(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 422 868**

(51) Int. CI.:

H04L 9/06 (2006.01)
H04L 9/30 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.07.2010 E 10752070 (2)**

(97) Fecha y número de publicación de la concesión europea: **01.05.2013 EP 2457344**

(54) Título: **Procedimiento de conversión de un primer cifrado en un segundo cifrado**

(30) Prioridad:

23.07.2009 FR 0955153

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.09.2013

(73) Titular/es:

ORANGE (100.0%)
78, rue Olivier de Serres
75015 Paris, FR

(72) Inventor/es:

SEURIN, YANNICK y
GILBERT, HENRI

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Procedimiento de conversión de un primer cifrado en un segundo cifrado

La presente invención se refiere al ámbito de la criptografía con clave secreta. Más concretamente, la invención trata de un procedimiento de conversión por parte de una entidad de conversión de un primer cifrado en un segundo cifrado.

La invención tiene una interesante aplicación en servicios denominados de transcifrado adaptados para recibir un contenido cifrado de una primera entidad y para transmitirlo cifrado a la atención de una segunda entidad.

En criptografía simétrica, el emisor y el destinatario de un mensaje comparten el conocimiento de una misma clave secreta K. Esta permite al emisor transformar un mensaje en abierto en un criptograma, o mensaje cifrado, y al destinatario recuperar el mensaje en abierto a partir del mensaje cifrado.

Algunas aplicaciones requieren que una entidad intermediaria entre el emisor y el destinatario convierta un primer cifrado C1 de un mensaje en abierto M, obtenido mediante una primera entidad U1 por medio de una primera clave secreta K1, en un segundo cifrado C2 del mismo mensaje en abierto M por medio de una segunda clave secreta K2 para una segunda entidad U2. La segunda entidad U2, que posee la segunda clave secreta K2, es capaz de obtener el mensaje en abierto mediante descifrado del segundo cifrado C2. Un ejemplo de dicho servicio consiste en un servicio de almacenamiento remoto de contenidos. La primera entidad transmite a un servidor remoto de almacenamiento datos cifrados por medio de su clave secreta K1. Más adelante, la primera entidad U1 desea dar acceso a sus datos a una segunda entidad U2 sin revelarle su clave secreta. Una manera evidente de proceder consiste en transmitir a la entidad intermediaria, en este caso el servidor remoto, las claves secretas K1 y K2 de ambas entidades, con el fin de que la entidad intermediaria descifre por medio de la clave K1 el primer cifrado C1 para obtener el mensaje en abierto M, y cifre por medio de la clave secreta K2 de la segunda entidad el mensaje M obtenido a la atención de la segunda entidad U2. Sin embargo, procediendo de esta manera, la entidad intermediaria toma conocimiento del mensaje en abierto M. Además, la entidad intermediaria posee las respectivas claves secretas de las entidades. Se entiende sin embargo que unos usuarios deseosos de poner en funcionamiento semejante servicio puedan no confiar en la entidad intermediaria. Por lo tanto, se entiende que algunos usuarios deseen, por motivos de confianza, tener la garantía de que la entidad intermediaria no accede al mensaje en abierto y que, por otra parte, no desean, por motivos de seguridad, transmitir su clave secreta a la entidad intermediaria.

Por lo tanto, la manera evidente de proceder puede no convenir. Ahora bien, no existe procedimiento alguno que permite cifrar de nuevo para otro usuario en el marco de la criptografía con clave secreta.

Se conoce mediante el documento D1 del estado de la técnica: “How to encrypt with the LPN Problem”, de Henri Gilbert, Matthew Robshaw y Yannick Seurin, un esquema de cifrado probabilista con clave privada denominado LNP_C, cuya seguridad puede reducir la dificultad de aprendizaje a partir del problema de paridad con ruido. El protocolo propuesto implica únicamente operaciones básicas en GF(2) y un código corrector de error.

