(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 572 159**

(51) Int. CI.:

H04L 9/32 (2006.01)
G06Q 20/40 (2012.01)
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.11.2009 E 09175755 (9)**

(97) Fecha y número de publicación de la concesión europea: **23.03.2016 EP 2323308**

(54) Título: **Un método de asignación de un secreto a un testigo de seguridad, un método de operación de un testigo de seguridad, un medio de almacenamiento y un testigo de seguridad**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.05.2016

(73) Titular/es:

MORPHO CARDS GMBH (100.0%)
Konrad-Zuse-Ring 1
24220 Flintbek, DE

(72) Inventor/es:

HÜBNER, THOMAS DR.

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Un método de asignación de un secreto a un testigo de seguridad, un método de operación de un testigo de seguridad, un medio de almacenamiento y un testigo de seguridad

Campo de la invención

La presente invención se refiere al campo de testigos de seguridad y más particularmente a asignar de manera segura un secreto a un testigo de seguridad.

Antecedentes y técnica relacionada

Los testigos de seguridad son como tales conocidos a partir de la técnica anterior. Típicamente un número de identificación personal (PIN) secreto se almacena en un testigo de seguridad para la autenticación de un usuario con relación al testigo de seguridad. Con el propósito de autenticación el usuario tiene que introducir el PIN en el testigo de seguridad el cual determina si el PIN almacenado y el PIN introducido son coincidentes.

Además, se conocen testigos de seguridad para generar una firma digital. Un testigo de seguridad para generar una firma digital almacena una clave privada de un par de claves criptográficas de un usuario. La discreción de la clave privada almacenada en el testigo de seguridad se puede preservar mediante medidas hardware de manera que cuando se abre el testigo hardware, se destruye inevitablemente la memoria que almacena la clave privada.

El documento WO 2008/010773 muestra un método de recuperación de un secreto descifrando un secreto cifrado biométricamente usando datos biométricos y comprobando el secreto comparando un valor de comprobación aleatoria del secreto recuperado con un valor de comprobación aleatoria del secreto original que se generó durante la fase de inscripción.

La invención aspira a proporcionar un método mejorado de asignación de un secreto a un testigo de seguridad, un método de operación de un testigo de seguridad para realizar una operación criptográfica, un medio de almacenamiento y un testigo de seguridad.

Compendio de la invención

La presente invención proporciona un método de operación de un testigo de seguridad para realizar una operación criptográfica según la reivindicación 1, un medio de almacenamiento que almacena instrucciones ejecutables según la reivindicación 11 y un testigo de seguridad como se reivindica en la reivindicación independiente 12. Las realizaciones de la invención se dan en las reivindicaciones dependientes.

De acuerdo con las realizaciones de la invención se proporciona un método de asignación de un secreto a un testigo de seguridad que comprende recibir unos primeros datos biométricos de un rasgo biométrico de una persona por el testigo de seguridad, almacenar los primeros datos biométricos en el testigo de seguridad, almacenar el secreto no cifrado en el testigo de seguridad, cifrar biométricamente el secreto usando los primeros datos biométricos mediante el testigo de seguridad, almacenar el secreto cifrado en el testigo de seguridad y borrar el secreto no cifrado y los primeros datos biométricos del testigo de seguridad.

Un ‘testigo de seguridad’ como se entiende en la presente memoria abarca cualquier dispositivo físico portátil que incluye una función criptográfica, tal como con los propósitos de autenticación, verificación, cifrado, descifrado o generación de una firma digital. Tales dispositivos físicos incluyen testigos hardware, testigos de autenticación, testigos USB, en particular memorias USB, tarjetas con chip, tarjetas con circuito integrado, tarjetas inteligentes, tarjetas de módulo de identidad de abonado (SIM), en particular tarjetas USIM, documentos de identidad que tienen un circuito electrónico integrado y etiquetas RFID.

El término ‘datos biométricos’ como se usa en la presente memoria puede referirse a los datos entregados por un sensor biométrico, tal como un sensor de huella dactilar o un sensor óptico, como resultado de la adquisición de datos biométricos o según el resultado del procesamiento de los datos biométricos en bruto que se entregan por tal sensor biométrico. Por ejemplo el procesamiento realizado por el testigo de seguridad usando los datos biométricos en bruto puede abarcar redondeo y/o una proyección de los datos biométricos en bruto sobre un cuerpo finito predefinido.

El término ‘cifrado biométrico’ como se usa en la presente memoria abarca cualquier método de cifrado que usa datos biométricos o datos que se derivan de datos biométricos como información de entrada para un algoritmo de cifrado dado. Por ejemplo, los datos biométricos se pueden usar como una clave para realizar el cifrado del secreto o una clave se deriva de los datos biométricos que entonces se usan por el algoritmo de cifrado para cifrar el secreto.

De acuerdo con las realizaciones de la invención los datos biométricos son datos de huella dactilar, datos de exploración del iris, datos de voz o datos biométricos faciales. Los datos biométricos se pueden adquirir por medio de un sensor externo, tal como un sensor de huella dactilar o una cámara, que se acopla directa o indirectamente al testigo de seguridad o por un sensor que se integra en el testigo de seguridad.

El secreto a ser asignado al testigo de seguridad se puede generar por el testigo de seguridad en sí mismo, tal como por medio de un generador de números aleatorios o se puede seleccionar externamente, tal como por un usuario e introducir en el testigo de seguridad a través de una interfaz de comunicación del testigo de seguridad.

Las realizaciones de la presente invención son particularmente ventajosas ya que el secreto no cifrado no se almacena permanentemente en el testigo de seguridad o en otro lugar. Después del cifrado se borra el secreto no cifrado así como los primeros datos biométricos que se usaron para realizar la operación de cifrado biométrico. Como resultado solamente se almacena el secreto cifrado biométricamente en la memoria no volátil del testigo de seguridad. La única forma de descifrar el secreto es adquirir los datos biométricos del mismo rasgo biométrico de la misma persona que se usó para el cifrado proporcionando un mayor grado de seguridad respecto a la protección del secreto.

De acuerdo con una realización de la invención, el testigo de seguridad tiene almacenamiento volátil, tal como la memoria de acceso aleatorio de su procesador y memoria no volátil. Los primeros datos biométricos y el secreto se almacenan temporalmente en el almacenamiento volátil y el secreto cifrado se almacena en el almacenamiento no volátil. Suponiendo que el testigo de seguridad no tiene una fuente de alimentación integrada como es típicamente el caso para tarjetas inteligentes, quitar el testigo de seguridad de algún dispositivo externo que proporciona la fuente de alimentación, tal como un lector de tarjeta con chip, borra automáticamente los datos biométricos y el secreto no cifrado almacenado en los medios de almacenamiento volátil.

De acuerdo con una realización de la invención los primeros datos biométricos y/o el secreto se borran de manera segura de la memoria volátil mientras que la fuente de alimentación aún está disponible. Esto se puede implementar mediante la ejecución de un módulo de programa que ejecuta una rutina respectiva para borrar de manera segura los primeros datos biométricos y/o el secreto de una RAM del testigo de seguridad.

De acuerdo con una realización de la invención el cifrado biométrico del secreto comprende codificación con corrección del secreto no cifrado.

El término ‘codificación con corrección de errores’ como se entiende en la presente memoria abarca cualquier codificación del secreto que permite detección y corrección de errores, en particular añadiendo datos redundantes al secreto, tal como corrección de errores sin canal de retorno (FEC) usando códigos de convolución o de bloques.

