(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 510 642**

(51) Int. CI.:

G11B 20/00 (2006.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04N 21/426 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.12.2003 E 03780530 (6)**

(97) Fecha y número de publicación de la concesión europea: **09.07.2014 EP 1590804**

(54) Título: **Método y dispositivo de control de acceso a medio de almacenamiento fiable**

(30) Prioridad:

24.01.2003 EP 03100145

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.10.2014

(73) Titular/es:

INTRINSIC ID B.V. (100.0%)
HIGH TECH CAMPUS 9
5656 AE EINDHOVEN, NL

(72) Inventor/es:

LINNARTZ, JOHAN P. M. G.

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método y dispositivo de control de acceso a medio de almacenamiento fiable

La presente invención se refiere a un procedimiento y dispositivo para dar acceso a contenido de un medio de almacenamiento en el que datos criptográficos utilizados para determinar si se debe dar acceso se obtienen a partir de una propiedad del medio de almacenamiento.

La presente invención se refiere además a un aparato de reproducción y/o grabación que comprende tal dispositivo, y a un producto de programa informático dispuesto para hacer que un procesador ejecute el método de acuerdo con la invención.

Para proteger el contenido de medios de almacenamiento como CD, DVD, etc. contra copias no autorizadas, el contenido se suele almacenar de manera cifrada. Esto significa que un aparato de reproducción autorizado necesita poder obtener las claves de descifrado necesarias, preferentemente de tal forma que los aparatos de reproducción no autorizados no puedan obtener estas claves. Normalmente, estas claves de descifrado se generan basándose en datos escondidos en el medio de almacenamiento, preferentemente junto con datos escondidos en el reproductor. Los reproductores autorizados se proveen con tales datos durante su fabricación. Este sistema se usa, por ejemplo, para los vídeos en DVD.

En lo anteriormente referido, existe la posibilidad de un ataque de clonación en el que el contenido cifrado y los datos de descifrado escondidos en el medio de almacenamiento pueden copiarse por completo sobre un segundo medio de almacenamiento. La protección contra este tipo de ataque de clonación se puede lograr escondiendo los datos de descifrado en el disco mismo, en vez de almacenarlos como datos en el medio de almacenamiento. Una forma de realizar esto es mediante el uso de la denominada “fluctuación”. Los datos de descifrado se obtienen del medio de almacenamiento como variaciones en un parámetro físico del medio de almacenamiento. Distintos medios tendrán una fluctuación distinta o estarán desprovistos de fluctuación, de manera que se generarán distintas claves de descifrado para ese disco, lo que significa que fallará el descifrado del contenido. Se hace referencia a la patente US 5.724.327 (expediente del mandatario PHN 13922) del mismo cesionario que la presente invención, en la cual se describen varias técnicas para crear dicha “fluctuación” y almacenar información en la misma.

Las aberraciones que suceden de modo natural que se producen en el proceso de estampado de discos CD o DVD grabables pueden usarse para crear una clave criptrográfica para el cifrado del contenido que se va a grabar en estos discos. Se hace referencia al documento EP-A-0 706 174 como ejemplo del uso de propiedades que suceden de modo natural de un disco para generar un identificador único. Un problema conocido con este tipo de planteamientos es que pequeñas desviaciones en la medición de las propiedades físicas pueden producir la clave equivocada. Normalmente esto se evita usando, en vez de propiedades que suceden de modo natural, identificadores medibles con fiabilidad, realizados intencionadamente. Se hace referencia a la patente US 6.209.092 (expediente del mandatario PHN 16372) del mismo cesionario y del mismo inventor que la presente invención, que describe una técnica para deducir un identificador criptográfico a partir de datos complementarios escritos intencionadamente. Esto requiere un procesamiento adicional del disco, lo cual complica y encarece el proceso.

Es un objetivo de la presente invención proporcionar un método de acuerdo con el preámbulo, que tolere pequeñas desviaciones en el valor medido de la propiedad del medio de almacenamiento.

Este objetivo se logra de acuerdo con la invención mediante un método que comprende obtener datos criptográficos a partir de una propiedad del medio de almacenamiento, leer datos de ayuda del medio de almacenamiento, y dar el acceso basándose en una aplicación de una función contractiva de delta a los datos criptográficos y los datos de ayuda.

Una función contractiva de delta es una función que tiene una entrada primaria (los datos criptográficos), una entrada secundaria (los datos de ayuda) y que genera una salida basándose en las entradas primaria y secundaria. La entrada secundaria es una entrada de control en el sentido de que define intervalos de valores para la señal de entrada primaria y el valor de salida correspondiente para cada intervalo de valores de entrada primarios.

Más concretamente, para cualquier valor de entrada original arbitrario, la función contractiva de delta permite elegir un valor adecuado para la entrada secundaria, de manera que cualquier valor de la entrada primaria lo suficientemente parecido a dicho valor de entrada primaria original lleva al mismo valor de salida. Por otro lado, valores sustancialmente diferentes de la entrada primaria llevan a valores diferentes de la salida.

El valor medido ha de cuantificarse en valores discretos antes de poder procesarse criptográficamente. Puesto que es probable que toda medida contenga algo de ruido, el resultado de la cuantificación puede diferir de un experimento a otro. En particular, si un parámetro físico adopta un valor cercano a un umbral de cuantificación, cantidades mínimas de ruido podrían cambiar el resultado. Tras la aplicación de los datos cuantificados a una función criptográfica, los cambios mínimos se verán magnificados y el resultado no se parecerá en absoluto al resultado previsto. Esto es fundamentalmente una propiedad necesaria de las funciones criptográficas.

La función contractiva de delta mejora la fiabilidad de los datos criptográficos obtenidos porque permite elegir los datos de ayuda de manera adecuada para adaptar los datos criptográficos que estén demasiado cerca de un umbral de cuantificación a una portadora es particular. Entonces es posible usar medidas de aberraciones que suceden de modo natural aunque tales medidas sean poco fiables.

