema se representa en la figura 6. En esta realización, el sistema básico de entrada y salida (BIOS) de software se almacena en una memoria ROM 50, la primera de dos ROM que componen la ROM de arranque del sistema 14 (Figura 1). El código de arranque, el código del sistema operativo (OS), los controladores del OS y un cargador seguro se almacenan en una ROM 52. Una aplicación de anclaje 54 que incluye gráficos y controladores de sonido, controladores del sistema, el software de manejo de dinero, un segundo cargador seguro, y una firma se almacenan en la memoria masiva 18 (Figura 1).

Cuando se aplica energía inicialmente a la red en el arranque, o cuando el sistema experimenta un re - arranque en caliente, la CPU 12 comenzará la ejecución del código por medio del BIOS 50 de la ROM. El BIOS es el responsable de la inicialización de la placa base y tarjetas periféricas del sistema. Después de que el BIOS haya completado la inicialización, salta al código de arranque en la ROM 252 haciendo que el código de arranque copie el OS, los controladores del OS y el cargador seguro en la memoria RAM.

Una vez en la memoria RAM, el OS se inicia y el cargador seguro almacenado en la memoria ROM 52 se utiliza para cargar la aplicación de anclaje 54 del disco 18. En el disco, la aplicación de anclaje tiene una firma que se utiliza durante la carga para verificar la validez de la aplicación de anclaje.

Después de que se haya iniciado la aplicación de anclaje 54, se podrá utilizar para cargar todas las otras aplicaciones. El cargador seguro de la aplicación de anclaje verificará la validez de una solicitud para debe ser cargada mediante el cálculo de la firma y comparándolo con la almacenada en el disco con la aplicación, como se ha descrito con anterioridad.

Una ventaja importante de la invención que no se encuentra en 20 sistemas de la técnica anterior es la forma en laque el conjunto de datos de juego de casino se puede autenticar. En los sistemas de la técnica anterior, la autenticación del conjunto de datos de juego de casino normalmente sólo se realiza cuando un pago superior a un umbral determinado es requerido por el resultado del juego, y esto requiere que el juego se desactive mientras la ROM es retirada físicamente y se verifican los contenidos de la ROM. En los sistemas que incorpora la invención, la autenticidad de los datos de un determinado conjunto de datos de juego de casino se puede comprobar en una variedad de maneras. Por ejemplo, el conjunto de datos de juego 36 puede ser sometido automáticamente al procedimiento de autenticación que se ilustra en la figura 5 cada vez que el juego se carga desde la unidad de almacenamiento masivo en la memoria principal 13. Por lo tanto, cuando un jugador selecciona un juego de casino para jugar en el sistema, la autenticidad de ese juego que está almacenada realmente en la unidad de almacenamiento masivo, se controla automáticamente mediante el procedimiento de autenticación que se ha descrito con anterioridad sin la retirada de la ROM 29. Además, si se desea, el proceso de autenticación puede ser iniciado como respuesta a la activación de una palanca de un juego de tragaperras, la detección de la inserción de una moneda, el pago de las monedas o la emisión de crédito, o cualquier otro evento detectable relacionado con juego. La autenticidad del conjunto de datos de juego 36 de casino dado también se puede comprobar bajo demanda, ya sea localmente en la consola del juego o de forma remota a través de una red, proporcionando un procedimiento de demanda. Este procedimiento puede ser iniciado, por ejemplo, proporcionando un conmutador manual operable en la consola del juego, accesible sólo a personas autorizadas para iniciar la rutina de autenticación. Por otra parte, el sistema de la figura 1 puede ser configurado para que responda a una orden de demanda generada remotamente (por ejemplo, en un área de seguridad en el casino o fuera del sitio) y se transmite por una red a la consola de juego al subsistema de red 21.