Se realiza una operación XOR sobre el secreto codificado con corrección de errores y los primeros datos biométricos para proporcionar el secreto cifrado biométricamente. El secreto cifrado biométricamente se almacena en la memoria no volátil del testigo de seguridad para uso posterior en una operación criptográfica, tal como con los propósitos de autenticación de un usuario o realizar otra operación criptográfica, en particular una operación de codificación o decodificación o la generación de una firma digital.

Para descifrar el secreto cifrado biométricamente se adquieren unos segundos datos biométricos del mismo rasgo biométrico de la misma persona a partir de la cual se adquirieron los primeros datos biométricos. Los segundos datos biométricos típicamente no son idénticos a los primeros datos biométricos debido a imprecisiones del proceso de adquisición de los datos biométricos, tal como debido a imprecisiones del sensor biométrico que se usa para la adquisición, imprecisiones con respecto a la colocación del rasgo biométrico respecto al sensor y/o errores de redondeo del algoritmo que se usa para transformar los datos biométricos en bruto entregados por el sensor biométrico en los datos biométricos. Debido a la codificación con corrección de errores del secreto el secreto correcto se puede recuperar a partir del secreto cifrado biométricamente incluso si los segundos datos biométricos no son exactamente los mismos que los primeros datos biométricos. Si los segundos datos biométricos no son idénticos a los primeros datos biométricos como es el caso típicamente, el resultado de la operación XOR realizada sobre el secreto cifrado biométricamente y los segundos datos biométricos proporciona una palabra de código que contiene errores. Mediante decodificación con corrección de errores de la palabra de código aún se recupera el secreto correcto.

De acuerdo con una realización de la invención se usa un polinomio p para codificar biométricamente el secreto, tal como

$$p(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + ... + b_{k-1}x^{k-1}$$

Para cifrar un secreto que tiene un número k de dígitos se usa el polinomio p que tiene grado k – 1 a medida que los coeficientes del polinomio p se determinan por los dígitos del secreto a ser codificado, es decir, el secreto que es (b_0, b_1, ..., b_{k-1}).

Los primeros datos biométricos se interpreta que son las coordenadas x de puntos que se sitúan en el polinomio p que se determina por el secreto, tales como los primeros datos biométricos A = (x_1, x_2, …, x_t), donde t es el número de valores contenidos en el conjunto de rasgos A que constituyen los primeros datos biométricos. Preferiblemente t es mayor que k para añadir redundancia.

Usando las coordenadas x proporcionadas por el conjunto de rasgos A se calcula el número de puntos t que se sitúan en el polinomio p. Estos puntos en el polinomio p que se determinan por las coordenadas x dadas por el

conjunto de rasgos A se conocen como ‘puntos reales’ a continuación, es decir, $P_1 = (x_1, p(x_1))$, $P_2 = (x_2, p(x_2))$, …, $P_t = (x_t, p(x_t))$.

El número de puntos seleccionados aleatoriamente que no se sitúan en el polinomio p se combina con los puntos reales. Estos puntos seleccionados aleatoriamente que no se sitúan en el polinomio p se conocen a continuación como ‘puntos parásitos’. Para obtener un número total de r puntos se añade un número de r – t puntos parásitos al conjunto de puntos reales. La unión del conjunto, que es la unión del conjunto de puntos reales y el conjunto de puntos parásitos, constituye el secreto cifrado biométricamente en donde no se almacena información de si un punto dado es un punto real o un punto parásito a fin de ‘disfrazar’ la presencia de los puntos reales dentro de la unión del conjunto. Por lo tanto, los puntos reales no se pueden identificar en la unión del conjunto de los r puntos por un ataque de terceras partes. Los r puntos se almacenan en memoria no volátil del testigo de seguridad para uso posterior.

De acuerdo con una realización de la invención la unión del conjunto se proporciona en forma de una lista no ordenada que contiene datos que son indicativos de los puntos reales y los puntos parásitos tal como en orden aleatorio.

Para descripción del secreto cifrado biométricamente que se representa por la unión del conjunto, se adquieren los segundos datos biométricos. Los segundos datos biométricos se usan para identificar al menos un subconjunto de los puntos reales dentro de la unión del conjunto. Por ejemplo, si una coordenada x dada por un valor del conjunto de rasgos A’ de los segundos datos biométricos coincide con una coordenada x de uno de los r puntos de la unión del conjunto ese punto se considera que es un punto real. Es importante señalar que no todos los puntos reales contenidos en el conjunto de r puntos necesitan ser identificados de esta forma debido a la redundancia que se ha añadido en la operación de codificación. Por lo tanto, los segundos datos biométricos no necesitan ser exactamente idénticos a los primeros datos biométricos para obtener un secreto decodificado correctamente.

A partir de los t valores contenidos en el conjunto de rasgos A’ solamente necesitan coincidir k valores con una de las coordenadas x de los r puntos para identificación de k puntos reales. Ya que los k puntos reales determinan inequívocamente el polinomio p, los coeficientes b_0, b_1, ..., b_{k-1} del polinomio p se pueden obtener mediante cálculo, tal como mediante la resolución de un sistema de ecuaciones dado por los puntos reales identificados. Usando decodificación Reed Solomon el polinomio p correcto se puede recuperar incluso si algunos puntos parásitos además de los puntos reales se seleccionan erróneamente a partir del conjunto de r puntos usando las coordenadas x proporcionadas por el conjunto de rasgos A’.

De acuerdo con una realización de la invención se genera un valor de comprobación aleatoria del secreto no cifrado por el testigo de seguridad y se saca para uso como una denominada pseudo identidad (PI) por la persona. La PI se puede usar para propósitos de autenticación con relación al testigo de seguridad.

De acuerdo con una realización de la invención el secreto cifrado se puede almacenar en una plantilla.

Las realizaciones de la invención son particularmente ventajosas ya que el secreto cifrado se puede generar por el testigo de seguridad en sí mismo, tal como mediante la denominada generación en tarjeta, sin necesidad de introducir el secreto. Por ejemplo, el secreto se proporciona por un generador de números aleatorios del testigo de seguridad. Esto tiene la ventaja de que no necesita ocurrir ningún almacenamiento externo del secreto ni transmisión del secreto desde una entidad externa, tal como un ordenador personal o un lector de tarjeta con chip, al testigo de seguridad que implicaría el riesgo de espionaje en la transmisión del secreto. Además, las realizaciones de la invención son ventajosas ya que el ordenador personal o un lector de tarjeta con chip no necesita ser una entidad de confianza lo cual es debido al hecho de que no necesitan ser comunicados datos críticos desde el testigo de seguridad a tal entidad externa. Además, no se generarán incluso temporalmente datos críticos fuera del testigo (por ejemplo, en el lector de tarjeta, terminal o PC).

Alternativamente, el secreto cifrado biométricamente se puede generar por un sistema de ordenador externo que usa los primeros datos biométricos. El secreto cifrado biométricamente se almacena en el testigo de seguridad tal como usando una técnica de personalización. Como alternativa adicional el secreto cifrado biométricamente se saca por el testigo de seguridad a través de una interfaz externa, tal como para uso de una contraseña de un solo uso o como una clave criptográfica.

