(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 509 345**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.12.2006 E 06832130 (6)**

(97) Fecha y número de publicación de la concesión europea: **30.07.2014 EP 1964305**

(54) Título: **Cálculo de protocolo de descifrado de umbral de seguridad**

(30) Prioridad:

13.12.2005 EP 05112048

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.10.2014

(73) Titular/es:

KONINKLIJKE PHILIPS N.V. (100.0%)
HIGH TECH CAMPUS 5
5656 AE EINDHOVEN, NL

(72) Inventor/es:

TUYLS, PIM T. y
SCHOENMAKERS, BERRY

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Cálculo de protocolo de descifrado de umbral de seguridad

La presente invención se refiere a un procedimiento de conversión de un conjunto de datos cifrados en el cifrado de bits individuales que representan el conjunto de datos. Además, la invención se refiere a un sistema para convertir un conjunto de datos cifrados en un cifrado de bits individuales que representan el conjunto de datos.

En esquemas de cálculo seguro de múltiples partes, un grupo de participantes, también denominados 'jugadores', los cuales no se fían necesariamente unos de otros, desean calcular una función común usando datos privados como entradas de la función, sin revelar los datos privados, mientras se garantiza que la salida de la función se calcula correctamente. Por ejemplo, en el ampliamente conocido protocolo del millonario, dos millonarios desean saber quién es el más rico de los dos sin revelar ninguna información sobre su fortuna. Los dos millonarios proporcionan a una función pública datos privados (es decir, la fortuna del millonario respectivo), y la función proporciona una variable que indica cuál de los dos es el más rico, sin revelar nada más acerca de los datos privados.

Las técnicas utilizadas en esquemas de cálculo seguro de múltiples partes son muy adecuadas para llevar a cabo operaciones que conservan la privacidad entre un grupo de jugadores. Estas técnicas pueden implementarse, por ejemplo, en campos técnicos tales como subastas seguras, la comparación segura de perfiles, votaciones electrónicas seguras y la autenticación biométrica segura. Algoritmos eficaces para el cálculo seguro de múltiples partes basados en sistemas de cifrado homomórfico de umbrales se describen en el documento "*Practical Two-Party Computation based on the Conditional Gate*" de B. Schoenmakers y P. Tuyls, Asiacrypt 2004, páginas 119 a 126, LNCS Springer-Verlag 2004.

La autenticación de objetos físicos puede usarse en muchas aplicaciones, tal como el acceso condicional a edificios seguros o el acceso condicional a datos digitales (por ejemplo, almacenados en un ordenador o en medios de almacenamiento extraíbles), o con fines de identificación (por ejemplo, para cobrar a una persona identificada una actividad particular, o incluso para entrar en un país). El uso de la biometría para la identificación y/o la autenticación, en donde se usan características que son únicas para un usuario tales como las huellas dactilares, el iris, los oídos, el rostro, etc., se considera cada vez más una mejor alternativa a los medios de identificación tradicionales, tales como las contraseñas y los códigos PIN, y la identificación "manual" que implica la comparación visual entre una persona y, por ejemplo, una foto.

Un problema que debe resolverse en la técnica anterior es cómo dividir el cifrado de un conjunto de datos en forma de, por ejemplo, una característica biométrica, tal como un número x, donde $x \in \{0, 1,\ldots, n-1\}$, en cifrados individuales de bits $x_0, x_1,\ldots, x_{t-1}$ que forman el número x, donde t es el número de bits del número n-1, sin perder información acerca de x o sus bits $x_0, x_1,\ldots,x_{t-1}$. Las aplicaciones de un algoritmo de este tipo son numerosas, por ejemplo test conjuntos y seguros de primalidad, exponenciación segura, reducción de la carga computacional y de comunicación de un sensor biométrico, reducción de la carga computacional en protocolos de votación, etc. Un protocolo para dividir un número cifrado $[[x]]$ en bits cifrados $[[x_0]], [[x_1]],\ldots [[x_{t-1}]]$ se denomina protocolo de división en bits.

En el documento "*How to Split a Shared Secret into Shared Bits in Constant-Round*", de I. Damgaard et al, Universidad de Aarhus, 23 de junio de 2005, se trata un problema similar. Sin embargo, se utiliza una configuración segura sin condiciones. En esta divulgación, se supone que los jugadores implicados en los cálculos seguros de múltiples partes descritos en ese documento tienen acceso a una parte de un conjunto de datos binarios para la que va a determinarse de manera segura una representación binaria. Como resultado, un jugador adquiere parte de los bits que forman el conjunto de datos binarios y tiene que hacer que los otros jugadores consigan un conjunto de datos binarios completo.

El documento WO 2005/043808 da a conocer un procedimiento para una multiplicación eficaz de múltiples partes.

Un objeto de la presente invención es resolver los problemas mencionados anteriormente y proporcionar un procedimiento/dispositivo para llevar a cabo una división segura en bits; es decir, convertir un número cifrado $[[x]]$ en cifrados de bits $[[x_0]], [[x_1]],\ldots [[x_{t-1}]]$ que forman el número usando propiedades del cifrado homomórfico.