Otra ventaja de la invención radica en el hecho de que la capacidad de almacenamiento del conjunto de datos de juego de un sistema que incorpora la invención no está limitada por el tamaño de una ROM, sino que por el contrario, es dictada por el tamaño de la unidad de almacenamiento masivo. Como consecuencia, los juegos con alta resolución, vídeo con mucho movimiento y sonido estéreo de alta calidad se pueden diseñar y reproducir en sistemas que incorporan la invención. Además, puesto que la unidad de almacenamiento masivo no tiene por qué ser un dispositivo de sólo lectura, y no tiene que estar situado físicamente en la consola de juego, la invención proporciona una gran flexibilidad en el contenido del juego, programación y cambios. Por ejemplo, para cambiar las imágenes gráficas en un juego de casino o un conjunto de juego en particular, se pueden generar nuevos conjuntos de datos de juego de casino, junto con nuevas firmas y se almacenan en la unidad de almacenamiento masivo, ya sea intercambiando las unidades de disco, reemplazando los discos (por unidades de disco de sólo lectura)), o escribiendo nuevos datos en el medio. En la aplicación de almacenamiento masivo en red, se pueden hacer estos cambios a los archivos controlados por el servidor de archivos de red. Puesto que los conjuntos de datos de juego de casino deben pasar la prueba del procedimiento de autenticación, ya sea periódicamente o bajo demanda, los conjuntos de datos corruptos no pueden pasar desapercibidos. De

esta manera, la invención abre el campo de los sistemas electrónicos de juego de casino a juegos fácilmente modificables con pantallas y reglas flexibles, sin sacrificar la seguridad esencial de tales sistemas. De hecho, la seguridad aumenta en gran medida por la capacidad de la invención para autentificar todos los conjuntos de datos de juego, tanto con regularidad (por cada activación de la palanca) y en cualquier momento (bajo demanda), sin interferir con el juego normal (a menos que no se produzca ninguna coincidencia entre las dos formas de compendio de mensaje).

Aunque lo anterior proporciona una explicación plena y completa de las realizaciones preferidas de la invención, varias modificaciones, construcciones alternativas y equivalentes se pueden emplear sin separarse del verdadero espíritu y alcance de la invención. Por ejemplo, aunque se prefiere la técnica de encriptado RSA de clave pública / privada (debido a las ventajas conocidas de esta técnica), se puede emplear una técnica de encriptado de una única clave privada, si así se desea. En un sistema que utiliza esta técnica, la clave única estaría almacenada en la ROM 29 en lugar de la clave pública 34. Además, el compendio de mensaje 42 y la firma 37 para una aplicación dada 36 no tienen que ser calculados por el conjunto completo de datos de juego de casino. Por ejemplo, para algunos juegos de casino, puede ser conveniente proporcionar un conjunto fijo de reglas aunque se permitan cambios futuros en los gráficos de juego de casino, en el sonido o en ambos. Para tales juegos de casino, puede ser suficiente calcular el compendio de mensaje 42 y la firma 37 desde sólo la porción de regla del programa de aplicación 36. En otros casos, puede ser deseable o conveniente mantener constante el video del juego de casino y las porciones de audio, al mismo tiempo que se permiten futuros cambios a las reglas del juego. Para los juegos de casino de esta categoría, el compendio de mensaje 42 y la firma 37 pueden ser calculados a partir de los gráficos y de las porciones de sonido del programa de aplicación 36. También puede ser deseable calcular un compendio de mensaje 42 y la firma 37 a partir de un subconjunto de las reglas, gráficos o porciones de sonido de un programa de aplicación dado 36, o de algún otro subconjunto tomado de un programa de aplicación dado 36. Por lo tanto, lo anterior no se debe interpretar como limitación del alcance de la invención, que se define en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un procedimiento de autenticación de un conjunto de datos o de una información de software de un juego de tipo casino visualizable, comprendiendo el citado procedimiento las etapas de:

(a) proporcionar un conjunto de datos (36) o un software de información de un juego de casino;

(b) calcular un primer valor de hash único para el conjunto de datos (36) o la información de software utilizando una función de hash;

(c) encriptar la cadena del primer valor de hash para proporcionar una firma (37);

(d) almacenar el conjunto de datos (36) o la información del software y la firma (37);

(e) proporcionar una memoria no modificable (29) que almacena un programa de autenticación y una porción inicial de un programa cargador, en el que la porción inicial del programa cargador requiere que el programa de autenticación se invoque antes de la iniciación de cualquier juego de casino;

(f) proporcionar una memoria modificable (30) que almacena la porción restante del programa cargador;

(g) calcular un segundo valor de hash, usando el programa de autenticación, a partir del conjunto de datos almacenados (36) o la información de software utilizando la citada función de hash;

(h) desencriptar la firma almacenada (37) para recuperar el primer valor de hash, y

(i) comparar los valores de hash primero y segundo para determinar si los valores de hash primero y segundo coinciden.