Las realizaciones de la invención son particularmente ventajosas debido a que el secreto cifrado no necesita ser sacado por el testigo de seguridad para realizar una operación criptográfica tal como con el propósito de verificación/autenticación, descifrado, cifrado o la generación de una firma digital. Tanto el descifrado del secreto como la realización de la operación criptográfica se pueden realizar por el testigo de seguridad por sí mismo de manera que no necesitan ser sacados del testigo de seguridad datos sensibles para la realización de tal operación; cualquier dato crítico que está disponible temporalmente debido a la realización de la operación criptográfica, tal como el secreto descifrado, los datos biométricos, la selección de puntos reales, el valor de comprobación aleatoria que constituye la pseudo identidad o similares se pueden borrar después de que se ha completado la realización de la operación criptográfica. Tal borrado puede ocurrir automáticamente si el testigo de seguridad no tiene ninguna fuente de alimentación integrada, es decir, no tiene batería y si los datos críticos excepto el secreto cifrado se

almacenan en memoria volátil de manera que los datos críticos se borran automáticamente cuando el testigo de seguridad se retira de algún dispositivo externo que proporciona la fuente de alimentación. De acuerdo con una realización de la invención los primeros datos biométricos y/o el secreto se borran de manera segura de la memoria volátil mientras que aún está disponible la fuente de alimentación. Esto se puede implementar mediante la ejecución de un módulo de programa que ejecuta una rutina respectiva para borrar de manera segura los primeros datos biométricos y/o el secreto de una RAM del testigo de seguridad.

Breve descripción de los dibujos

A continuación las realizaciones preferidas de la invención se describirán en mayor detalle a modo de ejemplo solamente haciendo referencia a los dibujos en los que:

La figura 1 muestra un diagrama de bloques de una realización de un testigo de seguridad que es ilustrativo de cifrado de un secreto,

La figura 2 es un diagrama de bloques de la realización del testigo de seguridad de la fig. 1, que es ilustrativo de descifrado del secreto,

La figura 3 es un diagrama de flujo que es ilustrativo de una realización de un método de la invención de asignación de un secreto a un testigo de seguridad,

La figura 4 es un diagrama de flujo que es ilustrativo de una realización de un método de la invención de operación de un testigo de seguridad para realizar una operación criptográfica usando el secreto cifrado que se ha asignado al testigo de seguridad mediante la realización del método de la fig. 3,

La figura 5 es un diagrama de bloques de una realización de un testigo de seguridad de la invención que es ilustrativo de cifrado del secreto,

La figura 6 es un diagrama de flujo que es ilustrativo de una realización de un método de la invención de operación de un testigo de seguridad para realizar una operación criptográfica usando el secreto cifrado que se ha asignado al testigo de seguridad mediante la realización del método de la fig. 5,

La figura 7 es un diagrama de flujo de un método de asignación del secreto a un testigo de seguridad de acuerdo con una realización de la invención,

La figura 8 es un diagrama de flujo que es ilustrativo de una realización de un método de la invención de operación de un testigo de seguridad para realizar una operación criptográfica usando el secreto cifrado que se ha asignado al testigo de seguridad mediante la realización del método de la fig. 7.

Descripción detallada

En la siguiente descripción detallada elementos iguales de las diversas realizaciones se designan por números de referencia idénticos.

La fig. 1 muestra un testigo de seguridad 100, tal como una tarjeta inteligente. El testigo de seguridad 100 tiene un generador de números aleatorios (RNG) 102 integrado que puede generar un número aleatorio que constituye el secreto a ser asignado al testigo de seguridad. El generador de números aleatorios 102 se puede implementar como un pseudo generador de números aleatorios o como un generador de números aleatorios físico verdadero, por ejemplo mediante una fuente de ruido o una fuente simétrica binaria. En particular, el generador de números aleatorios 102 se puede implementar mediante software y/o mediante hardware, tal como por medio de un registro de desplazamiento con realimentación y/o un módulo de programa que se ejecuta por un procesador del testigo de seguridad 100.

El testigo de seguridad 100 tiene un módulo 104 para codificación con corrección de errores (ECC). El secreto proporcionado por el generador de números aleatorios 102 se introduce en el módulo 104 para codificación con corrección de errores del secreto. El módulo 104 se puede implementar por circuitería lógica dedicada o por un módulo de programa que se ejecuta por el procesador del testigo de seguridad 100.

Alternativamente, algunas de las funcionalidades del módulo 104 se implementan por un módulo de programa y otras funcionalidades del módulo 104 se implementan por circuitería lógica dedicada, tal como por circuitería lógica de un coprocesador criptográfico 116. Por ejemplo, el coprocesador criptográfico 116 puede incluir circuitería lógica para proporcionar funciones de desplazamiento, funciones aritméticas de polinomio tales como para decodificación Reed-Solomon. Tales funciones pueden ser llamadas por el módulo de programa de manera que se puede reducir el número de cálculos que consumen tiempo que necesitan ser implementados en software.

El testigo de seguridad 100 tiene un componente lógico 106 para recibir el secreto codificado con corrección de errores desde el módulo 104 y de los primeros datos biométricos 108 a través de una interfaz de comunicación 111. De acuerdo con una realización de la invención, el componente lógico 106 se puede implementar por medio del coprocesador criptográfico 116.

En una implementación los datos biométricos 108 se adquieren por un sensor externo, tal como un sensor biométrico que está acoplado a un ordenador personal o a un dispositivo de lectura externo para el testigo de seguridad 100. Los datos biométricos en bruto adquiridos externamente se procesan previamente tal como por el ordenador personal o el dispositivo de lectura, por ejemplo, redondeando los datos biométricos en bruto y/o realizando otra transformación de los datos biométricos en bruto, tal como proyectando los datos biométricos en bruto. Los datos biométricos resultantes 108 entonces se transmiten al testigo de seguridad 100 y se reciben por el testigo de seguridad 100 por medio de su interfaz de comunicación 111. La interfaz de comunicación 111 del testigo de seguridad 100 se puede adaptar para comunicación con contacto o sin contacto. Por ejemplo, la interfaz de comunicación 111 del testigo de seguridad 100 es una interfaz de tarjeta con chip con contacto o sin contacto, una interfaz RFID o similares.

En otra implementación el testigo de seguridad 100 tiene un sensor biométrico integrado de manera que la adquisición de los datos biométricos en bruto y cualquier procesamiento previo de los datos biométricos en bruto para proporcionar los datos biométricos 108 se realizan por el testigo de seguridad 100 por sí mismo.

El componente lógico 106 realiza una operación XOR sobre el secreto codificado con corrección de errores recibido desde el módulo 104 y sobre los datos biométricos 108 que proporciona la plantilla 110 que contiene el secreto cifrado resultante. La plantilla 110 se almacena en la memoria no volátil 112 del testigo de seguridad 100.

El componente lógico 106 se puede implementar por circuitería lógica dedicada o por un módulo de programa que se ejecuta por el procesador del testigo de seguridad 100.

El testigo de seguridad 100 puede comprender un componente lógico 114 que recibe el secreto no cifrado desde el generador de números aleatorios 102. El componente lógico 114 se aplica a una función de comprobación aleatoria dada sobre el secreto y saca un valor de comprobación aleatoria del secreto que se puede usar como una PI. La PI se puede sacar a través de la interfaz de comunicación 111 del testigo de seguridad 100 para almacenamiento externo. Como alternativa o además, la PI se almacena en memoria no volátil del testigo de seguridad 100 para referencia posterior.

El componente lógico 114 se puede implementar mediante circuitería lógica dedicada o mediante un módulo de programa que se ejecuta por el procesador del testigo de seguridad 100.

Se tiene que señalar que el generador de números aleatorios 102, el módulo 104, el componente lógico 106 y el componente lógico 114 se pueden proporcionar por un único procesador del testigo de seguridad 100 que ejecuta las instrucciones de programa respectivas. El testigo de seguridad 100 puede comprender un procesador adicional, es decir, el coprocesador criptográfico 116, que implementa algunas o todas de estas funcionalidades criptográficas, especialmente la codificación con corrección de errores y/o la transformación de los datos biométricos en bruto en los datos biométricos 108.