Este objeto se consigue mediante un procedimiento de conversión de un conjunto de datos cifrados en un cifrado de bits individuales que representan el conjunto de datos según la reivindicación 1, y un sistema para convertir un conjunto de datos cifrados en un cifrado de bits individuales que representan el conjunto de datos según la reivindicación 11.

Según un primer aspecto de la presente invención, se proporciona un procedimiento que comprende las etapas de generar un número aleatorio y calcular un cifrado basado en bits del número aleatorio, calcular de manera segura una suma cifrada en función del conjunto de datos cifrados y del número aleatorio cifrado, descifrar la suma cifrada y

determinar una representación binaria de la suma y crear el cifrado de los bits individuales que representan el conjunto de datos cifrados procesando la suma con el número aleatorio cifrado.

Según un segundo aspecto de la presente invención, se proporciona un sistema que comprende al menos un primer y un segundo dispositivo de cálculo dispuestos para generar conjuntamente un número aleatorio y calcular un cifrado basado en bits del número aleatorio. Al menos uno de los dispositivos de cálculo está dispuesto para calcular una suma cifrada en función del conjunto de datos cifrados y del número aleatorio cifrado, y estando dispuestos el primer y el segundo dispositivo de cálculo para descifrar conjuntamente la suma cifrada y determinar una representación binaria de la suma. Además, el primer y el segundo dispositivo de cálculo están dispuestos para crear conjuntamente el cifrado de los bits individuales que representan el conjunto de datos cifrados procesando la suma con el número aleatorio cifrado.

Una idea básica de la presente invención es proporcionar un protocolo en el que sea posible dividir un cifrado de un conjunto de datos en forma de, por ejemplo, una característica biométrica, tal como un número x, donde $x \in \{0, 1,\ldots, n-1\}$, en un cifrado de bits respectivos $x_0, x_1,\ldots,x_{t-1}$ que forman el número x, donde t es el número de bits del número n-1, sin perder información acerca de x o sus bits $x_0, x_1,\ldots,x_{t-1}$. Por tanto, la presente invención permite dividir el cifrado [[x]] en bits cifrados respectivos $[[x_0]], [[x_1]],\ldots [[x_{t-1}]]$ que forman el número cifrado $x=\Sigma_{l=1}^{n} x$; 2'.

Esto es ventajoso ya que permite, por ejemplo en la autenticación biométrica, un único cifrado inicial de una cadena de bits expresada como un número $x=\Sigma\_x_i2^i$. Por tanto, uno/varios servidor(es) de verificación ejecuta(n) un protocolo de división en bits para obtener cifrados de los bits que forman el número. La cadena de bits cifrados puede compararse posteriormente con características biométricas cifradas obtenidas durante un registro, de modo que puede realizarse una comprobación de correspondencia para autenticar a un usuario. La comparación real de datos biométricos cifrados se lleva a cabo normalmente haciendo que un sensor biométrico y un dispositivo de verificación participen en un protocolo de dos partes (o de múltiples partes) en el que dos conjuntos de datos biométricos cifrados se comparan entre sí para comprobar si hay una correspondencia (suficiente) entre los dos conjuntos, usando por ejemplo distancias de Hamming.

Los participantes del protocolo se denominan jugadores. Los jugadores generan conjuntamente un número aleatorio y llevan a cabo un cifrado basado en bits de este número aleatorio. Preferiblemente, los cifrados del número aleatorio van acompañados de pruebas que pueden verificarse públicamente y que están dispuestas para mostrar que el número aleatorio se ha descifrado correctamente. Una suma basada en el número aleatorio cifrado y en el conjunto de datos cifrados se cifra usando un esquema de cifrado homomórfico. El término "homomórfico" implica que [[x + y]] = [[x]][[y]], es decir, el cifrado de (x + y) es igual al cifrado de x multiplicado por el cifrado de y.

Después de haberse calculado la suma cifrada, los jugadores llevan a cabo un protocolo de descifrado de umbral y obtienen una copia sin cifrar de la suma, que tiene las características de un número aleatorio, para la que se determina una representación binaria. Después, los jugadores sustraen conjuntamente de una copia sin cifrar de la suma los bits cifrados del número aleatorio usando la representación binaria. Esta operación crea una representación binaria $[[x_0]],\ldots, [[x_{t-1}]]$ del conjunto de datos [[x]].

La presente invención es ventajosa, ya que los cifrados $[[x_0]], [[x_1]],\ldots, [[x_{t-1}]]$ están disponibles para todos los jugadores, quienes pueden usarlos para cálculos posteriores sin tener que necesitar a otros jugadores. La presente invención soluciona este problema en una configuración criptográfica en lugar de en una configuración sin condiciones. Además, la presente invención permite reducir la carga computacional y de comunicación de, por ejemplo, un sensor biométrico, suponiendo que el conjunto de datos que está cifrado se extrae de una característica biométrica de una persona.

Características y ventajas adicionales de la presente invención resultarán evidentes cuando se analicen las reivindicaciones adjuntas y la siguiente descripción. Los expertos en la técnica se percatarán de que diferentes características de la presente invención pueden combinarse para crear realizaciones diferentes a las descritas a continuación.