2. El procedimiento de la reivindicación 1, **que se caracteriza porque** los valores de hash primero y segundo, respectivamente, constituyen el compendio de mensaje (46) del conjunto de datos (36) o la información de software.

3. El procedimiento de la reivindicación 1 ó 2, **que se caracteriza porque** la citada etapa de encriptación (c) se realiza mediante una clave privada de encriptado (44).

4. El procedimiento de la reivindicación 3, **que se caracteriza porque** la citada etapa (g) de descodificación se realiza mediante una clave pública de desencriptado (34).

5. El procedimiento de cualquiera de las reivindicaciones anteriores, **que se caracteriza porque** las citadas etapas (a) - (d) se realizan en un primer lugar y las citadas etapas (e) - (h) se realizan en un segundo lugar.

6. El procedimiento de la reivindicación 5, **que se caracteriza porque** el primer lugar comprende una instalación de fabricación, y el citado segundo lugar es una instalación de juegos de azar.

7. El procedimiento de cualquiera de las reivindicaciones anteriores, **que se caracteriza porque** la citada etapa de almacenamiento (d) incluye la etapa de almacenar el conjunto de datos (36) o la información de software y la firma (37) en un dispositivo de almacenamiento masivo (18) o en un dispositivo de memoria.

8. El procedimiento de la reivindicación 7, **que se caracteriza porque** el dispositivo de almacenamiento masivo (18) comprende una unidad de disco duro.

9. El procedimiento de la reivindicación 7, **que se caracteriza porque** el dispositivo de almacenamiento masivo (18) comprende una unidad de CD-ROM.

10. El procedimiento de la reivindicación 7, **que se caracteriza porque** el dispositivo de almacenamiento masivo (18) comprende un sistema de almacenamiento en red.

11. Un sistema de juego electrónico para proporcionar la autenticación de un conjunto de datos (36) de un juego de tipo casino o software de información relativa a un juego de tipo casino, comprendiendo el citado sistema:

un primero medio (18, 19,21), para almacenar un conjunto de datos de juego de casino (36) o la información de software y una firma (37) del citado conjunto de datos de juego de casino o información de software, comprendiendo la citada firma (37) una versión encriptada de un único primer valor de hash calculado a partir del conjunto de datos (36) de juego de casino o el software de información por medio de una función de hash;

un segundo medio (29) para almacenar: a) un programa de autenticación que puede calcular un segundo valor de hash a partir del conjunto de datos de juego de casino o software de información almacenado en el primer medio de almacenamiento (18, 19, 21), utilizando la citada función de hash y para desencriptar una firma encriptada almacenada en el primer medio de almacenamiento (18) para recuperar el primer valor de hash; y b) una porción inicial de un programa cargador en el que la porción inicial del programa cargador requiere que el programa de autenticación se invoque antes de la iniciación de cualquier juego de casino;

un tercer medio (30) para almacenar una porción restante del programa cargador en el que el tercer medio (30) es una memoria modificable;

un medio de proceso (12) para permitir que el programa de autenticación calcule un valor de hash a partir de conjunto de datos (36) de juego de casino la información almacenada en el software del primer medio de almacenamiento (18, 19, 21), utilizando una función de hash y para permitir que el programa de autenticación desencripte la firma encriptada (37) almacenada en el primer medio de almacenamiento (18, 19, 21) para proporcionar un valor de hash desencriptado, y

un medio (12) para comparar el segundo valor de hash calculado con el valor de hash desencriptado abreviado para determinar si existe una coincidencia.

12. El sistema de la reivindicación 11, **que se caracteriza porque** el citado primer medio de almacenamiento (18, 19, 21) comprende un dispositivo de almacenamiento masivo (18, 19) o un dispositivo de memoria.

13. El sistema de la reivindicación 12, **que se caracteriza porque** el citado dispositivo de memoria comprende una memoria de sólo lectura.

14. El sistema de la reivindicación 12, **que se caracteriza porque** el citado dispositivo de memoria comprende una memoria RAM.

15. El sistema de la reivindicación 12, **que se caracteriza porque** el citado dispositivo de almacenamiento masivo (18, 19) comprende una unidad de disco (18, 19).

16. El sistema de la reivindicación 12, **que se caracteriza porque** el citado dispositivo de almacenamiento masivo (18, 19) comprende una unidad de CD-ROM.