Tanto en la solicitud de patente internacional WO 00/51244 como el artículo correspondiente, "*A Fuzzy Commitment Scheme*", de An Juels y Martin Wattenberg, publicado en G. Tsudik, ed., *Sixth ACM Conference on Computer and Communications Security*, págs. 28-36, ACM Press, 1999, se divulga el denominado sistema de asignación difusa que autentica a las personas basándose en un valor biométrico cercano a, pero no necesariamente igual que, un valor de referencia. El sistema evita cualquier aprendizaje acerca del valor de referencia por parte de un agresor. El artículo se limita a describir aplicaciones biométricas del sistema y no divulga, insinúa ni sugiere la aplicación del sistema a la protección contra copias, ni mucho menos a la autenticación basada en fluctuación de los medios de almacenamiento.

En las reivindicaciones dependientes se exponen varios modos de realización ventajosos.

Es otro objetivo de la presente invención proporcionar un dispositivo de acuerdo con el preámbulo, que pueda tolerar pequeñas desviaciones en el valor medido de la propiedad del medio de almacenamiento.

Este objetivo se logra de acuerdo con la invención mediante un dispositivo dispuesto para dar acceso al contenido de un medio de almacenamiento, que comprende unos primeros medios de lectura para obtener datos criptográficos a partir de una propiedad del medio de almacenamiento, unos segundos medios de lectura para leer datos de ayuda del medio de almacenamiento, y medios de control de acceso para dar el acceso basándose en una aplicación de una función contractiva de delta a los datos criptográficos y los datos de ayuda.

Estos y otros aspectos de la invención serán evidentes y se dilucidarán con referencia a los modos de realización representados en los dibujos, en los que:

la figura 1 muestra una representación esquemática de un sistema que comprende un medio de almacenamiento y un aparato anfitrión de acuerdo con la invención;
la figura 2 muestra una ilustración esquemática de un proceso de autorización;
la figura 3 muestra una ilustración esquemática de un modo de realización de una función contractiva de delta;
la figura 4 muestra una ilustración esquemática de un aparato de reproducción de audio que comprende el aparato anfitrión.

En todas las figuras, referencias numéricas iguales indican características similares o correspondientes. Algunas de las características que se indican en los dibujos se implementan normalmente en el software, y por lo tanto representan entidades de software, tales como módulos u objetos de software.

La figura 1 muestra una representación esquemática de un sistema 100 que comprende un medio de almacenamiento 101 y un aparato anfitrión 110 conforme a la invención. El aparato anfitrión 110 comprende un receptáculo 111 en el que un usuario puede colocar el medio de almacenamiento 101, un módulo de lectura 112 para leer datos del medio de almacenamiento 101, varios medios de procesamiento 113-117 para procesar el contenido leído a partir del medio de almacenamiento 101 y para alimentar los datos procesados del contenido hacia una salida 119, y hacia un módulo de entrada 118 del usuario, con el que utilizando el usuario podrá controlar las operaciones del aparato anfitrión 110. El aparato anfitrión 110 también comprende un módulo de control 120, cuyos funcionamientos se tratan a continuación.

En la figura 1 el aparato anfitrión 110 se materializa en un lector de discos óptico, como por ejemplo un lector de Discos Compactos (CD) o de Discos Versátiles Digitales (DVD). Sin embargo, el aparato 110 podría también materializarse fácilmente en una disquetera o en un lector para medios de almacenamiento tales como discos duros externos, tarjetas inteligentes, memorias flash, etc. El sistema 100 del que forma parte el aparato anfitrión 110 puede ser, por ejemplo, un reproductor y/o una grabadora de Discos Compactos, un Disco Versátil Digital y/o un reproductor/grabadora de estos, un ordenador personal, un sistema de televisión o radio, etc. La figura 4 muestra una ilustración esquemática de un aparato de reproducción de audio 400 que comprende el aparato anfitrión 110. Se ha dispuesto el aparato 400 para reproducir y/o grabar el contenido del medio de almacenamiento 101 solo si el aparato anfitrión 110 da el acceso adecuado. Por ejemplo, si el aparato anfitrión 110 solo da acceso de lectura, el aparato 400 no realizará ninguna grabación ni copia del contenido.

Después de que el usuario coloque el medio de almacenamiento 101 en el receptáculo 111, se activa el módulo de lectura 112. Esta activación puede ser automática o en respuesta a una activación por parte del usuario del módulo de entrada del usuario 118, por ejemplo pulsando un botón. Se da por hecho que se necesita autorización para acceder al contenido grabado en el medio de almacenamiento 101, por ejemplo para permitir que el contenido se lea, se reproduzca, se procese o se copie. Para determinar si está autorizado el acceso, el módulo de lectura 112 pasa a leer datos criptográficos del medio de almacenamiento 101 y alimenta estos datos criptográficos al módulo de control 120.

El módulo de control 120 recibe los datos criptográficos e intenta autorizar el acceso basándose en estos datos. Este intento posiblemente también implique los datos criptográficos almacenados en el aparato anfitrión 110 o datos criptográficos suministrados por el sistema 100. Si esta autorización no puede establecerse, el módulo de control 120 indica un estado de error, por ejemplo suministrando una señal de error a la salida 119 o activando un LED en el panel anterior del aparato anfitrión 110.

Si la autorización se establece, el módulo de lectura 112 lee los datos del contenido del medio de almacenamiento 101 y los alimenta a los medios de procesamiento 113-117. Es posible que se necesiten distintos medios de lectura para leer los datos criptográficos y para leer los datos del contenido, en función de la naturaleza del almacenamiento de los datos criptográficos. La salida de los medios de procesamiento 113-117 va a la salida 119, desde la cual otros componentes del sistema 100 podrán leer el contenido (por ejemplo, reproduciéndolo como una película o generando señales de audio para su reproducción a través de altavoces). Podría ser deseable permitir que el aparato anfitrión 110 establezca primero que está instalado en un sistema compatible 100. Esto cobra particular importancia cuando la salida 119 es una salida digital. Si no puede establecerse la compatibilidad del sistema 100, ningún contenido deberá presentarse en la salida 119.