Realizaciones preferidas de la presente invención se describirán en detalle con referencia a los dibujos adjuntos, en los que:

la Fig. 1 muestra un sistema básico de la técnica anterior para la identificación y la autenticación de una persona en función de datos biométricos asociados a la persona, en el que la presente invención puede aplicarse de manera ventajosa; y

la Fig. 2 muestra otro sistema para la identificación y la autenticación de una persona en función de datos biométricos asociados a la persona, en el que la presente invención puede aplicarse de manera ventajosa.

Con el fin de llevar a cabo los cálculos seguros de múltiples partes descritos en esta solicitud, se usa un sistema de cifrado homomórfico de umbrales, tal como, por ejemplo, Paillier o El Gamal. El término "homomórfico" implica que [[x + y]] = [[x]][[y]], es decir, el cifrado de (x + y) es igual al cifrado de x multiplicado por el cifrado de y. El término implica además que $[[x]]^a = [[x*a]]$ para cualquier 'x' y 'a'. El término "umbral" implica que cada jugador de entre un

grupo de t jugadores tiene acceso a una parte de una clave secreta, de modo que cualquier grupo de t o más jugadores puede descifrar conjuntamente un texto cifrado, pero un grupo más pequeño no puede descifrar el texto cifrado.

La presente invención puede utilizarse de manera ventajosa en un sistema de autenticación biométrica, en el que características biométricas de un usuario se comparan con datos de referencia. Si se produce una coincidencia, el usuario es identificado y se le concede acceso. Los datos de referencia del usuario se han obtenido anteriormente y están almacenados de manera segura, por ejemplo en una base de datos segura o una tarjeta inteligente. El objeto físico a autenticar también puede ser no humano. Por ejemplo, el objeto puede ser un medio de almacenamiento como un CD, un DVD o una memoria de estado sólido que contiene contenido digital protegido. En ese caso no se usa necesariamente la biometría sino que, de manera análoga, alguna característica de identificación (en forma de, por ejemplo, una secuencia de bits) que debe mantenerse en secreto se proporciona y se compara con los datos de referencia correspondientes.

En la autenticación, el usuario proclama tener una determinada identidad y una plantilla biométrica ofrecida se compara con una plantilla biométrica almacenada que está relacionada con la identidad proclamada, con el fin de verificar la correspondencia entre la plantilla ofrecida y la almacenada. En la identificación, la plantilla biométrica ofrecida se compara con todas las plantillas disponibles almacenadas con el fin de verificar la correspondencia entre la plantilla ofrecida y la almacenada. Debe observarse que los datos biométricos son una buena representación de la identidad de una persona, y la adquisición no autenticada de datos biométricos asociados a una persona puede considerarse un equivalente electrónico de la usurpación de la identidad de la persona. Después de haber adquirido datos biométricos apropiados que identifican a una persona, el intruso puede suplantar a la persona cuya identidad ha adquirido el intruso. Además, los datos biométricos pueden contener información delicada y privada sobre el estado de salud. Por tanto, debe protegerse la integridad de las personas que utilizan sistemas biométricos de autenticación/identificación.

En un sistema de cifrado homomórfico se usa un cifrado de claves públicas y dos (o más) jugadores, por ejemplo un usuario y un verificador (o varios verificadores), tienen acceso a la misma clave pública. Además, el usuario y el verificador tienen acceso a una parte de una clave privada correspondiente. Las partes de la clave privada se usan para el descifrado.

El usuario puede llevar encima su parte (por ejemplo, en una tarjeta inteligente) o la parte puede estar almacenada en un sensor de, por ejemplo, un sistema biométrico de identificación con el que el usuario interacciona. Durante el registro se captura una secuencia de bits $x_0, x_1,\ldots,x_{t-1}$ que representan un identificador biométrico, se convierte en un número x:

$$x = \sum_{i=0}^{t-1} x_i 2^i ,$$

y se cifra con la clave pública común. El cifrado [[x]] del número x se transfiere después al verificador, que lo almacena. Debe observarse que el verificador no puede descifrar el número cifrado, ya que el verificador solo tiene acceso a su parte de la clave privada y no a la parte del usuario. Por tanto, la representación sin cifrar x del identificador biométrico permanece oculta al verificador. Debe observarse que el verificador consiste preferiblemente en varios servidores que llevan a cabo de manera conjunta y segura cálculos de correspondencias. Cada servidor tiene una parte de la clave secreta. Solo si un número suficiente de servidores colaboran puede llevarse a cabo el descifrado.

Durante la autenticación, una representación ruidosa ‘y’ del identificador biométrico se obtiene en un sensor del sistema. Debe observarse que este sensor no es necesariamente el mismo sensor con el que se llevó a cabo el registro, siendo normalmente un sensor de bajo coste que tiene recursos de cálculo limitados. Normalmente, el sensor de autenticación es remoto con respecto al sensor de registro. Por ejemplo, el registro, que solo se lleva a cabo una vez, puede realizarse en una autoridad de registro en forma de cualquier tienda de DVD/vídeo comprendida en una cadena más grande de tiendas, mientras que la autenticación se lleva a cabo normalmente en una tienda específica en la que un usuario alquila un DVD. Esta tienda puede considerarse el verificador real en el que el usuario va a autenticarse. El proceso de autenticar al usuario se lleva a cabo cada vez que alquila un DVD en la tienda. Este sensor de autenticación cifra ‘y’ con la clave pública común. Posteriormente, los servidores de verificación segura convierten el número cifrado [[y]] en cifrados de bits respectivos $[[y_0]],\ldots, [[y_{t-1}]]$ que forman el número ‘y’. Después, las representaciones binarias cifradas $[[x_0]],\ldots, [[x_{t-1}]]$ e $[[y_0]],\ldots, [[y_{t-1}]]$ se comparan entre sí de manera segura. Por tanto, se realiza una comprobación de correspondencias de modo que el usuario pueda autenticarse.