17. El sistema de la reivindicación 12, **que se caracteriza porque** el citado dispositivo de almacenamiento masivo (18, 19) comprende una unidad de almacenamiento en red.

18. El sistema de una de las reivindicaciones 11 a 17, **que se caracteriza porque** el citado segundo medio de almacenamiento masivo (29) comprende un dispositivo de memoria de sólo lectura (29).

19. El sistema de la reivindicación 18, **que se caracteriza porque** el citado dispositivo de memoria de sólo lectura (29) comprende un dispositivo de memoria no modificable.

20. El sistema de la reivindicación 18 ó 19, **que se caracteriza porque** el citado dispositivo de memoria de sólo lectura (29) incluye una primera porción para almacenar la porción del citado programa de autenticación que puede calcular el valor de hash del conjunto de datos (36) o la información de software, y una segunda porción para almacenar la parte del programa de autenticación que puede desencriptar la firma encriptada.

21. El sistema de la reivindicación 20, **que se caracteriza porque** la citada segunda porción de ROM se utiliza para almacenar una clave de desencriptado (34).

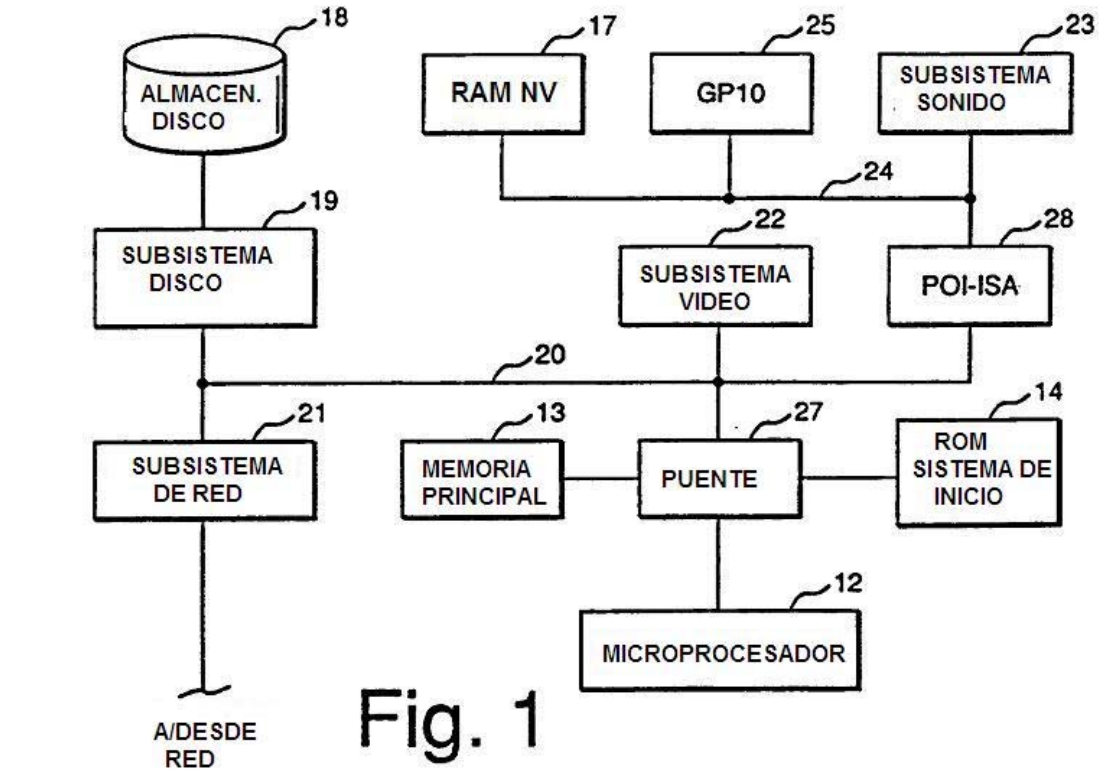

Fig. 1

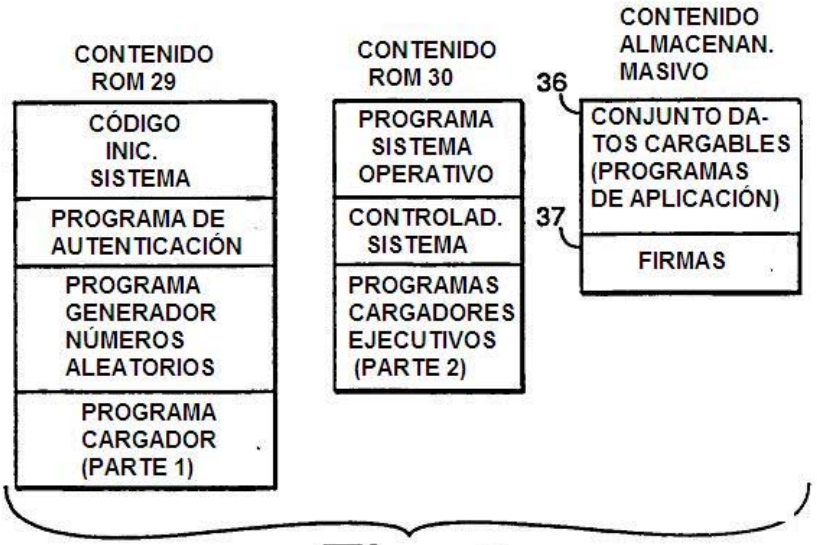

Fig. 2

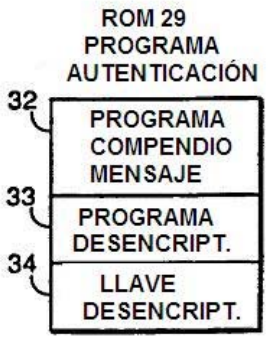

Fig. 3

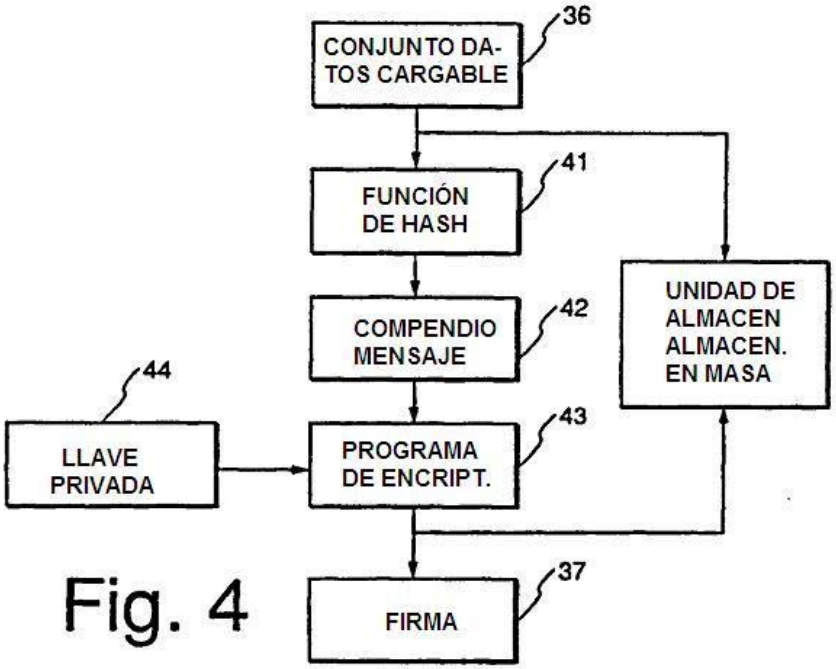
CONJUNTO DA-
TOS CARGABLE
36
FUNCIÓN
DE HASH
41
COMPENDIO
MENSAJE
42
UNIDAD DE
ALMACEN
ALMACEN.
EN MASA
44
LLAVE
PRIVADA
PROGRAMA
DE ENCRIPT.
43
FIRMA
37