El aparato anfitrión 110 podrá dotarse de una gran variedad de medios de procesamiento. En el ejemplo de realización de la figura 1, los medios de procesamiento comprenden un módulo de descifrado 113, un módulo de detección de marca de agua 114, un módulo de acceso condicional 115, un módulo de procesamiento de señal 116 y un módulo de cifrado de bus 117.

En primer lugar, el módulo de descifrado 113 descifra el contenido tal y como se lee en el medio de almacenamiento 101, utilizando una clave de descifrado que suministra el módulo de control 120. El módulo de detección de marca de agua 114 procesa los datos de contenido descifrados para encontrar una marca de agua que contenga datos incorporados. La marca de agua podría comprender, por ejemplo, datos de gestión de derechos digitales, una identificación del titular del contenido o una referencia a la portadora de almacenamiento.

Se dispone el módulo de acceso condicional 115 para regular el acceso a los datos del contenido. Podría programarse para imponer un régimen estricto de no copiar, o para no permitir que se alimente el contenido a una salida digital. En tal caso, el módulo de acceso condicional 115 señala al módulo de procesamiento de señal 116 que solo se han de generar y alimentar señales analógicas a la salida 119. El módulo de acceso condicional 115 también podría programarse para activar mecanismos de protección contra copias (tipo Macrovision u otro) en las señales con las que se va a alimentar la salida analógica 119. El módulo de acceso condicional 115 también podría programarse para incorporar un tipo particular de marca de agua en las señales con las que se va a alimentar la salida 119. El modo de acceso condicional 115 también podría programarse para activar el cifrado de un tipo particular en las señales con las que se va a alimentar una salida digital 119.

El módulo de procesamiento de señal 116 es el encargado de transformar los datos de contenido en señales que puedan presentarse en la salida 119. Esto comprende, por ejemplo, la generación de señales analógicas de audio y/o vídeo, pero podría comprender también la incorporación de datos de marca de agua en las señales, el filtrado de porciones concretas del contenido, la generación de una versión de modos de reproducción no convencional del contenido, etc. Las operaciones exactas de procesamiento y transformación de señal que han de realizarse dependerán, por ejemplo, del tipo de contenido, los datos de gestión de derechos digitales incorporados en el contenido, la salida del módulo de acceso condicional 115, etc.

El módulo de cifrado de bus 117 cifra las señales de audio y/o vídeo que han de presentarse en la salida 119. Por ejemplo, el aparato anfitrión 110 podría emprender un protocolo de autenticación con otro componente del sistema 100. Como resultado de esto, el aparato anfitrión 110 y el otro componente comparten una clave secreta. Entonces el contenido puede cifrarse con la clave secreta y presentarse en la salida 119 de forma cifrada. De esta manera, otros componentes con capacidad de leer a partir de la salida 119 (por ejemplo, al escuchar en el bus al que va conectada la salida 119) no podrán acceder al contenido.

Es importante observar que los módulos de procesamiento 113-117 son todos componentes del aparato anfitrión 110 que podrán implementarse total o parcialmente a través de software. No es necesario siempre usar todos estos módulos 113-117. Una configuración y control flexibles de estos módulos 113-117 puede lograrse mediante el uso del planteamiento descrito en la solicitud de patente europea con número de serie 02077406.3 (expediente del mandatario PHNL020549) del mismo cesionario que la presente solicitud.

Los datos criptográficos se codifican en el medio de almacenamiento 101 como variaciones 102 en un parámetro físico del medio de almacenamiento, presentando dichas variaciones un patrón de modulación que representa los datos criptográficos. Este tipo de parámetro físico de un medio de almacenamiento a veces se denomina una “fluctuación” del medio de almacenamiento. Se hace referencia a la patente US 5.724.327 (expediente del mandatario PHN 13922) del mismo cesionario que la presente invención, en la cual se describen varias técnicas para crear dicha “fluctuación” y almacenar información en la misma. Lógicamente, también pueden usarse como semilla las variaciones que suceden de modo natural de dicho parámetro físico.

Preferentemente, los datos criptográficos se representan como patrón de marcas detectables ópticamente en alternancia con zonas intermedias dispuestas a lo largo de dicha pista del mismo. Estas variaciones 102 son preferentemente variaciones en la posición de la pista en dirección transversal al sentido de la pista.

En otra realización, el medio de almacenamiento 101, con marcas de información a lo largo de una pista del mismo, presenta unas primeras variaciones provocadas por la existencia y no existencia de las marcas de información a lo largo de la pista, representando dichas primeras variaciones una señal de información grabada en la portadora de registro, y unas segundas variaciones provocadas por variaciones asociadas con la pista, presentando dichas segundas variaciones un patrón de modulación que representa un código.

Entonces el módulo de lectura 112 lee estas variaciones 102 de un parámetro físico del medio de almacenamiento y reconstruye los datos criptográficos, los cuales se suministran a continuación al módulo de control 120. La medición de las variaciones en el parámetro físico suele exigir un circuito especial, por ejemplo conectado al lazo de control de servos del lector óptico del disco. Las variaciones medidas pueden comprender los datos criptográficos con datos adicionales, por ejemplo una Comprobación de Redundancia Cíclica (CRC) para compensar pequeños errores de la medición. Los datos criptográficos pueden almacenarse de forma comprimida o cifrarse de otra manera. Por lo tanto, puede ser necesario descomprimir, decodificar o procesar de otra manera las variaciones medidas antes de que los datos criptográficos estén disponibles de forma útil. Si hay que aumentar o procesar de otra manera estas variaciones antes de poder usarlas para otros fines, entonces las variaciones procesadas representan los datos criptográficos.