El esquema de cifrado enriquece el número de primitivas criptográficas cuya seguridad reposa en la dificultad del LNP.

Con objeto de remediar los problemas identificados anteriormente, la invención propone un procedimiento de conversión, mediante una entidad de conversión, de un primer cifrado en un segundo cifrado, correspondiendo el primer cifrado al resultado de un cifrado probabilista simétrico de un elemento de mensaje en abierto por medio de una primera matriz secreta parametrada mediante un vector aleatorio, correspondiendo el segundo cifrado al resultado de un cifrado probabilista simétrico del elemento de mensaje en abierto por medio de una segunda matriz secreta parametrada mediante el vector aleatorio, caracterizado por el hecho de que el procedimiento incluye una etapa de cálculo del segundo cifrado mediante cifrado del primer cifrado por medio de una matriz secreta de conversión en función de la primera y la segunda matriz secreta, y parametrada mediante el vector aleatorio.

Inmediatamente, se observa que, por definición, un “elemento de mensaje” incluye todo o parte de un mensaje.

Con el procedimiento de la invención, es posible, en un contexto de criptografía simétrica, convertir un primer cifrado de un mensaje en abierto obtenido por medio de una primera clave secreta en un segundo cifrado del mismo mensaje en abierto para ser descifrado por medio de una segunda clave secreta. Esta conversión se realiza sin que la entidad encargada de la conversión pueda tomar conocimiento del mensaje en abierto asociado correspondiente a estos dos cifrados. En efecto, la entidad de conversión procesa el primer cifrado que resulta de un cifrado probabilista simétrico por medio de una primera matriz secreta, pero no dispone de la primera matriz secreta que le permitiría descifrar el primer cifrado para obtener el mensaje en abierto. Asimismo, la entidad de conversión calcula el segundo cifrado, destinado a ser descifrado conforme a un descifrado probabilista simétrico por medio de una segunda matriz secreta, pero no dispone de la segunda matriz secreta que le permitiría descifrar el segundo cifrado para obtener el mensaje en abierto. En efecto, la entidad de conversión utiliza, para efectuar la conversión del primer cifrado en el segundo cifrado, una matriz de conversión que no proporciona información alguna sobre las matrices

secretas. Por lo tanto, no es posible, a partir de la matriz de conversión, encontrar la primera o la segunda matriz secreta.

Se observa además que el procedimiento de conversión es simétrico en el sentido de que la entidad de conversión está asimismo adaptada para convertir el segundo cifrado asociado obtenido mediante cifrado simétrico probabilista por medio de la segunda matriz secreta en el primer cifrado asociado a la primera matriz secreta utilizando la misma matriz de conversión que para una conversión del primer cifrado en el segundo cifrado.

En un modo de realización de la invención, el procedimiento incluye una etapa de:

- recepción del primer cifrado acoplado al vector aleatorio procedente de una primera entidad,

- envío del segundo cifrado acoplado al vector aleatorio con destino a una segunda entidad.

Este modo de realización corresponde a una utilización del procedimiento de conversión por dos entidades para transmitir datos cifrados de la primera entidad a la segunda entidad. Unas entidades, por ejemplo usuarios que utilizaran esta entidad de conversión en el marco de un servicio de intercambio de datos cifrados, quedarían así tranquilizadas sobre la seguridad empleada por el servicio, y confiadas en lo que se refiere al carácter confidencial de los datos transmitidos.

De manera ventajosa, la matriz secreta de conversión se calcula mediante una operación de O EXCLUSIVO entre la primera y la segunda matriz secreta.

La matriz de conversión, aunque calculada a partir de las matrices secretas de la primera y la segunda entidad, no proporciona información que permita encontrar la primera o la segunda matriz secreta. Por lo tanto, no es posible, a partir de la matriz de conversión, obtener el mensaje en abierto asociado al primero y al segundo cifrado.