En una realización de la invención, se supone que un número x va a cifrarse, donde $x \in \{0, 1,\ldots, n-1\}$. La entrada del protocolo utilizado para el cifrado viene dada por el cifrado $[[x]]$ y la salida por $[[x_0]],\ldots, [[x_{t-1}]]$, donde t denota la longitud en bits del número n-1. Los participantes del protocolo se denominan jugadores.

En primer lugar, los jugadores, que normalmente adoptan la forma de un grupo de servidores seguros, generan conjuntamente un número aleatorio $0 \leq r < n$ y llevan a cabo un cifrado basado en bits $[[r_0]], [[r_{t-1}]]$ del número aleatorio, donde

$$r = \sum_{i=0}^{t-1} r_i 2^i .$$

Por tanto, suponiendo que r=9, entonces $r_0=1$, $r_1=0$, $r_2=0$ y $r_3=1$. Por consiguiente, $r = 1*2^0 + 0*2^1 + 0*2^2 + 1*2^3 = 1 + 0 + 0 + 8 = 9$. En caso de que se usen dos servidores seguros, los dos servidores generan y cifran conjuntamente bits aleatorios. Por ejemplo, para r_0, el primer servidor calcula $[[r_0']]$ y el segundo servidor calcula $[[r_0'']]$. Después se calcula de manera segura $[[r_0]] = [[r_0' \oplus r_0'']]$, donde $\oplus$ denota una operación XOR. Este procedimiento se aplica a todos los bits $[[r_0]],\ldots, [[r_{t-1}]]$ del número aleatorio.

Los cifrados van acompañados de pruebas de conocimiento cero necesarias, que están dispuestas para mostrar que los bits cifrados son correctos. Existen varias técnicas diferentes para calcular tales pruebas. En una configuración de El Gamal, las pruebas pueden calcularse de la siguiente manera. Dada una clave privada $\alpha = \log_g h$, el descifrado se lleva a cabo calculando b/a^{α}, que es igual a g^m para algún mensaje $m \in Zq$. Los cifrados se calculan mediante una clave pública común h, mientras que los descifrados se realizan usando un protocolo conjunto entre partes, poseyendo cada jugador una parte de la clave privada $\alpha = \log_g h$. Los jugadores obtienen su parte ejecutando un protocolo de generación de claves distribuidas.

La generación de claves distribuidas se consigue haciendo que los jugadores P_1, P_2 (por ejemplo, un sensor biométrico y un verificador, o el primer y el segundo servidor) difundan en primer lugar condiciones $c_i = g^{\alpha_i} h^{r_i}$, donde α_i, $r_i \in Zq$ para i = 1, 2, y después difundan los valores r_i junto con pruebas de conocimiento de $\log_g h_i$, donde $h_i = c_i/h^{r_i}$ para i = 1,2. La clave pública conjunta es $h = h_1 h_2$, siendo la clave privada $\alpha = \alpha_1 + \alpha_2$. Para descifrar un cifrado (a, b), el jugador P_i produce $d_i = a^{\alpha i}$, junto con una prueba de que $\log_a d_i = \log_g h_i$, es decir, una prueba dispuesta para mostrar que los datos de salida cifrados son correctos sin revelar información acerca de las copias sin cifrar de los datos que están cifrados. Después, el mensaje se recupera a partir de $b/(a_1 a_2)$. Debe observarse que en un sistema de Paillier el procedimiento es diferente.

Después de que los jugadores hayan generado bits cifrados $[[r_0]],\ldots, [[r_{t-1}]]$, calculan el cifrado $[[x + r]]$ de la siguiente manera

$$[[x]] \prod_{i=0}^{t-1} [[r_i]]^{2^i} .$$

Esto se realiza usando una puerta de multiplicación segura genérica o una puerta de multiplicación restringida denominada puerta condicional. Usando una puerta condicional, dos valores cifrados 'r' y 'x' pueden multiplicarse de manera eficaz, siempre que r esté limitado a un dominio de dos valores, por ejemplo $r \in \{0, 1\}$. No hay restricciones en el valor de x, por ejemplo $x \in Z_{n^*}$. El cifrado $[[x + r]]$ no es calculado necesariamente por todos los jugadores, sino que puede calcularse por un único jugador, por ejemplo el primer servidor seguro, y distribuirse a los otros jugadores, es decir, el segundo servidor seguro.