El secreto proporcionado por el generador de números aleatorios 102, el secreto codificado con corrección de errores proporcionado por el módulo 104, los datos biométricos 108 y los datos biométricos en bruto, si son aplicables, así como la PI se almacenan solamente temporalmente en el testigo de seguridad 100 tal como en una memoria de acceso aleatorio del procesador o el coprocesador criptográfico 116 del testigo de seguridad 100. Después de que la plantilla 110 se ha almacenado en la memoria no volátil 112 y después de que se ha sacado la PI, si es aplicable, estos valores de datos críticos se borran de la memoria de acceso aleatorio. No obstante, para algunas aplicaciones se prefiere almacenar la PI en memoria no volátil en lugar de borrarla.

La fig. 2 muestra el testigo de seguridad 100 que ilustra el descifrado del secreto cifrado contenido en la plantilla 110. El testigo de seguridad 100 tiene un módulo 118 para decodificación con corrección de errores de la codificación con corrección de errores realizada por el módulo 104 mostrado en la Fig. 1. El módulo 118 se puede implementar mediante circuitería lógica dedicada o mediante un módulo de programa que se ejecuta por el procesador o el coprocesador criptográfico 116 del testigo de seguridad 100.

Alternativamente, algunas de las funcionalidades del módulo 118 se implementan mediante un módulo de programa y otras funcionalidades del módulo 118 se implementan mediante circuitería lógica dedicada, tal como mediante circuitería lógica de un coprocesador criptográfico 116. Por ejemplo, el coprocesador criptográfico 116 puede incluir circuitería lógica para proporcionar funciones de desplazamiento, funciones aritméticas de polinomio tales como para decodificación Reed-Solomon. Tales funciones pueden ser llamadas por el módulo de programa de manera que se puede reducir el número de cálculos que consumen tiempo que necesitan ser implementados en software.

Para descifrado del secreto contenido en la plantilla 110 se realiza adquisición de datos biométricos del rasgo biométrico de la misma persona desde la cual se han obtenido los datos biométricos 108. Debido a imprecisiones del proceso de adquisición los segundos datos biométricos resultantes 108' típicamente no son exactamente idénticos a los datos biométricos originales 108. Para realizar la operación de descifrado los datos biométricos 108' y el secreto cifrado contenido en la plantilla 110 se someten a una operación XOR por el componente lógico 106 y la palabra de código resultante entonces se decodifica con corrección de errores por el módulo 118 que proporciona el secreto correcto. El secreto que se recupera de esta manera se puede usar entonces por el testigo de seguridad 100, tal

como por el coprocesador criptográfico 116, para realizar una operación criptográfica tal como con los propósitos de autenticación, descifrado, cifrado o generación de una firma digital, usando el secreto como una clave criptográfica.

Por ejemplo, la persona de la que se ha obtenido el rasgo biométrico necesita introducir su PI en el testigo de seguridad 100. El testigo de seguridad 100 compara la PI recibida a través de su interfaz de comunicación 111 con la PI entregada por el componente lógico 114, es decir, el valor de comprobación aleatoria del secreto. Si la PI recibida y la PI proporcionada por el componente lógico 114 son idénticas, la autenticación de la persona tiene éxito de manera que se habilita la funcionalidad del testigo de seguridad 100. Por ejemplo, después de la autenticación con éxito de la persona se permite la generación de una firma digital por el testigo de seguridad 100.

La fig. 3 es un diagrama de flujo que ilustra una realización de asignación de un secreto a un testigo de seguridad.

En el paso 200 los primeros datos biométricos A se reciben por el testigo de seguridad o bien a través de una interfaz de comunicación externa (véase la interfaz de comunicación 111 de las fig. 1 y 2) o internamente desde un sensor biométrico integrado del testigo de seguridad. En el paso 202 se define un secreto B. Por ejemplo, la persona de la cual se han adquirido los datos biométricos A puede seleccionar el secreto B e introducir el secreto B a través de la interfaz de comunicación externa en el testigo de seguridad. Alternativamente, el secreto B se puede determinar con ocasión de una personalización del testigo de seguridad e introducir en el testigo de seguridad a través de la interfaz de comunicación externa. Por lo tanto, el secreto B se puede determinar fuera del testigo de seguridad. Alternativamente, el secreto B se determina por el testigo de seguridad por sí mismo, tal como generando un número aleatorio que usa su generador de números aleatorios interno (véase el generador de números aleatorios 102 de la fig. 1).

En el paso 204 se realiza una codificación con corrección de errores sobre el secreto B para proporcionar el secreto codificado b. En el paso 206 se realiza una operación XOR sobre el secreto codificado con corrección de errores b y los datos biométricos A, tal como realizando la operación XOR en modo bit que proporciona la plantilla protegida T. En el paso 208 T se almacena en la memoria no volátil del testigo de seguridad y en el paso 210 los datos biométricos A y el secreto B se borran del testigo de seguridad de manera que solamente la plantilla T permanece dentro del testigo de seguridad como resultado de la realización de la asignación del secreto al testigo de seguridad. Es importante señalar que el secreto B no se almacena de cualquier forma en el testigo de seguridad sino que solamente la plantilla T desde la cual el secreto B no se puede recuperar a menos que se adquieran de la persona los datos biométricos. Por lo tanto, el secreto B se asigna al testigo de seguridad sin almacenar el secreto B dentro del testigo de seguridad o en otro lugar.

De acuerdo con una realización de la invención, se genera un valor de comprobación aleatoria del secreto B y se saca por el testigo de seguridad, tal como a través de su interfaz 111, en el paso 202. El valor de comprobación aleatoria se almacena en la memoria no volátil del testigo de seguridad.

La fig. 4 ilustra la operación para recuperar el secreto B a partir de la plantilla T. En el paso 300 los segundos datos biométricos A' se reciben como resultado de adquisición de datos biométricos del rasgo biométrico de la persona desde la cual se han adquirido los datos biométricos A originales. En el paso 302 se realiza una operación XOR sobre la plantilla T y los datos biométricos A' que proporcionan la palabra de código codificada con corrección de errores b' que puede contener errores si A' no es idéntica a A. En el paso 304 b' se corrige usando decodificación con corrección de errores que proporciona el secreto B correcto. En el paso 306 B entonces se puede usar para realizar una operación criptográfica. A', b' y B se borran en el paso 308.

De acuerdo con una realización de la invención, el valor de comprobación aleatoria del secreto B se introduce en el testigo de seguridad, tal como a través de su interfaz 111, en el paso 300 además de los datos biométricos A'. El valor de comprobación aleatoria recibido se compara con el valor de comprobación aleatoria almacenado en la memoria no volátil del testigo de seguridad. Solamente si son coincidentes el valor de comprobación aleatoria recibido y el valor de comprobación aleatoria almacenado se ejecutan los siguientes pasos 302 a 308 y un resultado del uso de B se devuelve por el testigo de seguridad a través de su interfaz. De otro modo no se devuelve ningún resultado.