La invención se describe en este caso con una única matriz de conversión calculada a partir de dos matrices secretas, estando cada matriz asociada a una entidad. Se entiende que la entidad de conversión puede emplear el procedimiento de conversión para n entidades, con n > 2. Las entidades se escriben 1, 2, …, n. En este caso, la entidad de conversión solo necesita almacenar en su memoria (n - 1) matrices de conversión. Se calcula entonces (n-1) matrices de conversión M_{12}, M_{23}, M_{34}, …, M_{n-1n}, que se transmiten a la entidad de conversión. Se observa en efecto que no es necesario calcular todas las matrices de conversión propias de todas las parejas de entidades (i, j). En efecto, es posible obtener una matriz de conversión para una pareja (i, j) con j>i+1, a partir de las matrices calculadas. En efecto, se observa que $M_{ij} = M_{i(i+1)} \oplus \ldots \oplus M_{(i+(j-i-1))j}$.

Ventajosamente, la matriz de conversión es una matriz de Toeplitz. Se conoce que con una matriz de Toeplitz, los coeficientes sobre una diagonal descendente de izquierda a derecha son los mismos. Por lo tanto, el conjunto de coeficientes de la matriz de conversión M_{12} puede deducirse únicamente de los coeficientes de la primera línea y la primera columna de la matriz. Asimismo, es suficiente con almacenar únicamente los coeficientes de la primera línea y la primera columna de la matriz de conversión, para disponer del conjunto de coeficientes de la matriz de conversión. Esto es interesante cuando la entidad de conversión dispone de poca memoria de almacenamiento.

Según un modo de realización de la invención, la matriz de conversión se obtiene mediante la entidad de conversión ante una entidad de confianza que calcula la matriz de conversión por medio de la primera y la segunda matriz secreta transmitida respectivamente por la primera y la segunda entidad.

En este modo de realización, se calcula la matriz de conversión mediante una entidad de confianza a partir de la primera y la segunda matriz secreta que le han transmitido la primera y la segunda entidad. La matriz de conversión, una vez calculada, se pone a disposición de la entidad de conversión. Se observa que la operación, delicada en términos de seguridad, que consiste en manipular la primera y la segunda matriz secreta para calcular la matriz de conversión se efectúa con una seguridad máxima por parte de una entidad dedicada en la que confían la primera y la segunda entidad.

La invención se refiere asimismo a un procedimiento de transmisión de un elemento de mensaje en abierto en forma cifrada entre una primera y una segunda entidad, que incluye una etapa de:

- cifrado por parte de la primera entidad por medio de un cifrado probabilista simétrico del mensaje en abierto, por medio de una primera matriz secreta, parametrada mediante un vector aleatorio, con objeto de obtener un primer cifrado,

- envío del primer cifrado acoplado al vector aleatorio, a una entidad de conversión,

- conversión por la entidad de conversión del primer cifrado en un segundo cifrado según el procedimiento de conversión,

- envío por parte de la entidad de conversión a la segunda entidad del segundo cifrado acoplado al vector aleatorio,

- recepción por la segunda entidad del segundo cifrado acoplado al vector aleatorio,

- descifrado por la segunda entidad del segundo cifrado por medio de una segunda matriz secreta mediante descifrado probabilista simétrico.

El procedimiento corresponde en este caso a un procedimiento de transmisión de extremo a extremo que integra una conversión de un primer cifrado en un segundo cifrado.

La invención se refiere asimismo a una entidad de conversión adecuada para convertir un primer cifrado en un segundo cifrado, correspondiendo el primer cifrado al resultado de un cifrado probabilista simétrico de un elemento de mensaje en abierto por medio de una primera matriz secreta parametrada mediante un vector aleatorio, correspondiendo el segundo cifrado al resultado de un cifrado probabilista simétrico del elemento de mensaje en abierto por medio de una segunda matriz secreta parametrada mediante el vector aleatorio, incluyendo la entidad de conversión:

- medios de cálculo del segundo cifrado, adecuados para calcular el segundo cifrado mediante cifrado del primer cifrado recibido por medio de una matriz secreta de conversión en función de la primera y la segunda matriz secreta, y parametrada mediante el vector aleatorio.