Después, los jugadores llevan a cabo conjuntamente un protocolo de descifrado de umbral y calculan $y = (x + r) \bmod n$ de manera no cifrada. Debido a los datos que forman el número 'y', 'y' también tiene las características de un número aleatorio, y las representaciones sin cifrar x, r no pueden obtenerse de 'y', ya que ni x ni r son datos públicos. Los jugadores determinan la representación binaria de 'y' y restan conjuntamente de esta representación binaria el cifrado $[[r]]$ del número aleatorio generado r. Esto se consigue mediante una resta basada en bits, es decir, $y_0 - [[r_0]]$, $y_1 - [[r_1]],\ldots, y_{t-1} - [[r_{t-1}]]$. Esto da como resultado otro cifrado $[[z]]$, que se calcula como

$$[[z]] = y - [[r]],$$

usando un circuito de resta segura (en bits cifrados).

Esto da como resultado la representación binaria de un número z=x o z=x – n dados los bits cifrados $[[z_0]],\ldots, [[z_{t-1}]]$, donde z_t es un bit de signo. Por tanto, dependiendo del bit de signo se adquiere $[[x_0]],\ldots, [[x_{t-1}]]$ o $[[(x - n)_0]],\ldots, [[(x - n)_{t-1}]]$. Los jugadores reducen el valor de z módulo n sumando nz_t a z usando las representaciones binarias. Por tanto, se crean representaciones binarias $[[x_0]], [[x_{t-1}]]$.

En otra realización de la invención, se supone que $0 \leq x < 2^m << 2^k < n$, $k » m$, y, por tanto, $2k >> 2^m$. La entrada del protocolo usado para el cifrado viene dada de nuevo por el cifrado $[[x]]$ y la salida por $[[x_0]],\ldots, [[x_{t-1}]]$. En esta realización a modo de ejemplo se describe cómo se determinan los m bits menos significativos $x_0,\ldots, x_{m-1}$ de x. Cada jugador P_i, $1 \leq i \leq 1$, elige bits aleatorios $r_{0,i},\ldots, r_{m-1,i}$, donde $r_{*,i} \in_R \{0, 1\}$ y $r'_i \in \{0,\ldots, 2^{k-m} -1\}$, cifra estos bits y distribuye los cifrados $[[r_{0,i}]],\ldots, [[r_{m-1,i}]]$ y $[[r'_i]]$ junto con pruebas de que los cifrados se han calculado correctamente.

Los jugadores usan estos bits cifrados para crear conjuntamente cifrados de bits aleatorios $[[r_0]],\ldots, [[r_{m-1}]]$, donde el cifrado del bit aleatorio r se calcula de manera segura como

$$r = \sum_{i=1}^{1} r_{j,\,i} \bmod 2$$

usando puertas de multiplicación seguras y un número aleatorio r' que se calcula como

$$r' = \sum_{i=1}^{1} r_i'$$

usando propiedades criptográficas homomórficas.

Los jugadores forman conjuntamente el cifrado $[[x – r]]$, y el cifrado $[[x – r]]$ se descifra después conjuntamente usando un protocolo de descifrado de umbral para revelar el valor $y = x-r$, donde

$$r = \sum_{j=0}^{m-1} r_j * 2^j + r'2^m < 2^k .$$

Los bits públicos $y_0,\ldots, y_{m-1}$ denotan la representación binaria de y mod 2^m. Un circuito de suma seguro para entradas públicas $y_0,\ldots, y_{m-1}$ y $[[r_0]],\ldots, [[r_{-1}]]$ se usa para producir una salida de m bits cifrados $[[x_0]],\ldots, [[x_{m-1}]]$. Calculando y mod 2^m se ignora un bit de arrastre final.

La Fig. 1 muestra un sistema básico de la técnica anterior para la identificación y la autenticación de una persona en función de datos biométricos asociados a la persona, en el que el sistema de la presente invención puede utilizarse de manera ventajosa. Datos biométricos sin tratar de una persona, por ejemplo huellas dactilares, el iris o la retina, la geometría del resto o las manos, características de la voz etc., se capturan en un sensor 101. Normalmente, una secuencia de bits $x_0, x_1,\ldots, x_{t-1}$ que representa los datos biométricos se obtiene en el sensor. Los datos adquiridos (es decir, datos no procesados sin cifrar) son procesados normalmente en un dispositivo de procesamiento 102, tal como un procesador de señales digitales (DSP). El dispositivo de procesamiento puede estar integrado en el sensor. Este procesamiento implica la conversión de los bits en un número x, que se cifra con la clave pública común. El cifrado $[[x]]$ del número x se almacena después (o los cifrados de los bits de x) a través de la trayectoria 105 en un medio de almacenamiento de base de datos 103 de un proveedor de servicios. Esto es un procedimiento de inicialización que se lleva a cabo una vez para cada persona que desee acceder al sistema particular, con el fin de registrar a la persona.