Fig. 4

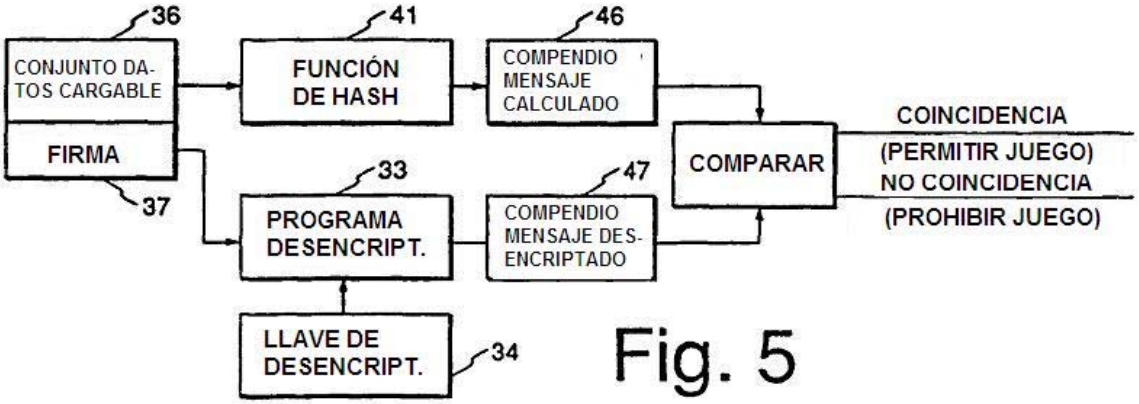
36
CONJUNTO DA-
TOS CARGABLE
FIRMA
37
41
FUNCIÓN
DE HASH
46
COMPENDIO
MENSAJE
CALCULADO
COMPARAR
COINCIDENCIA
(PERMITIR JUEGO)
NO COINCIDENCIA
(PROHIBIR JUEGO)
33
PROGRAMA
DESENCRIPT.
47
COMPENDIO
MENSAJE DES-
ENCRIPTADO
LLAVE DE
DESENCRIPT.
34

Fig. 5

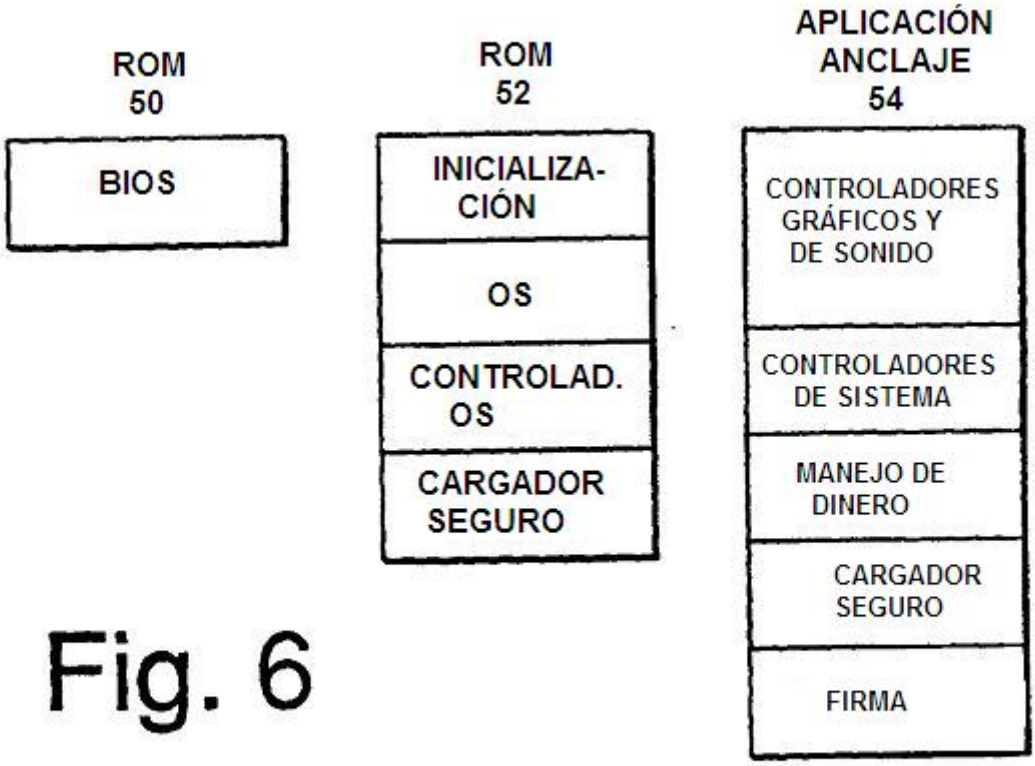
ROM
50
BIOS
ROM
52
INICIALIZA-
CIÓN
OS
CONTROLAD.
OS
CARGADOR
SEGURO
APLICACIÓN
ANCLAJE
54
CONTROLADORES
GRÁFICOS Y
DE SONIDO
CONTROLADORES
DE SISTEMA
MANEJO DE
DINERO
CARGADOR
SEGURO
FIRMA

Fig. 6