En un modo de realización de la invención, la entidad de conversión incluye además:

- medios de recepción adecuados para recibir el primer cifrado acoplado a un vector aleatorio,

- medios de envío adecuados para enviar el segundo cifrado acoplado al vector aleatorio.

La invención se refiere asimismo a un sistema de conversión adecuado para convertir un primer cifrado en un segundo cifrado, correspondiendo el primer cifrado al resultado de un cifrado probabilista simétrico de un elemento de mensaje en abierto por medio de una primera matriz secreta parametrada mediante un vector aleatorio, correspondiendo el segundo cifrado al resultado de un cifrado probabilista simétrico del elemento de mensaje en abierto por medio de una segunda matriz secreta parametrada mediante el vector aleatorio, incluyendo el sistema:

- una entidad de conversión según la invención,

- una entidad de confianza adecuada para calcular la matriz de conversión a partir de las matrices secretas.

La invención se refiere asimismo a un programa de ordenador destinado a ser instalado en una memoria de una entidad intermediaria, con instrucciones para la aplicación de las etapas del procedimiento de la invención, cuando el programa es ejecutado por un procesador.

La invención trata asimismo de un soporte de datos en el que está grabado el programa de ordenador de la invención.

Otras características y ventajas de la presente invención se entenderán mejor mediante la siguiente descripción y los dibujos adjuntos, en los cuales:

- las figuras 1a y 1b representan respectivamente un organigrama de las etapas de un procedimiento de cifrado simétrico probabilista y un organigrama de las etapas de un procedimiento de descifrado simétrico según el estado anterior de la técnica;

- la figura 2 representa un organigrama de las etapas del procedimiento de conversión de un primer cifrado y un segundo cifrado según un modo de realización particular descrito;

- la figura 3 representa un esquema bloque funcional de una forma particular de una entidad de conversión adecuada para poner en práctica el procedimiento de la figura 2.

El procedimiento de conversión según la invención se basa en un cifrado/descifrado probabilista simétrico como el descrito en [GRS08] (H. Gilbert, M. Robshaw and Y. Seurin. How to Encrypt with the LPN Problem? In ICALP'08, Lectures Notes in Computer Science, volumen 5126, págs. 679-690, Springer Verlag, 2008). Un cifrado se denomina "probabilista" cuando interviene un aleatorio en el cifrado. De esta forma, cuando se cifra dos veces el mismo mensaje en abierto, se obtienen dos mensajes cifrados distintos con una elevada probabilidad. El cifrado probabilista utilizado en el marco de la presente invención se basa en la combinación de una codificación mediante código corrector de errores y de la incorporación de un ruido. Esta combinación tiene por efecto dificultar el descifrado del cifrado por parte de un adversario, al mismo tiempo que está adaptado para ser naturalmente eliminado mediante la descodificación del código corrector de errores. Con este cifrado, es posible demostrar la seguridad mediante un

planteamiento reduccionista consistente en traducir la seguridad en una hipótesis sobre la dificultad de resolver un problema conocido. Dicho de otro modo, es posible demostrar que, para romper la seguridad de este método de cifrado, un atacante debe ser capaz de resolver un problema conocido, presuntamente difícil. En el marco del presente cifrado, el problema bien definido y bien conocido es el problema “LPN” (para “Learning Parity with Noise).

Las etapas de los procedimientos de cifrado y descifrado según un modo particular de realización se describen en relación con las figuras 1a y 1b. Según el estado anterior de la técnica, el procedimiento de cifrado probabilista simétrico utiliza una clave secreta compartida por una primera y una segunda entidad, una de cifrado y otra de descifrado, respectivamente con referencia 1 y 2. La entidad de descifrado 2 es capaz de aplicar un procedimiento de descifrado, o de restitución de un mensaje en abierto x a partir de un mensaje cifrado proporcionado por la primera entidad 1. La clave secreta puede estar representada en forma de una matriz M de k líneas y n columnas, con $1 \leq k$ y $1 \leq n$.