La fig. 5 muestra un diagrama de bloques de una realización alternativa del testigo de seguridad 100. A diferencia de las realizaciones de las fig. 1 y 2 se usa un polinomio p para la codificación. El generador de números aleatorios 102 entrega un número aleatorio, es decir, el secreto B, que tiene un número de k dígitos b_0, b_1, …, b_{k-1}. Alternativamente el secreto se puede recibir a través de la interfaz de comunicación 111. El testigo de seguridad 100 tiene un codificador de polinomio 120 que usa los k dígitos del secreto B para determinar los coeficientes del polinomio p, es decir,

$$p(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + ... + b_{k-1}x^{k-1}$$

El testigo de seguridad además comprende un módulo de cálculo 122 que sirve para el cálculo de los puntos reales que se sitúan en el polinomio p. Los puntos reales se calculan por el módulo de cálculo 122 usando los datos biométricos 108 que comprenden t valores. El polinomio se evalúa en cada uno de los t valores *para proporcionar los puntos reales* P_i, *donde* $0 < i \leq t$. Esto proporciona el conjunto de puntos reales que contiene los puntos $P_1 = (x_1, p(x_1))$, $P_2 = (x_2, p(x_2))$, …, $P_t = (x_t, p(x_t))$.

Además un número de r – t puntos parásitos seleccionados aleatoriamente se proporcionan por un generador de números aleatorios 124. El conjunto de puntos reales proporcionado por el módulo de cálculo 122 y el conjunto de puntos parásitos proporcionado por el generador de números aleatorios 124 en combinación constituyen la plantilla 110 que contiene un número de r puntos.

Se tiene que señalar que el codificador de polinomio 120, el módulo de cálculo 122, el generador de números aleatorios 124, el módulo de selección de puntos 126 y/o el decodificador de polinomio 128 se pueden implementar mediante circuitería lógica dedicada o mediante un procesador del testigo de seguridad 100, tal como mediante el coprocesador criptográfico 116, que ejecuta los módulos de programa respectivos.

La fig. 6 muestra el testigo de seguridad 100 de la fig. 5 que ilustra la operación de descifrado.

El testigo de seguridad 100 tiene un módulo de selección de puntos 126 para la selección de puntos reales a partir de la plantilla 110 y que proporciona los puntos reales identificados a un decodificador de polinomio 128 del testigo de seguridad 100.

La selección de puntos reales a partir de la plantilla 110 se realiza por el módulo de selección de puntos 126 que usa los datos biométricos 108'. La selección de un punto real se puede realizar usando un valor contenido en los datos biométricos 108' y buscando un punto contenido en la plantilla 110 que tiene una coordenada x coincidente o tiene alto grado de coincidencia. Si se puede identificar tal punto, este punto se considera un punto real. Este proceso de selección se realiza para cada uno de los valores contenidos en los datos biométricos 108' y los puntos reales identificados resultantes se proporcionan al decodificador de polinomio 128 que reconstruye el polinomio b a partir de los puntos reales entregados desde el módulo de selección de puntos 126. Ya que los coeficientes del polinomio p constituyen el secreto B el decodificador de polinomio 128 proporciona de esta manera el secreto B.

El decodificador de polinomio 128 puede implementar decodificación Reed Solomon de manera que incluso si algunos de los puntos reales identificados por el módulo de selección de puntos 126 son de hecho puntos parásitos el polinomio p aún se puede decodificar correctamente.

La fig. 7 ilustra un método respectivo de asignación del secreto B al testigo de seguridad usando codificación de polinomio. En el paso 400 los datos biométricos A que tienen un número de t valores se reciben por el testigo de seguridad. En el paso 402 el secreto B que tiene k dígitos se recibe o determina por el testigo de seguridad determinando de esta manera el polinomio p que tiene el grado k – 1, donde t es mayor que k para añadir redundancia.

En el paso 404 se calcula un punto real que está situado en el polinomio p para cada valor de A y en el paso 406 un número de r – t puntos parásitos que no están situados en el polinomio p se añaden al conjunto de puntos reales proporcionando un total de r puntos que constituyen la plantilla T. La plantilla T se almacena en la memoria no volátil del testigo de seguridad en el paso 408 y los datos biométricos A y el secreto B se borran del testigo de seguridad en el paso 410.

La fig. 8 ilustra la operación inversa: en el paso 500 se reciben los datos biométricos A' (véanse los datos biométricos 108' de la fig. 6). En el paso 502 los puntos reales contenidos en T se identifican usando los valores contenidos en los datos biométricos A'. Esto se realiza mediante la búsqueda en T de la presencia de un punto que tiene una coordenada x coincidente o tiene alto grado de coincidencia con un valor contenido en A'. Como resultado del paso 502 se identifican puntos que son de hecho puntos reales que se sitúan en el polinomio p. Dependiendo de la implementación se pueden identificar erróneamente uno o más puntos parásitos como que son puntos reales en el paso 502; esto puede ocurrir si un punto parásito por casualidad tiene una coordenada x que es coincidente o tiene alto grado de coincidencia con un valor de A'.

En el paso 504 el polinomio p se reconstruye usando los puntos reales que se han identificado en el paso 502. Dependiendo de la implementación la reconstrucción del polinomio p es incluso posible si los puntos identificados en el paso 502 también contienen algunos puntos parásitos, en particular si la reconstrucción del polinomio p se realiza por medio de decodificación Reed Solomon.

En el paso 506 el secreto B se puede usar para realizar una operación criptográfica y en el paso 508 los datos críticos tales como A', B y la información de identificación obtenida en el paso 502 con respecto a los puntos reales se borra en el paso 508 del testigo de seguridad.

Análogo a las realizaciones de las figuras 3 y 4, se puede almacenar en el testigo de seguridad un valor de comprobación aleatoria del secreto B, tal como en el paso 400 y la ejecución de los pasos 502 a 508 puede estar sujeta a recibir el valor de comprobación aleatoria correcto del secreto B, tal como en el paso 500.

Lista de números de referencia

100	Testigo de seguridad
102	Generador de números aleatorios
104	Módulo
106	Componente lógico
108	Datos biométricos
108’	Datos biométricos
110	Plantilla
111	Interfaz de comunicación
112	Memoria no volátil
114	Componente lógico
116	Coprocesador criptográfico
118	Módulo
120	Codificador de polinomio
122	Módulo de cálculo
124	Generador de números aleatorios
126	Módulo de selección de puntos
128	Decodificador de polinomio

REIVINDICACIONES

1. Un método de operación de un testigo de seguridad para realizar una operación criptográfica, el testigo de seguridad (100) que tiene asignado al mismo un secreto cifrado biométricamente, el método de operación del testigo de seguridad que comprende:

- recibir unos segundos datos biométricos (108') del rasgo biométrico de la persona y una pseudo identidad (PI) mediante el testigo de seguridad,

- almacenar los segundos datos biométricos (108') en el testigo de seguridad,

- leer el secreto cifrado biométricamente desde una memoria (112) del testigo de seguridad (100),

- descifrar biométricamente el secreto usando los segundos datos biométricos (108') mediante el testigo de seguridad (100),

- comparar la pseudo identidad (PI) con un valor de comprobación aleatoria (114) del secreto no cifrado,

- usar el secreto para realizar la operación criptográfica en caso de que la pseudo identidad (PI) sea idéntica con el valor de comprobación aleatoria (114) del secreto no cifrado,

- borrar el secreto descifrado y los segundos datos biométricos (108').

2. El método de la reivindicación 1, en donde el secreto se usa como una clave para realizar la operación criptográfica.

3. El método de la reivindicación 1 o 2, en donde descifrar biométricamente el secreto se realiza realizando una operación XOR (106) sobre el secreto cifrado y los segundos datos biométricos (108') que proporciona un secreto incorrecto, corregir errores (118) del secreto incorrecto usando el código de corrección de errores que proporciona el secreto corregido y que además comprende borrar el secreto incorrecto.