Después, cuando la persona desea acceder al servicio, proporciona datos biométricos sin cifrar $y_0,\ldots, y_{t-1}$ al sensor 101. Posteriormente, estos datos, después del cifrado, se comparan a través de la trayectoria 106 con los datos biométricos $[[x]]$ de la persona, almacenados anteriormente en la base de datos. Si hay una correspondencia en la comparación realizada en un dispositivo de comparación 104 entre los conjuntos de datos proporcionados a través de la trayectoria 106 y 107, la persona obtiene acceso al servicio proporcionado. Cuando se lleva a cabo la comparación, el protocolo de división en bits descrito anteriormente se lleva a cabo para los datos cifrados $[[x]]$ almacenados en el medio de almacenamiento 103, de modo que puede realizarse una comparación basada en bits entre $[[y_0]],\ldots, [[y_{t-1}]]$ y $[[x_0]],\ldots, [[x_{t-1}]]$.

Por tanto, con referencia a la Fig. 1, el sensor 101 puede actuar en una sesión inicial de extracción de características como un dispositivo de registro, mientras que en una sesión subsiguiente, el sensor 101 actúa como un verificador que comprueba correspondencias, en el dispositivo de comparación 104, entre información biométrica 'y' proporcionada posteriormente (a través de la trayectoria 106) e información biométrica x registrada inicialmente (a través de la trayectoria 107). Como se ha mencionado anteriormente, los dispositivos de la Fig. 1 pueden estar situados de manera remota entre sí. Normalmente, en el tipo de sistema mostrado en la Fig. 1, el sensor 101 es relativamente potente para calcular operaciones criptográficas. En caso de que se use un sensor potente, el sensor

101 / dispositivo de procesamiento 102 y el dispositivo de comparación 104 llevan a cabo conjuntamente el protocolo de división en bits de la presente invención.

La Fig. 2 muestra otro sistema para la identificación y autenticación de una persona en función de datos biométricos asociados a la persona, en el que puede aplicarse la presente invención. En este caso, el sensor de registro 201 y el sensor de verificación, o autenticación, 208 están situados de manera remota entre sí. Al igual que en la Fig. 1, los datos adquiridos (es decir, los datos no procesados sin cifrar) x_0, x_1,…, x_{t-1} se convierten en un número x y se cifran con la clave pública común en un DSP 202. El cifrado [[x]] del número x se almacena después en un medio de almacenamiento de base de datos 203. Posteriormente, cuando la persona desea acceder al sistema, proporciona datos biométricos sin cifrar y_0, …, y_{t-1} al sensor de autenticación 208. Estos datos se convierten posteriormente en un número 'y' y se cifran mediante un DSP 209. Por tanto, con referencia a la Fig. 2, donde se supone que una plantilla biométrica x se ha proporcionado anteriormente al sensor de registro 201, se ha cifrado en el DSP 202 y almacenado en forma cifrada [[x]] en el medio de almacenamiento de base de datos 203, cuando una persona solicita acceder al sistema, su plantilla biométrica 'y' (que es una representación ruidosa de x) es extraída por el sensor de verificación 208 (también denominado sensor de autenticación) y es cifrada por el DSP 209 para crear una copia cifrada [[y]]. Normalmente, el DSP 209 está incluido en el sensor de autenticación 208. En este sistema particular, la presente invención es incluso más ventajosa que el sistema mostrado en la Fig. 1, ya que el sensor 208 es normalmente un sensor de bajo coste que tiene recursos de cálculo limitados.

El número [[x]] se transfiere al verificador 211, posiblemente a través de una red 210, tal como Internet, que almacena la cadena. El verificador 211 también contiene normalmente un DSP, aunque no se muestra en la Fig. 2. Debe observarse que el verificador no puede descifrar [[x]], ya que el verificador solo tiene acceso a su parte de la clave privada y no a la parte de la persona. Por tanto, la representación sin cifrar x del identificador biométrico permanece oculta al verificador 211. Un protocolo seguro de división en bits según la presente invención se ejecutará en el verificador 211. Para mejorar la seguridad, la ejecución del protocolo de división en bits se transfiere a un grupo de servidores seguros 212, 213. Por tanto, el verificador 211 proporciona a los servidores el cifrado [[x]] e [[y]] de cada conjunto de datos biométricos x e y, respectivamente.

Como se ha descrito anteriormente, los servidores seguros 212, 213 generan conjuntamente un número aleatorio $0 \leq r < n$ y llevan a cabo un cifrado basado en bits [[r_0]],…, [[r_{t-1}]] del número aleatorio. Los cifrados del número aleatorio van acompañados de pruebas necesarias de conocimiento cero, que están dispuestas para mostrar que los bits cifrados son correctos. Cuando los servidores 212, 213 han generado bits cifrados [[r_0]],…, [[r_{t-1}]], ambos (o al menos uno de los dos servidores) calculan el cifrado [[x + r]] como

$$[[x]] \prod_{i=0}^{t-1} [[r_i]]^{2^i} .$$

Después, los servidores 212, 213 llevan a cabo conjuntamente un protocolo de descifrado de umbral y calculan y = (x + r) mod n de manera no cifrada, y determinan la representación binaria de 'y' y restan conjuntamente de esta representación binaria el cifrado [[r]] del número aleatorio generado r. Por consiguiente, se crea otro cifrado [[z]], que se calcula como

$$[[z]] = y - [[r]].$$

Esto da como resultado la representación binaria de un número z=x o z=x – n dados los bits cifrados [[z_0]],…, [[z_{t-1}]], donde z_t es un bit de signo. Por tanto, dependiendo del bit de signo se adquiere [[x_0]],…, [[x_{t-1}]] o [[$(x - n)_0$]],…, [[$(x - n)_{t-1}$]]. Uno de los servidores 212, 213 (o ambos) reducen el valor de z módulo n sumando nz_t a z usando las representaciones binarias. Por tanto, se crean las representaciones binarias [[x_0]],…, [[x_{t-1}]]. Las representaciones binarias [[y_0]],…, [[y_{t-1}]] se crean de manera análoga.