Cabe observar que no es necesario elegir el parámetro físico de tal forma que pueda medirse de manera fiable. Las aberraciones que suceden de modo natural que ocurren en el proceso de estampado de discos CD o DVD grabables pueden usarse a modo de parámetro. Esto se explicará en más detalle a continuación.

El módulo de lectura 112 también lee los datos de ayuda del medio de almacenamiento 101. Estos datos de ayuda pueden grabarse en el medio de almacenamiento 101 de manera convencional, por ejemplo como pista de datos en un CD, o en un sector especial del medio 101. Es concebible que estos también puedan incorporarse en el contenido grabado en el medio de almacenamiento 101, por ejemplo usando una marca de agua.

El proceso de autorización del módulo de control 120 basándose en el cual se da acceso al medio de almacenamiento 101 se basa en una aplicación de una función contractiva de delta a los datos criptográficos y los datos de ayuda. Para presentar esta aplicación, en primer lugar se analiza algo de notación.

- Y: los datos criptográficos, tal y como se obtienen mediante la medición del valor del parámetro físico del medio de almacenamiento 101.
- W: los datos de ayuda leídos a partir del medio de almacenamiento 101.
- V: un valor de control.
- G(): la función contractiva de delta.
- F(): una función criptográfica, preferentemente una función de troceo unidireccional en sentido estricto, pero se puede usarse cualquier función criptográfica si esta es capaz de conseguir las propiedades criptográficas deseadas, por ejemplo una función de troceo unidireccional con clave, una función de troceo trampa, una función de descifrado asimétrico, o incluso una función de cifrado simétrico.

El proceso de autorización, ilustrado en la figura 2, procede entonces da la siguiente manera. Los datos criptográficos Y y los datos de ayuda W se obtienen de la forma descrita anteriormente y con ellos se alimenta el módulo de contracción 205. En el presente caso, la función contractiva de delta G() se aplica a los datos criptográficos Y y a los datos de ayuda W:

$$Z = G(Y, W)$$

La función criptográfica F(), por ejemplo una de las conocidas funciones criptográficas unidireccionales de troceo SHA-1, MD5, RIPE-MD, HAVAL o SNERFU, se aplica a la salida de la función contractiva de delta G() en el módulo de aplicación de función de troceo 206:

$$U = F(Z) = F(G(Y,W))$$

La salida U de la función F() se compara en el comparador 207 frente a un valor de control V. Si U concuerda con V, se da la autorización, en caso contrario no se da autorización alguna. El valor de control V puede estar presente en el medio de almacenamiento 101 al igual que el valor de ayuda W, u obtenerse a través de otra vía de acceso. Por ejemplo, podría almacenarse en una tarjeta inteligente, en una microplaca en disco (*Chip-In-Disc*) fijada al medio de almacenamiento (véase, por ejemplo, la solicitud de patente internacional WO 02/17316 (expediente del mandatario PHNL010233) del mismo solicitante de la presente solicitud) u obtenerse contactando con un servidor externo.

El valor de control V se calcula previamente, por ejemplo durante la fabricación del medio de almacenamiento 101 o al grabar el contenido en el medio de almacenamiento 101. Se lee el parámetro físico para obtener un valor X. El

valor V se calcula como la salida de una aplicación de la función de troceo F() a algún valor secreto S seleccionado de forma (pseudo-)aleatoria:

$$\mathbf{V = F(S)}$$

El valor secreto S también se utiliza para determinar el valor de ayuda W. W se calcula de tal forma que G(X, W) sea igual a S. En la práctica, esto significa que G() permite el cálculo de una inversa $W = G^{-1}(X, S)$.

Tal como se ha explicado anteriormente, para cualquier valor de entrada arbitrario, la función contractiva de delta G() permite elegir un valor adecuado para la entrada secundaria, de manera que cualquier valor de la entrada primaria lo suficientemente parecido a dicho valor de entrada primaria original lleva al mismo valor de salida. Por otro lado, valores sustancialmente diferentes de la entrada primaria llevan a valores de salida diferentes.

Una propiedad altamente deseable, pero para la finalidad de la invención no estrictamente necesaria, es la del "revelado de épsilon". Esta propiedad aborda el supuesto de que un verificador deshonesto vea solo el valor de la entrada secundaria de la función, pero no la entrada primaria. En tal caso, el verificador debería aprender poco (por ejemplo, no más que épsilon) acerca del valor de salida. Un ejemplo típico de tal ataque es una unidad de disco modificada por un pirata informático que intenta obtener datos de un disco copiado ilegalmente, sin los datos criptográficos Y.

Como primera realización, la entrada secundaria puede seleccionarse como lista exhaustiva de todos los posibles valores de entrada primaria y sus correspondientes valores de salida. Una segunda realización utiliza una función que resta de la entrada primaria la entrada secundaria y redondea el resultado al entero más cercano, o que correlaciona el resultado de la resta al punto más cercano de una retícula geométrica determinada (véase el artículo de Juels y Wattenberg al que se ha hecho referencia anteriormente).

En otro modo de realización, se supone que la entrada primaria Y es un vector de valores. La entrada secundaria es un vector W que contiene información acerca de qué registros de Y contienen 'grandes' valores que no provocarían ambigüedad en caso de cuantificarse en un valor discreto. Este Z = W * sign(Y), donde * es una multiplicación registro por registro, y el vector W contiene 0 y 1 valores. La función sign(Y) devuelve -1 si Y es negativo, +1 si Y es positivo, y 0 si Y es igual a 0, por lo que el vector resultante contiene -1, 0 y unos.