4. El método de la reivindicación 1 o 2, el testigo de seguridad (100) que tiene asignado al mismo un secreto de acuerdo a:

- recibir unos primeros datos biométricos (108) de un rasgo biométrico de una persona mediante el testigo de seguridad,

- almacenar los primeros datos biométricos (108) en el testigo de seguridad (100),

- almacenar el secreto no cifrado en el testigo de seguridad (100),

- cifrar biométricamente el secreto usando los primeros datos biométricos (108) mediante el testigo de seguridad (100),

- almacenar el secreto cifrado en el testigo de seguridad (100),

- borrar el secreto no cifrado y los primeros datos biométricos (108) del testigo de seguridad (100),

- generar (114) un valor de comprobación aleatoria (114) del secreto no cifrado mediante el testigo de seguridad (100) y sacar el valor de comprobación aleatoria.

5. El método de la reivindicación 4, en donde los primeros datos biométricos (108) y/o el secreto se almacenan en una memoria volátil (116) del testigo de seguridad (100).

6. El método de la reivindicación 4 o 5, en donde el secreto se genera mediante el testigo de seguridad (100).

7. El método de las reivindicaciones 4, 5 o 6, el testigo de seguridad (100) que es una memoria USB, una tarjeta con chip, en particular una tarjeta inteligente, una tarjeta SIM, en particular una tarjeta USIM o un documento de ID.

8. El método de cualquiera de las reivindicaciones precedentes, en donde

el paso de cifrar biométricamente el secreto se realiza mediante codificación con corrección de errores (104) del secreto no cifrado y realizando una operación XOR (106) sobre el secreto codificado con corrección de errores y los primeros datos biométricos (108) para proporcionar el secreto cifrado biométricamente.

9. El método de cualquiera de las reivindicaciones precedentes 4 a 8, en donde los primeros datos biométricos (108) tienen un primer número (t) de valores y el secreto tiene un segundo número (k) de dígitos que determinan los coeficientes de un polinomio (p), en donde el primer número es mayor que el segundo número, en donde el paso de cifrar biométricamente el secreto se realiza calculando un punto real para cada valor de los primeros datos biométricos usando el polinomio y proporcionando puntos parásitos aleatorios que no están situados en el polinomio,

en donde un conjunto de unión del conjunto de puntos reales y el conjunto de puntos parásitos aleatorios proporciona el secreto cifrado biométricamente y que además comprende borrar los puntos reales y los puntos parásitos aleatorios del testigo de seguridad (100).

10. El método de la reivindicación 9, en donde descifrar biométricamente el secreto se realiza identificando (126) al menos un subconjunto de los puntos reales contenidos en el secreto cifrado usando los segundos datos biométricos (108'), determinando el polinomio que usa los puntos reales que proporciona el secreto y que además comprende borrar la información de identificación que es indicativa de los puntos reales identificados del testigo de seguridad (100).

11. Un medio de almacenamiento legible por un procesador de un testigo de seguridad (100), el medio de almacenamiento que contiene instrucciones que cuando se ejecutan por el procesador del testigo de seguridad (100) hacen al testigo de seguridad (100) realizar un método según cualquiera de las reivindicaciones precedentes 1 a 10.

12. Un testigo de seguridad (100) para realizar un método según cualquiera de las reivindicaciones 1 a 10 que comprende:

- medios (111) para adquirir datos biométricos (108; 108'),

- medios de almacenamiento volátil (116) para almacenar temporalmente los datos biométricos y un secreto no cifrado,

- medios para cifrar biométricamente (104, 106; 120, 122) el secreto cifrado que usa datos biométricos adquiridos por los medios para adquirir datos biométricos,

- medios de almacenamiento no volátiles (112) para almacenar el secreto cifrado biométricamente,

- medios para generar (114) un valor de comprobación aleatoria del secreto no cifrado mediante el testigo de seguridad y sacar el valor de comprobación aleatoria,

- medios (116) para leer el secreto cifrado de los medios de almacenamiento no volátiles,

- medios para descifrar biométricamente (106, 118; 126, 128) el secreto cifrado usando los datos biométricos que usan el método de la reivindicación 1.

en donde los datos biométricos (108; 108') se adquieren a partir de un rasgo biométrico de una persona.

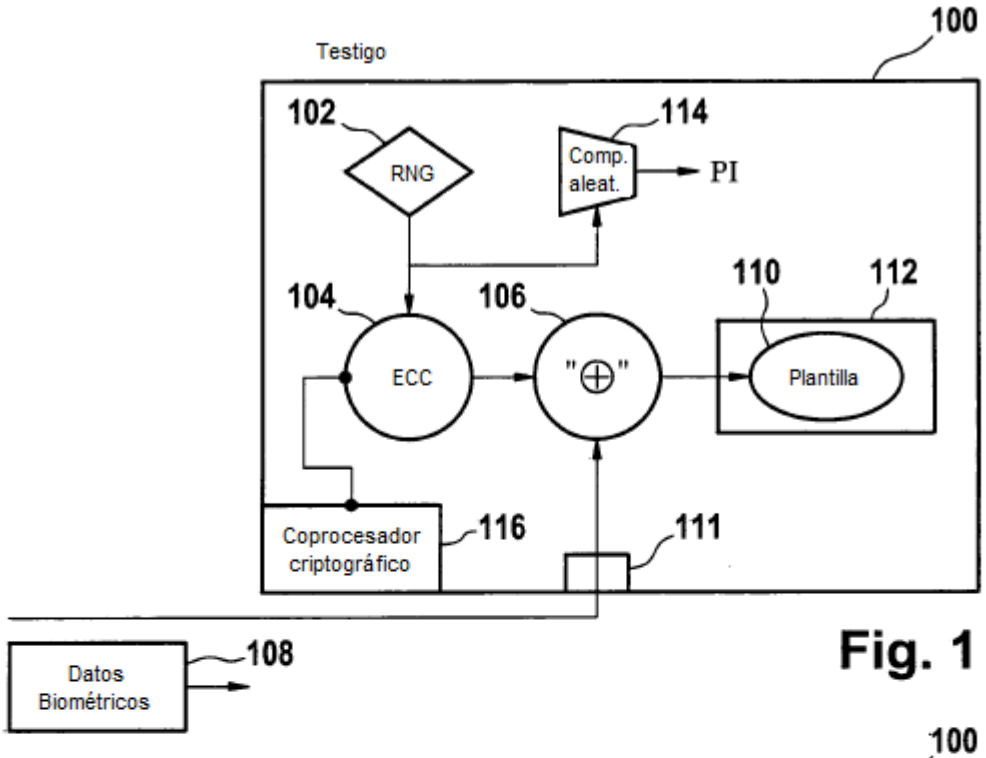
Testigo
100
102
RNG
114
Comp. aleat.
PI
104
ECC
106
"⊕"
110
112
Plantilla
Coprocesador criptográfico
116
111
Datos Biométricos
108