La entidad de cifrado 1 y la entidad de descifrado 2 están aquí integradas respectivamente en un equipamiento de comunicación emisor y en un equipamiento de comunicación receptor, no representados, capaces de comunicarse entre ellos, por ejemplo vía radio. Por ejemplo, el equipamiento emisor puede ser una etiqueta RFID y el equipamiento receptor un lector asociado.

El cifrado se denomina probabilista debido a que utiliza un aleatorio para calcular un mensaje cifrado a partir de un mensaje en abierto.

El mensaje en abierto x está representado por un vector binario con R bits.

El procedimiento incluye una etapa E1 de codificación del mensaje en abierto x con la ayuda de un código corrector de error, denominado C.

Un código corrector de errores es una técnica muy conocida por el especialista en la materia, basada en la redundancia. Tiene usualmente como vocación corregir errores de transmisión de un mensaje a través de un canal de comunicación poco fiable. En efecto, algunos datos del mensaje transmitido a través de este canal pueden verse alterados. El código corrector de errores desempeña como papel añadir datos redundantes en el mensaje antes de su transmisión. Estos datos redundantes permiten corregir los datos del mensaje tal como se ha recibido, que han sido alterados durante la transmisión.

En este caso, el código corrector de errores es un código lineal en bloques, denominado C. Este código corrector C es de longitud n, de dimensión r y de capacidad de corrección t. Dicho de otro modo, el código corrector C es una función del espacio binario de dimensión r $\{0,1\}^r$ en el espacio binario de dimensión n $\{0,1\}^n$. Esta función está adaptada para transformar un mensaje de r bits en una palabra de código de n bits, con $n > r$, mediante incorporación de bits de redundancia. Además, el código corrector C está adaptado para garantizar que, si se añade a la palabra de código un número de errores inferior a la capacidad de corrección t, la descodificación permite restituir el mensaje de origen.

En el ejemplo particular descrito aquí, se supone que el número de bits R del mensaje x es igual a la dimensión r del código corrector C.

La etapa E1 de codificación del mensaje x proporciona por lo tanto una palabra de código representada por un vector con n bits denominada C(x).

El procedimiento incluye una etapa E2 de generación de un aleatorio a. En el ejemplo de esta descripción, el imponderable a es un vector binario de k bits producido por una fuente seudoaleatoria de bits S.

La etapa E2 está seguida de una etapa E3 de cálculo del producto entre el vector aleatorio a, en forma de vector línea, con la matriz M representando la clave secreta. El resultado del producto $a \cdot M$ está representado por un vector de n bits.

Una vez realizadas las etapas E1 a E3, el procedimiento aplica un etapa de cálculo E4 en cuyo transcurso se añade el resultado del producto $a \cdot M$ a la palabra de código C(x). Dicho de otro modo, la etapa E4 realiza la operación $C(x) \oplus a \cdot M$. El papel de la etapa E4 es cifrar la palabra de código C(x).

El procedimiento incluye asimismo una etapa E5 de generación de un vector de ruido binario ε de n bits a partir de una fuente de ruido bernouilliano B. Esta está adaptada para producir bits independientes que valen 1 con una probabilidad η y bits independientes que valen 0 con una probabilidad $1 - \eta$, con $\eta \in]0, 1/2[$. Además, la fuente de ruido B está adaptada para que la probabilidad δ para el peso de Hamming del vector de ruido ε de ser superior a la capacidad de corrección t del código corrector sea muy fiable, inferior a un umbral Σ predefinido. A título de ejemplo, este umbral puede ser igual a 10^{-3}. Según el marco de utilización, podría ser inferior a dicho valor. Por definición, el peso de Hamming de un vector binario es el número de bits distintos de 0, es decir que valen 1, de dicho vector. Por

lo tanto, para la mayoría de los vectores de ruido ε generados por la fuente B, el peso de Hamming del vector ε, denominado Hwt(ε) es inferior o igual a la capacidad de corrección t del código corrector C. En el ejemplo particular descrito aquí, para cumplir la condición relativa a la probabilidad δ, los parámetros t, η y n verifican la siguiente relación: $t > \eta * n$.