En otro modo de realización, G(W,Y) aplica un esquema de corrección de errores. Y se cuantifica en valores discretos. W contiene redundancia. Por ejemplo en el presente caso, considérese un código Hamming (7,4) capaz de corregir un error. En este ejemplo de un código (7,4), la longitud de Y más la longitud de W es 7, y la longitud de Y es 4. Por lo tanto, W debería ser de longitud 3. Y contiene 4 elementos: $Y = (y_1, y_2, y_3, y_4)$ y W contiene 3 elementos: $W = (w_1, w_2, w_3)$. Durante la adquisición de datos, se define

- $w_1 = \text{sign}(x_1) \oplus \text{sign}(x_2) \oplus \text{sign}(x_3)$
- $w_2 = \text{sign}(x_1) \oplus \text{sign}(x_2) \oplus \text{sign}(x_4)$
- $w_3 = \text{sign}(x_1) \oplus \text{sign}(x_3) \oplus \text{sign}(x_4)$

La salida Z contiene 3 elementos (z_1, z_2, z_3). Estos se calculan como

$$\mathbf{(z_1, z_2, z_3) = G(sign(yi), sign(y_2), sign(y_3), sign(y_4), wi, w_2, w_3)}$$

donde G es una función de decodificación, por ejemplo como se describe en J. B. Fraleigh, "*A first code in Abstract Algebra*", Addison Wesley, Reading, MA, 1993, 5ª Ed. págs. 149-157. Un decodificador de distancia mínima investiga la cadena de 7 bits $\text{sign}(y_1)$, $\text{sign}(y_2)$, $\text{sign}(y_3)$, $\text{sign}(y_4)$, w_1, w_2, w_3 .

Si la cadena no cumple la condición

- $w_1 = \text{sign}(y_1) \oplus \text{sign}(y_2) \oplus \text{sign}(y_3)$,
- $w_2 = \text{sign}(y_1) \oplus \text{sign}(y_2) \oplus \text{sign}(y_4)$ y
- $w_3 = \text{sign}(y_1) \oplus \text{sign}(y_3) \oplus \text{sign}(y_4)$,

el decodificador tratará de invertir uno de los bits de la cadena de 7 bits hasta que bien la cadena modificada cumpla la condición anterior, bien todos los bits se hayan invertido sin que la cadena modificada haya cumplido la condición. Esta función es aparentemente contractiva de delta, donde delta es igual a 1 bit. El valor de control V se calcula previamente durante la adquisición de datos, como $V = F(s_1, s_2, s_3)$.

Aunque esta función G() es contractiva de delta, o sea que es insensible a perturbaciones mínimas de Y, presenta propiedades menos favorables a la hora de ocultar el valor de Z si solo se conoce W. De hecho, la función revela tres bits: para un W determinado, la incertidumbre en Y se reduce de 4 bits a 1 bit. Sin embargo, para palabras de código mayores, estas propiedades pueden realizarse de forma más favorable, particularmente si la tasa del código es significativamente inferior a la mitad. En estos casos solo un número reducido de bits de redundancia W se

ofrecen al verificador, con respecto al número de bits desconocidos de Y. Se hace referencia al artículo de Juels y Wattenberg al que se ha hecho referencia anteriormente para un análisis del uso de la codificación.

En otra realización más, las entradas primaria y secundaria son vectores de longitud idéntica: Y = (y_1, y_2, y_3, ...), W = (w_1, w_2, w_3, ...) y Z = (z_1, z_2, z_3, ...). Para la dimensión *i*-ésima de Y, W y Z, la función contractiva de delta G() es

$$z_i = \begin{cases} 1 & si\ 2nq \le y_i + w_i < (2n+1)q, \quad para\ cualquier\ n = .., -1, 0, 1, .. \\ 0 & si\ (2n-1)q \le y_i + w_i < nq,, \quad para\ cualquier\ n = .., -1, 0, 1, .. \end{cases}$$

donde *q* es el valor de incremento.

Durante la adquisición de datos, se mide el elemento *i*-ésimo de X (indicado como x_i). Para W, un valor de w_i debe calcularse de tal manera que el valor de x_i+w_i se pase a un valor donde $x_i + w_i + \delta$ se cuantifique al mismo z_i para cualquier δ pequeño. Se selecciona un valor secreto de S como vector con la misma longitud que Y, W y Z. Para la *i*-ésima dimensión de S, w_i y el entero *n* se seleccionan de tal forma que para el x_i medido,

$$w_i = \begin{cases} \left(2n + \frac{1}{2}\right) q - x_i & si\ s_i = 1 \\ \left(2n - \frac{1}{2}\right) q - x_i & si\ s_i = 0 \end{cases}$$

En el presente caso, *n* = ..., -1, 0, 1, 2, ... se selecciona de tal forma que $-q/2 < w_i < q/2$. El valor de *n* se desecha, pero los valores de w_i se facilitan como datos de ayuda W. El valor de control V se obtiene directamente del S secreto, como V = F(S). Durante la autenticación, el módulo contractivo 205 ejecuta la función contractiva de delta G() definida anteriormente para obtener Z.

De los modos de realización hasta ahora presentados, puede reconocerse la existencia de varias clases de funciones contractivas de delta. En una implantación versátil, la función contractiva de delta puede implicar una o más de las siguientes operaciones, en las que los datos de ayuda W se dividen en cuatro partes W_1, W_2, W_3 y W_4:

- una multiplicación de matrices (lineal) sobre el vector de entrada primaria Y (donde W_1 define la matriz).
- la suma lineal de datos de ayuda W_2, por ejemplo como Y + W2 (ilustrada en el último modo de realización mencionado).
- una cuantificación, donde W_3 define las áreas de cuantificación.
- decodificación de corrección de errores, donde W_4 puede contener, por ejemplo, bits de redundancia (ilustrado como el código Hamming (7,4), donde los bits de redundancia se toman de los datos de ayuda directamente).