Fig. 1

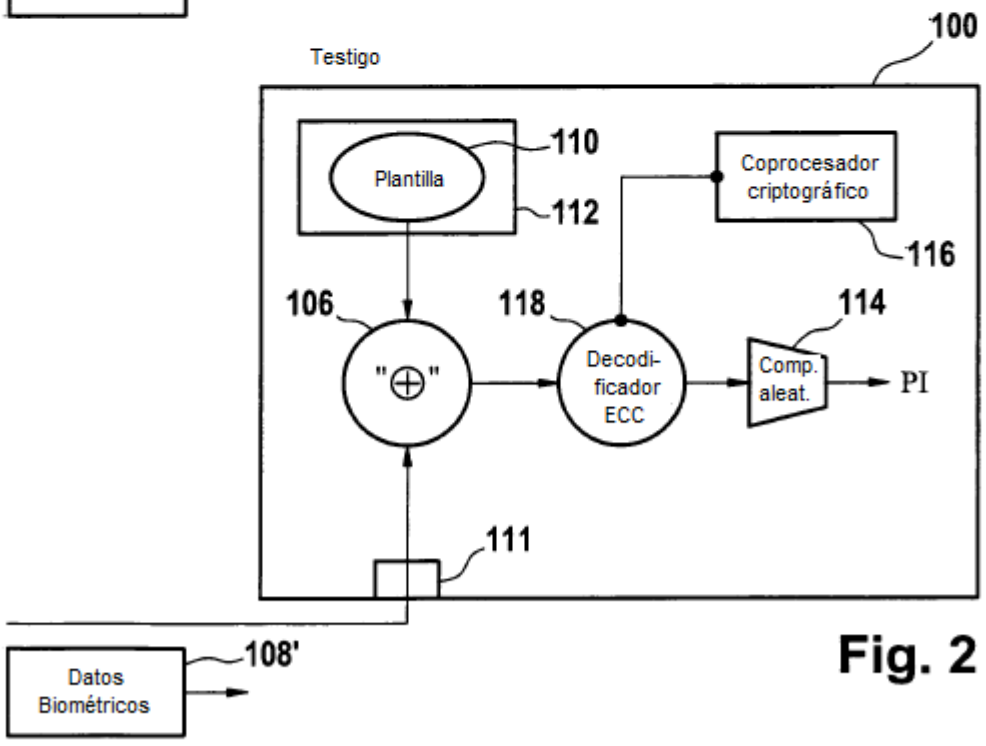
Testigo
100
Plantilla
110
112
Coprocesador criptográfico
116
106
"⊕"
118
Decodi-ficador ECC
114
Comp. aleat.
PI
111
Datos Biométricos
108'

Fig. 2

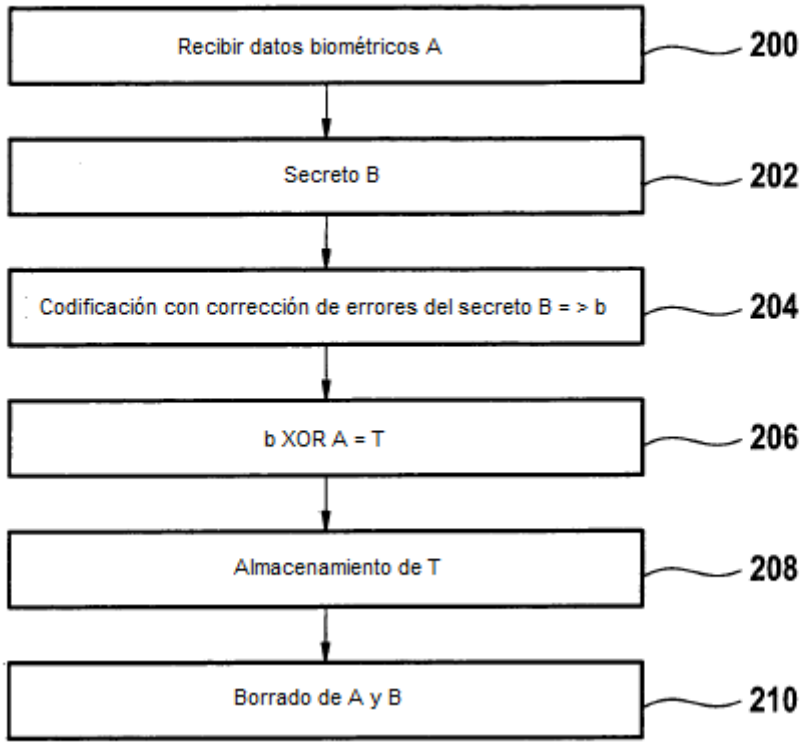
Recibir datos biométricos A
200
Secreto B
202
Codificación con corrección de errores del secreto B = > b
204
b XOR A = T
206
Almacenamiento de T
208
Borrado de A y B
210

Fig. 3

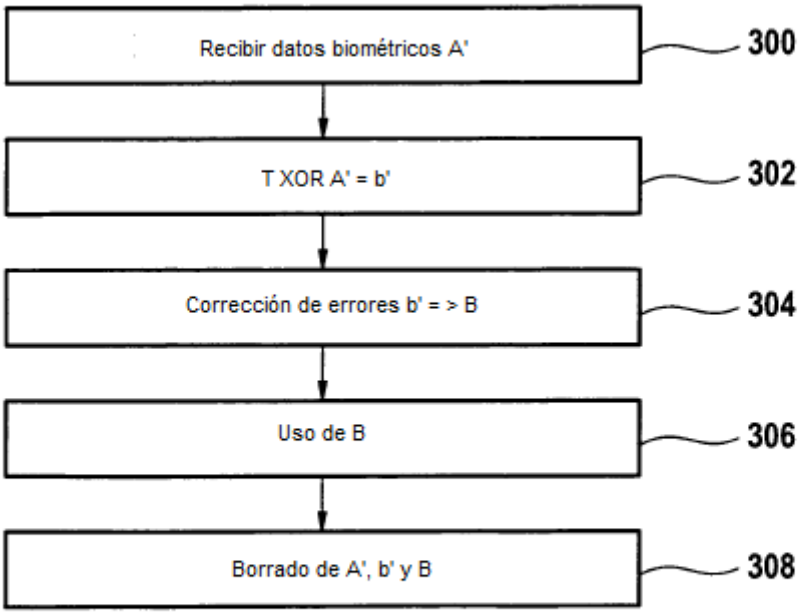
Recibir datos biométricos A'
300
T XOR A' = b'
302
Corrección de errores b' = > B
304
Uso de B
306
Borrado de A', b' y B
308

Fig. 4

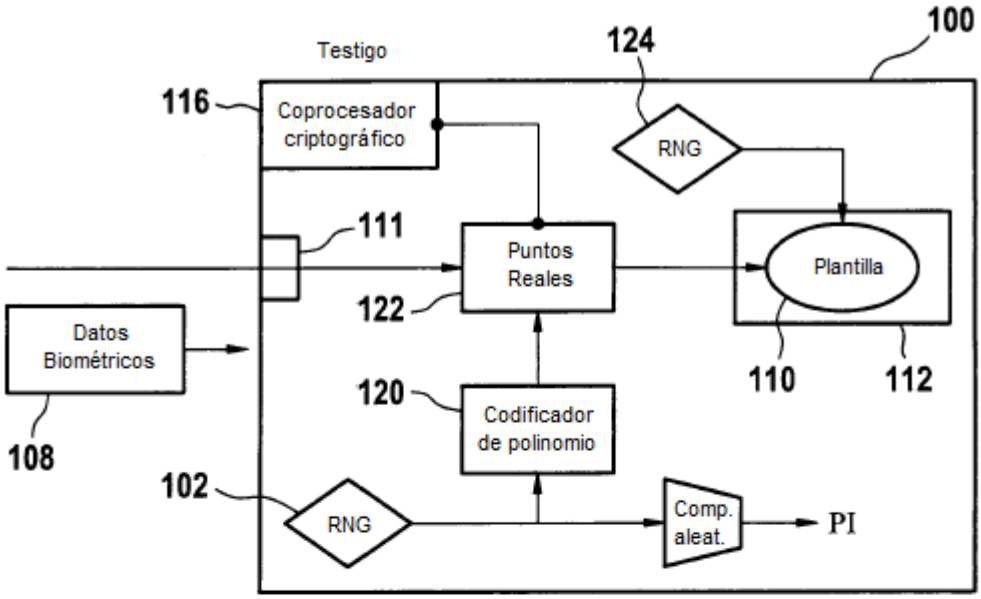
Testigo
100
124
116
Coprocesador criptográfico
RNG
111
Puntos Reales
Plantilla
122
Datos Biométricos
110
112
120
Codificador de polinomio
108
102
RNG
Comp. aleat.
PI