Una vez realizadas las etapas E4 y E5, el procedimiento aplica una etapa de cálculo E6, en la que el vector de ruido ε se añade al resultado de la operación E4, $C(x) \oplus a \cdot M$. El resultado de esta operación E6 es un vector de n bits, denominado y, correspondiente al mensaje x cifrado. Esta es en definitiva la palabra de código C(x), es decir el mensaje x codificado, cifrado y con ruido.

Finalmente, el procedimiento incluye una etapa E7 de envío del par (a, y), es decir $(a, C(x) \oplus a \cdot M \oplus \varepsilon)$, a partir del equipamiento de comunicación emisor hacia el equipamiento de comunicación receptor.

El par (a, y) circula a través de un canal de comunicación, en este caso de radio, hasta su recepción por parte del equipamiento receptor, durante una etapa E8 representada en la figura 1b. Como recordatorio, el equipamiento receptor integra una entidad de descifrado capaz de descifrar el mensaje cifrado y recibido, con objeto de recuperar el mensaje en abierto x.

En un caso en que el mensaje en abierto x es de tamaño R bits con R > r, se corta el mensaje en abierto en bloques de r bits con, eventualmente, la incorporación de valores predeterminados para completar un bloque de r bits (se suele hablar de padding) si el valor R no es un múltiplo del valor r. El procedimiento de cifrado descrito se aplica entonces a cada bloque.

En la figura 1b, se han representado las distintas etapas del procedimiento de restitución, o de descifrado, para recuperar el mensaje en abierto x a partir del par (a, y), empleadas por la entidad de descifrado 2.

Cabe recordar que la entidad de descifrado 2 tiene conocimiento de la clave secreta representada por la matriz secreta M.

El procedimiento de restitución incluye, en primer lugar, una fase de cálculo que incluye dos etapas de cálculo E9 y E10.

Durante la primera etapa de cálculo E9, se extrae el vector aleatorio del par (a, y) recibido y se calcula el producto $a \cdot M$, a estando representada en forma de un vector línea de k bits.

Durante la etapa de cálculo E10, el vector de n bits resultante del producto $a \cdot M$ se añade al vector y recibido; dicho de otro modo, se realiza la operación de cálculo $y \oplus a \cdot M$. En binario, esta operación corresponde a restar el resultado del producto $a \cdot M$ del vector y recibido.

Obsérvese que al ser e igual a la palabra de código cifrada y con ruido, es decir $C(x) \oplus a \cdot M \oplus \varepsilon$, el resultado de la etapa de cálculo E10 corresponde a la palabra de código únicamente con ruido, es decir $C(x) \oplus \varepsilon$.

A continuación, el procedimiento incluye una fase de descodificación E11, durante la que se descodifica el resultado de la etapa E10 con la ayuda del código corrector de errores utilizado durante el cifrado. El peso de Hamming del vector de ruidos ε siendo inferior o igual a la capacidad de corrección t del código corrector de errores, la descodificación proporciona directamente el mensaje en abierto x.