La figura 3 da un ejemplo de la combinación de todas las operaciones anteriores. La función contractiva de delta G() se divide en una operación de matriz lineal H (sobre los números reales o complejos), la suma de datos de ayuda W_2, un cuantificador/segmentador Q y un bloque de código de corrección de errores (CCE).

La operación H usa los datos de ayuda W_1 para producir la salida Y_1, que tiene una longitud de n_1 bits. El resultado de sumar los datos de ayuda W_2 es la salida Y_2, que tiene una longitud de *n2* bits. Con Y_2 se alimenta el cuantificador/segmentador Q, que produce a partir de Y_2 y W_3 una salida Y_3, también de longitud n_2. El bloque CCE calcula n_3 bits fiables Z a partir de la entrada Y_3 y W_4. La función criptográfica F() aplica una función de troceo a Z para obtener un U de longitud de n_4 bits.

Como ha demostrado el ejemplo de realización del código Hamming (7,4), este presenta ventajas en cuanto a propiedades de ocultación de información, para evitar el uso de bits de redundancia de corrección de errores en los datos de ayuda. Dicho de otra forma, es útil considerar una subclase de funciones contractivas de delta (funciones contractivas de delta sin redundancia) donde los datos de ayuda no se introduzcan en forma de bits redundantes (por ejemplo, bits CRC) en un código de corrección de errores. Los bits redundantes que se le ofrecen al decodificador se generan de la misma forma que las entradas primaria y secundaria, como bits de información, a diferencia del uso directo de bits de ayuda como entrada del decodificador de corrección de errores. La función contractiva de delta sin redundancia aun así puede contener decodificación de corrección de errores. En la figura 3, esto significaría que la señal W4 no está presente.

Es posible usar el valor Z como base para una clave de descifrado K para descifrar, en el módulo de descifrado 113, los datos de contenido cifrado DCC. El valor Z podría usarse tal cual, o procesarse, por ejemplo aplicándole una función de troceo. Sin embargo, en el presente caso no debería usarse la función de troceo F(Z), porque entonces la clave de descifrado sería igual al valor V, disponible en texto limpio. Aun así, para conservar la complejidad de una implantación práctica, se puede optar por usar F(Z'), donde Z' es una modificación mínima de Z, por ejemplo mediante la inversión de un bit.

Se puede deducir la clave de descifrado K adicionalmente a partir de datos suministrados por el sistema 100. Por ejemplo, el aparato 400 en el que está instalado el aparato anfitrión 110 puede programarse durante su fabricación

con un valor secreto que se concatena a la clave deducida de descifrado para obtener la clave de descifrado final necesaria para descifrar el contenido. Con la combinación del valor Z (procesado o sin procesar) y los datos suministrados por el sistema, podría alimentarse una función de troceo para obtener la clave de descifrado.

Posteriormente, el módulo de control 120 puede suministrar la clave de descifrado al módulo de descifrado 113, que la podrá usar de la manera descrita anteriormente para descifrar el contenido. De esta manera, el acceso al contenido se da de forma implícita. Si se obtiene la clave de descifrado equivocada, fallará el descifrado y no podrá obtenerse una salida adecuada. En este caso no es necesario obtener V y contrastar U con V, porque de la salida será evidente que el descifrado ha fallado.

También se puede controlar el acceso incluso si no hace falta suministrar claves de descifrado. Si el comparador 207 detecta alguna diferencia entre U y V, el módulo de control 120 puede suprimir las señales que se estén presentando en la salida 119. Dicho de otra forma, sea cual sea la protección del contenido en sí, si los datos U y V no concuerdan, no se da el acceso al contenido.

Esta última opción permite usar la presente invención como esquema de prevención de copias, por ejemplo para actualizar un sistema que no incluya cifrado. Un ejemplo es la grabación legal doméstica de audio descargado a un CD-R. Se puede aplicar el esquema de autenticación de la figura 2 a una nueva generación de reproductores. El valor de ayuda W y el valor de control V se almacenan en un CD-R virgen durante su fabricación. Un aparato de grabación almacena contenido sin codificar, para asegurar su compatibilidad con los reproductores de CD existentes. Los reproductores nuevos recuperan W y V del disco, ejecutan la autenticación y reproducen CD-R creados legalmente, pero no así copias de bits ilegales de estos. Dichas copias de bits ilegales también contendrán copias de los valores de W y V, pero puesto que este disco nuevo tiene una fluctuación diferente, el valor Y de este disco nuevo llevará a un valor de U que difiera de V.

Cabe señalar que los modos de realización mencionados anteriormente son de carácter ilustrativo y no limitativo, y que los expertos en la materia podrán diseñar muchos modos de realización alternativos sin alejarse del alcance de las reivindicaciones adjuntas.

Por ejemplo, la solicitud de la patente WO 01/95327 (expediente del mandatario PHNL000303) del mismo solicitante que la presente solicitud, divulga el almacenamiento de datos para la protección contra y el control de copias en un medio de almacenamiento según la manera habitual, utilizando a la par una variación hecha intencionadamente en un parámetro físico del medio de almacenamiento para almacenar un valor de troceo criptográfico de dichos datos. Mediante la comprobación de que un valor de troceo de los datos almacenados concuerda con el valor medido del parámetro físico, puede regularse el acceso al medio de almacenamiento. Almacenando también datos de ayuda y utilizando una función contractiva de delta de acuerdo con la presente invención, se mejora la fiabilidad de esta verificación.

En las reivindicaciones, los signos de referencia entre paréntesis no han de interpretarse como limitaciones a la reivindicación. La expresión “comprendiendo / que comprende” no excluye la presencia de elementos o etapas distintos de los que se enumeran en una reivindicación. La palabra “un” o “una” antes de un elemento no excluye la presencia de una pluralidad de tales elementos. La invención puede implantarse mediante hardware que comprenda varios elementos distintos, y mediante un ordenador adecuadamente programado.