A continuación, cuando se ha llevado a cabo el protocolo de división en bits, el verificador 211 y el sensor de autenticación 208 pueden usar cualquier procedimiento apropiado conocido de comparación de datos biométricos cifrados, por ejemplo el procedimiento dado a conocer en el documento ID695459/NL041335, para determinar si hay correspondencias entre las representaciones binarias cifradas [[y_0]],…, [[y_{t-1}]] y [[x_0]],…, [[x_{t-1}]]. Aunque la invención se ha descrito con referencia a realizaciones específicas a modo de ejemplo de la misma, muchas alteraciones, modificaciones, etc. diferentes resultarán evidentes para los expertos en la técnica. Por lo tanto, las realizaciones descritas no pretenden limitar el alcance de la invención, definida por las reivindicaciones adjuntas. Debe observarse que aunque dos servidores seguros llevan a cabo conjuntamente el protocolo de división en bits según las realizaciones a modo de ejemplo de la invención mostradas anteriormente, puede utilizarse cualquier número apropiado de servidores seguros para llevar a cabo conjuntamente el protocolo de división en bits.

REIVINDICACIONES

1.- Un procedimiento para convertir un conjunto de datos cifrados en un cifrado de bits individuales que representan el conjunto de datos, comprendiendo el procedimiento las etapas de:

generar un número aleatorio y calcular un cifrado basado en bits del número aleatorio;
calcular de manera segura una suma cifrada en función del conjunto de datos cifrados y el número aleatorio cifrado;
descifrar la suma cifrada y determinar una representación binaria de la suma; y
crear el cifrado de dichos bits individuales que representan el conjunto de datos cifrados procesando la representación binaria de la suma con el número aleatorio cifrado.

2.- El procedimiento según la reivindicación 1, que comprende además la etapa de adquirir el conjunto de datos cifrados.

3.- El procedimiento según la reivindicación 1, que comprende además la etapa de proporcionar una prueba públicamente verificable de que los cifrados del número aleatorio se han calculado correctamente.

4.- El procedimiento según la reivindicación 1, en el que dicha etapa de calcular una suma cifrada se lleva a cabo multiplicando el conjunto de datos cifrados y el número aleatorio cifrado usando una puerta de multiplicación segura.

5.- El procedimiento según la reivindicación 1, en el que la etapa de descifrar dicha suma cifrada se lleva a cabo usando un protocolo de descifrado de umbral.

6.- El procedimiento según la reivindicación 1, en el que la etapa de crear el cifrado de dichos bits individuales que representan el conjunto de datos cifrados se lleva a cabo restando de la representación binaria de la suma el numero aleatorio cifrado.

7.- El procedimiento según la reivindicación 6, en el que la resta se lleva a cabo usando una puerta de resta segura.

8.- El procedimiento según la reivindicación 6, en el que la etapa de crear el cifrado de dichos bits individuales comprende además la etapa de añadir un bit de signo a la representación binaria de la suma.

9.- El procedimiento según la reivindicación 1, en el que la etapa de crear el cifrado de dichos bits individuales que representan el conjunto de datos cifrados se lleva a cabo añadiendo el número aleatorio cifrado a la representación binaria de la suma.

10.- El procedimiento según la reivindicación 1, en el que el conjunto de datos que está cifrado se extrae de una característica biométrica de una persona.

11.- Un sistema para convertir un conjunto de datos cifrados en un cifrado de bits individuales que representan el conjunto de datos, comprendiendo el sistema:

al menos un primer y un segundo dispositivo de cálculo (212, 213) dispuestos para generar conjuntamente un número aleatorio y calcular un cifrado basado en bits del número aleatorio; en el que
al menos uno de los dispositivos de cálculo está dispuesto para calcular una suma cifrada en función del conjunto de datos cifrados y el número aleatorio cifrado;
estando dispuestos dichos primer y segundo dispositivos de cálculo para descifrar conjuntamente la suma cifrada y determinar una representación binaria de la suma, y
estando dispuestos dichos primer y segundo dispositivos de cálculo para crear conjuntamente el cifrado de dichos bits individuales que representan el conjunto de datos cifrados procesando la representación binaria de la suma con el número aleatorio cifrado.

12.- El sistema según la reivindicación 11, en el que dichos primer y segundo dispositivos de cálculo (212, 213) están dispuestos además para calcular una prueba públicamente verificable de que los cifrados del número aleatorio se han calculado correctamente.

13.- El sistema según la reivindicación 11, en el que dichos primer y segundo dispositivos de cálculo (212, 213) están dispuestos para descifrar la suma cifrada ejecutando conjuntamente un protocolo de descifrado de umbral.