Fig. 5

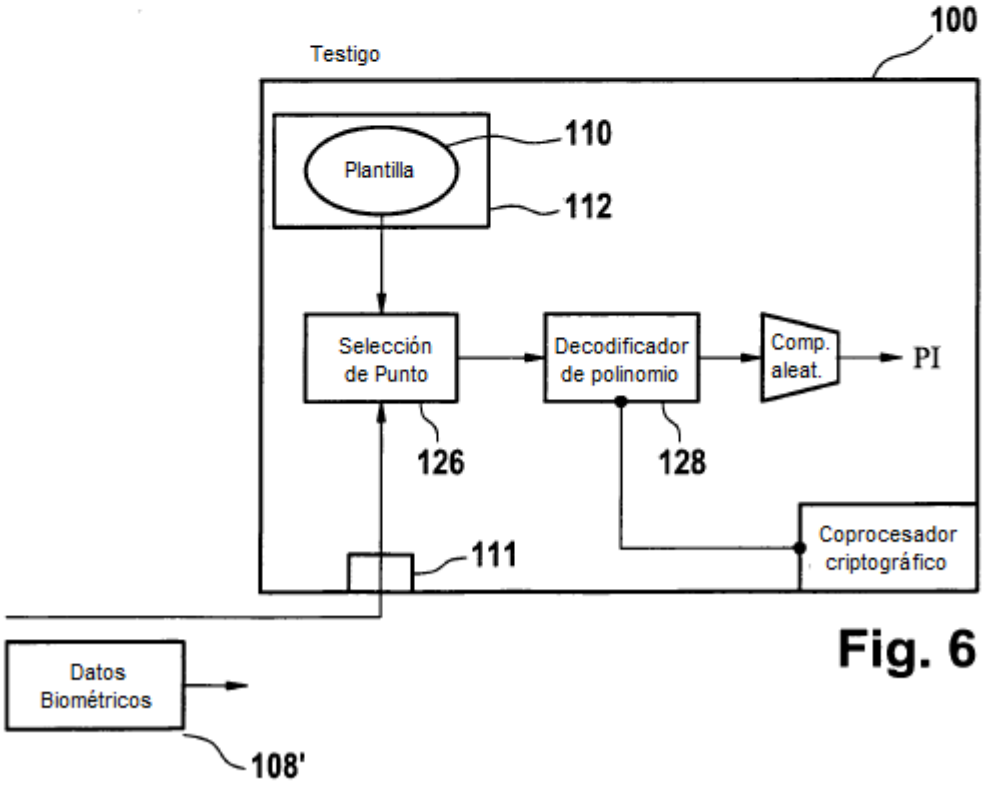
Testigo
100
Plantilla
110
112
Selección de Punto
Decodificador de polinomio
Comp. aleat.
PI
126
128
Coprocesador criptográfico
111
Datos Biométricos
108'

Fig. 6

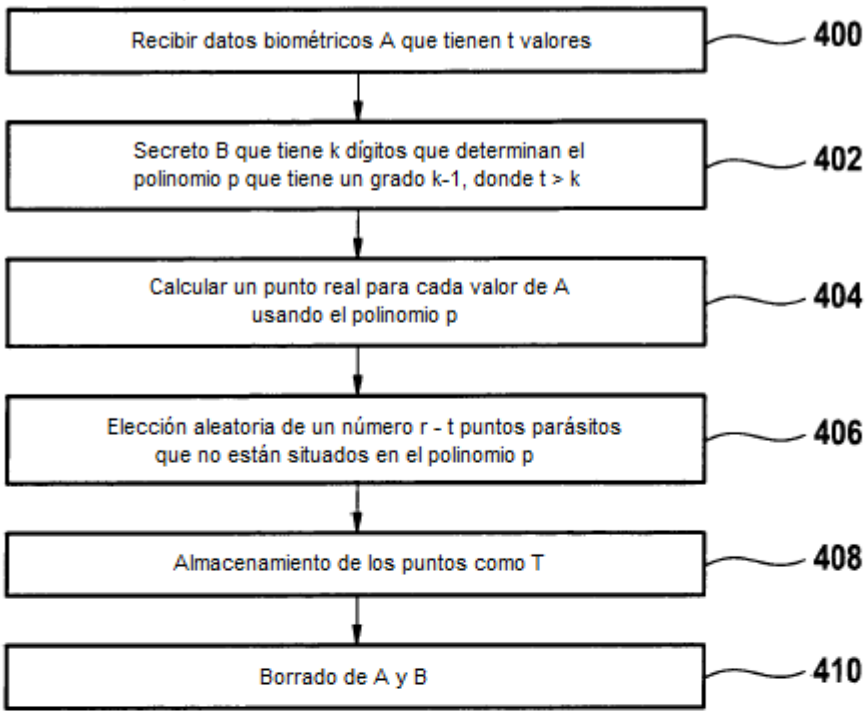
Recibir datos biométricos A que tienen t valores
400
Secreto B que tiene k dígitos que determinan el polinomio p que tiene un grado k-1, donde t > k
402
Calcular un punto real para cada valor de A usando el polinomio p
404
Elección aleatoria de un número r - t puntos parásitos que no están situados en el polinomio p
406
Almacenamiento de los puntos como T
408
Borrado de A y B
410

Fig. 7

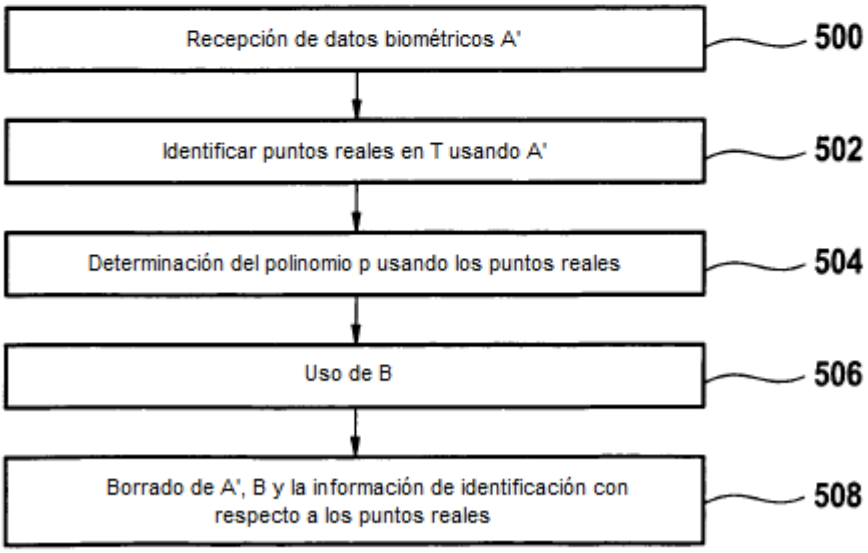
Recepción de datos biométricos A'
500
Identificar puntos reales en T usando A'
502
Determinación del polinomio p usando los puntos reales
504
Uso de B
506
Borrado de A', B y la información de identificación con respecto a los puntos reales
508

Fig. 8