En la reivindicación de dispositivo, que enumera varios medios, varios de estos medios pueden materializarse en un mismo artículo de hardware. El mero hecho de que ciertas medidas se mencionen en reivindicaciones dependientes diferentes entre sí no indica que una combinación de estas medidas no pueda usarse ventajosamente.

REIVINDICACIONES

1. Un método para dar acceso a contenido en un medio de almacenamiento (101), que comprende
obtener datos criptográficos (Y) a partir de variaciones en un parámetro físico del medio de almacenamiento (101), donde las variaciones en el parámetro físico (102) del medio de almacenamiento (101) son variaciones que suceden de modo natural en el parámetro físico,
leer datos de ayuda (W) del medio de almacenamiento (101), y
dar el acceso basándose en una aplicación de una función contractiva de delta a los datos criptográficos (Y) y los datos de ayuda (W).

2. El método de la reivindicación 1, que comprende deducir una clave de descifrado (K) para descifrar el contenido al menos de la aplicación de la función contractiva de delta.

3. El método de la reivindicación 2, que comprende deducir la clave de descifrado (K) adicionalmente a partir de datos suministrados por un aparato de reproducción o de grabación (400).

4. El método de la reivindicación 1, en el que se da el acceso si la salida de la función contractiva de delta corresponde a un valor de control (V).

5. El método de la reivindicación 4, que comprende aplicar una función criptográfica a la salida de la función contractiva de delta y comparar la salida de la función criptográfica con el valor de control (V).

6. El método de la reivindicación 5, en el que la función criptográfica es una función de troceo unidireccional.

7. El método de la reivindicación 4, donde el valor de control se almacena en una tarjeta inteligente.

8. El método de la reivindicación 4, donde el valor de control se graba en el medio de almacenamiento (101).

9. El método de la reivindicación 1, en el que la función contractiva de delta implica una combinación de uno o más de: una multiplicación de matrices sobre los datos criptográficos (Y), una suma lineal de al menos una porción de los datos de ayuda (W), una cuantificación en la cual las áreas de cuantificación las define una porción de los datos de ayuda (W), y decodificación de corrección de errores.

10. El método según una cualquiera de las reivindicaciones anteriores, donde los datos de ayuda definen intervalos de valores para los datos criptográficos y el valor de salida correspondiente para cada intervalo de los datos criptográficos.

11. El método según una cualquiera de las reivindicaciones anteriores, donde la función contractiva de delta aplica un esquema de corrección de errores y donde los datos de ayuda contienen redundancia, cuantificándose los datos criptográficos en valores discretos.

12. El método según la reivindicación 1, donde

- el medio de almacenamiento es un medio de almacenamiento estampado y el parámetro físico del medio de almacenamiento es una aberración producida durante el proceso de estampado del medio de almacenamiento.

13. Un método para calcular bits fiables a partir de datos criptográficos, que comprende obtener los datos criptográficos (Y) a partir de variaciones en un parámetro físico (102) de un medio de almacenamiento (101), donde las variaciones en el parámetro físico (102) del medio de almacenamiento (101) son variaciones que suceden de modo natural en el parámetro físico, leer datos de ayuda (W) del medio de almacenamiento (101), y calcular los bits fiables basándose en una aplicación de una función contractiva de delta a los datos criptográficos (Y) y los datos de ayuda (W).

14. Un dispositivo (110) dispuesto para dar acceso a contenido en un medio de almacenamiento (101), que comprende unos primeros medios de lectura (112) para obtener datos criptográficos (Y) a partir de variaciones en un parámetro físico del medio de almacenamiento (101), donde las variaciones en el parámetro físico (102) del medio de almacenamiento (101) son variaciones que suceden de modo natural en el parámetro físico, unos segundos medios de lectura (112) para leer datos de ayuda (W) del medio de almacenamiento (101), y unos medios de control de acceso para dar el acceso basándose en una aplicación de una función contractiva de delta a los datos criptográficos (Y) y los datos de ayuda (W).

15. Un aparato de reproducción y/o grabación (400) que comprende un dispositivo (101) según la reivindicación 14 y dispuesto para realizar la reproducción y/o grabación si el dispositivo (110) da acceso.

16. Un dispositivo (110) dispuesto para calcular bits fiables a partir de datos criptográficos, que comprende unos primeros medios de lectura (112) para obtener los datos criptográficos (Y) a partir de variaciones en un parámetro

físico (102) del medio de almacenamiento (101), donde las variaciones en el parámetro físico (102) del medio de almacenamiento (101) son variaciones que suceden de modo natural en el parámetro físico, unos segundos medios de lectura (112) para leer datos de ayuda (W) del medio de almacenamiento (101), y calcular los bits fiables basándose en una aplicación de una función contractiva de delta a los datos criptográficos (Y) y los datos de ayuda (W).

17. Un producto de programa informático dispuesto para hacer que un procesador ejecute el método de la reivindicación 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 y/o 13.