14.- El sistema según la reivindicación 11, en el que dichos primer y segundo dispositivos de cálculo (212, 213) están dispuestos para generar conjuntamente un número aleatorio y calcular un cifrado basado en bits del número aleatorio:

generando un bit respectivo para cada bit del número aleatorio y aplicando una función XOR a dichos bits respectivos para crear cada dicho bit del número aleatorio; y

cifrar de manera segura cada bit del número aleatorio.

15.- Un programa informático que comprende componentes ejecutables por ordenador para hacer que un dispositivo lleve a cabo las etapas mencionadas en la reivindicación 1 cuando los componentes ejecutables por ordenador se ejecutan en una unidad de procesamiento incluida en el dispositivo.

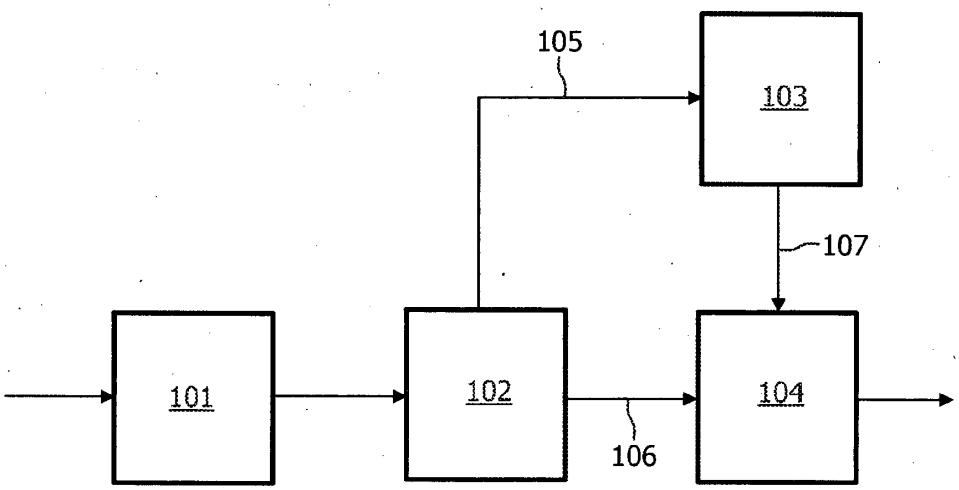

FIG. 1

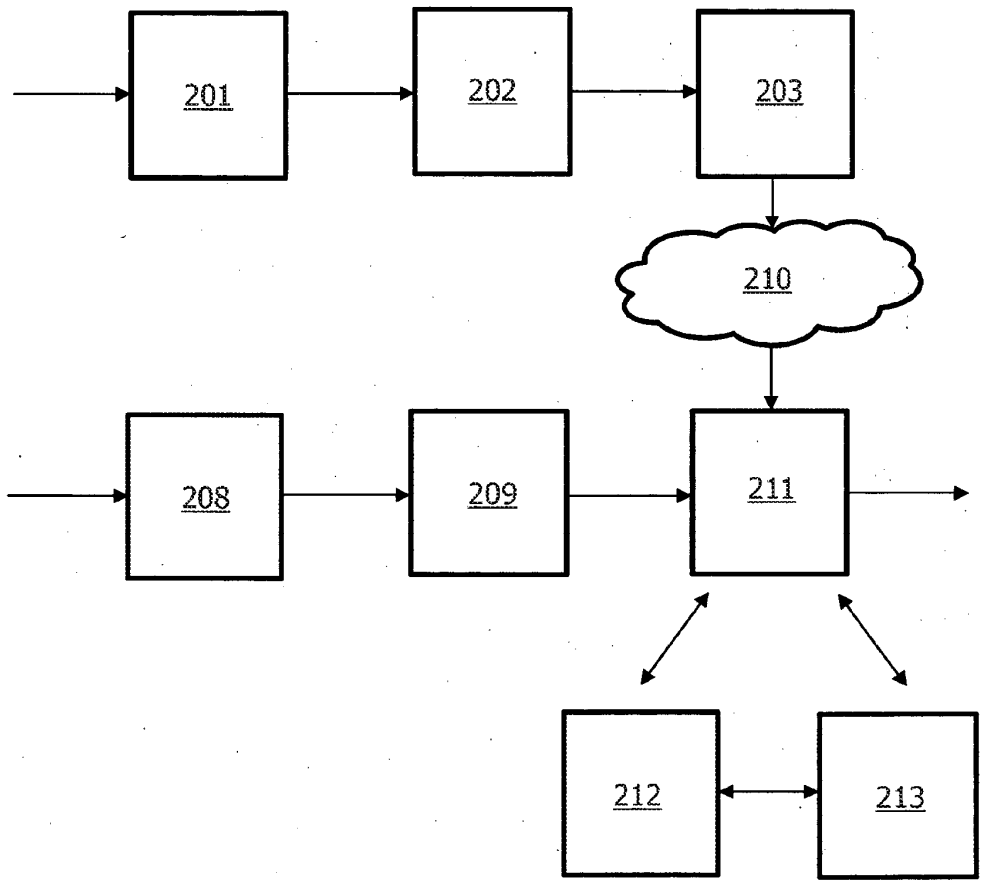

FIG. 2