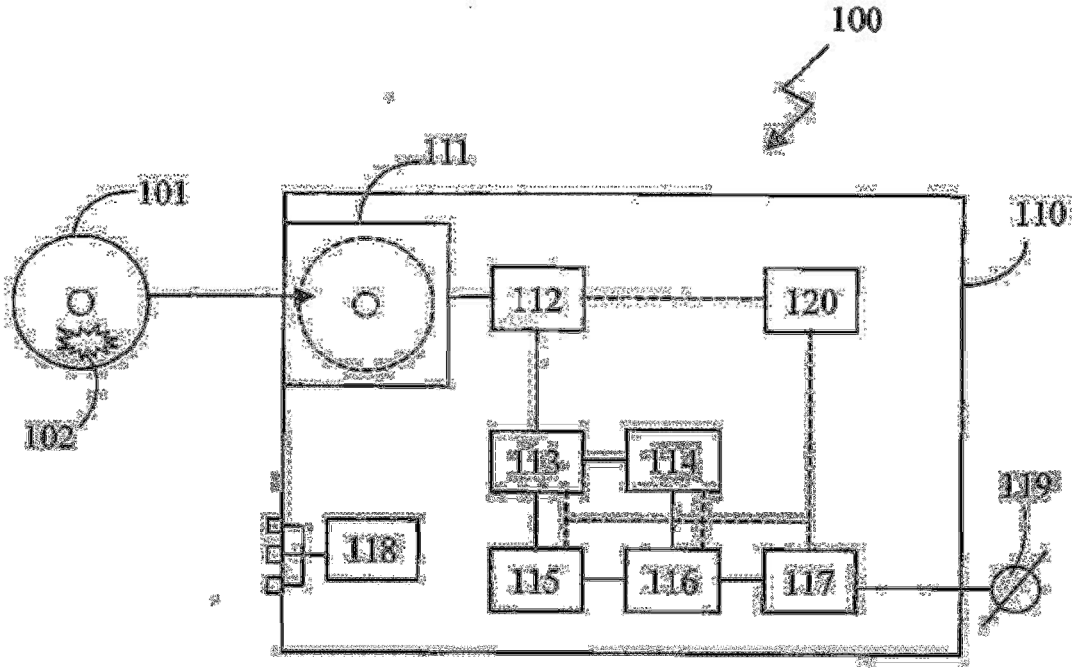
100
111
101
110
112
120
102
113
114
119
118
115
116
117

FIG.1

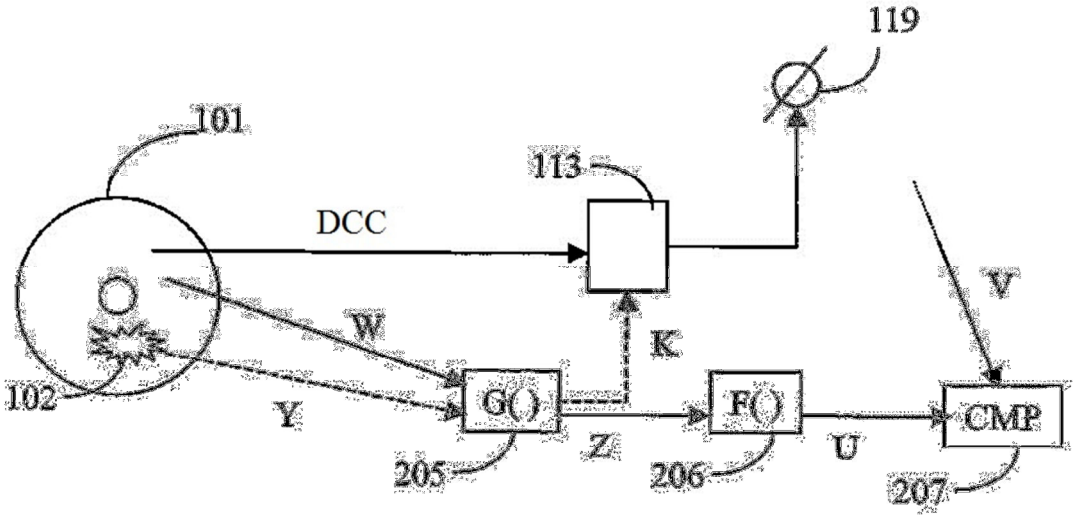
119
101
113
DCC
V
W
K
102
Y
G()
F()
CMP
Z
U
205
206
207

FIG.2

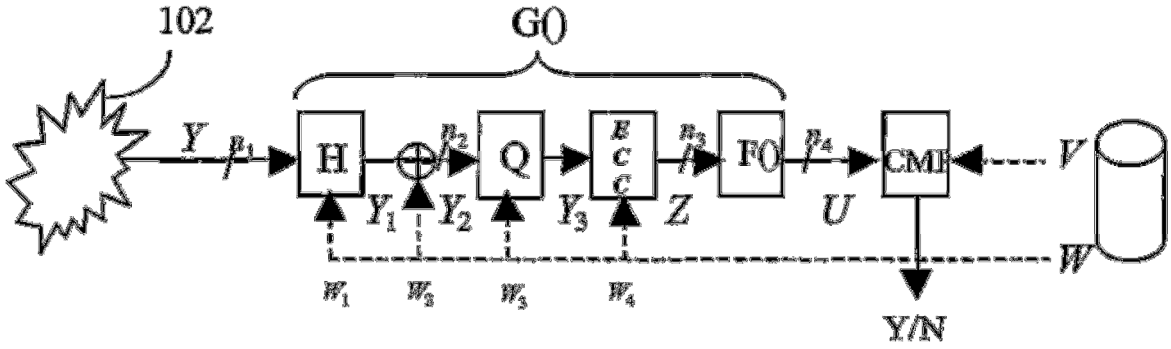

FIG.3

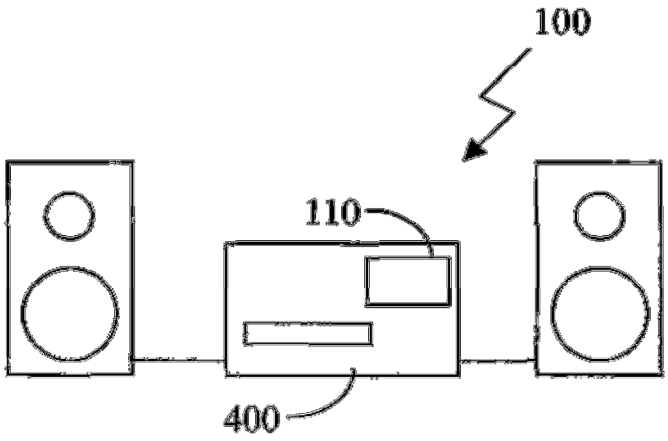

FIG.4