A título de ejemplo, se proporcionan a continuación algunos ejemplos de realización de este procedimiento de cifrado con parámetros concretos. Se recuerda que la seguridad del sistema de cifrado depende de la dificultad de la resolución del problema LPN. Ahora bien, esta dificultad se basa en los parámetros k y η, correspondientes al número de bits del vector aleatorio a y a la probabilidad para un bit del vector de ruido ε de valer 1 respectivamente. Por lo tanto, conviene elegir valores convenientes para dichos parámetros, que permitan garantizar una adecuada seguridad del sistema. Dos ejemplos de valores convenientes para dichos parámetros k y η son los siguientes:

- $k = 512$, $\eta = 0{,}125$

- $k = 768$, $\eta = 0{,}05$

Obsérvese además que si el mensaje en abierto x es de tamaño r bits, el tamaño total del mensaje cifrado transmitido, correspondiente al par (a, y) es de (n+k) bits, ya que el vector aleatorio a incluye k bits y el cifrado y n bits. Por lo tanto, se observa que el cifrado se acompaña de cierta expansión del mensaje. El factor de expansión se escribe $\sigma = \frac{(n+k)}{r}$. Con objeto de limitar esta expansión, conviene por lo tanto, con k fijado, adoptar el valor de r mayor posible y el valor de n menor posible. Se recuerda además que la capacidad de corrección t del código

corrector y la longitud n del código correctos deben verificar la siguiente condición: $t > \eta * n$, con objeto de garantizar un descifrado correcto del mensaje en la mayoría de los casos.

Se anota [n,r,d] un trío de parámetros de un código corrector de errores. Estos parámetros n, r y d corresponden respectivamente a la longitud, la dimensión y la distancia mínima del código. La distancia mínima d del código es función de la capacidad de corrección t, mediante la siguiente relación:

$$t = \frac{d-1}{2}.$$

A continuación, se proporcionan cuatro ejemplos de realización con parámetros concretos para la codificación y descodificación propiamente dichas:

• para los parámetros k = 512, $\eta = 0{,}125$, se puede utilizar:

- un código lineal parametrado por el trío [80, 27, 21], capaz de corregir 10 errores, con valor 21 para el parámetro de expansión σ;

- un código lineal parametrado por el trío [160, 42, 42], capaz de corregir 20 errores, con valor 16 para el factor de expansión σ.

• para los parámetros k = 768, $\eta = 0{,}05$, se puede utilizar:

- un código lineal parametrado por el trío [80, 53, 9], capaz de corregir 4 errores, con valor 16 para el parámetro de expansión σ.

- un código lineal parametrado por el trío [160, 99, 17], capaz de corregir 8 errores, con valor 8,8 para el factor de expansión σ.

Para optimizar el factor de expansión σ, es deseable por lo tanto utilizar un tamaño k grande para el vector aleatorio, una probabilidad η para cada bit del vector de ruido ε de valer 1 débil, y un código de gran longitud n y de gran dimensión r. Se puede asimismo disminuir el factor de expansión σ aumentando el tamaño de la matriz M. En efecto, tomando una matriz con k líneas y N * n columnas, con N entero estrictamente superior a 2, se puede cifrar N bloques de r bits al mismo tiempo, con el mismo vector aleatorio de k bits. El factor de expansión solo es entonces $\sigma = \frac{N*n+k}{N*r}$.

A continuación, se describe el procedimiento de conversión según un modo de realización de la invención, en relación con la figura 2.

Una entidad de conversión, con referencia 3, es capaz de aplicar el procedimiento de conversión según la invención. La entidad 3 se comunica con al menos una primera entidad, con referencia 1, y con una segunda entidad, con referencia 2. La entidad de conversión 3 se comunica con las entidades 1 y 2 por ejemplo por medio de una red. La primera entidad 1 es comparable con una entidad de cifrado adecuada para aplicar el procedimiento de cifrado probabilista simétrico descrito en relación con la figura 1a. Posee una clave secreta que puede estar representada en forma de una matriz M_1 de k líneas y n columnas, con $1 \leq k$ y $1 \leq n$. La segunda entidad 2 está adaptada para aplicar el procedimiento de descifrado descrito en relación con la figura 1b. La segunda entidad posee una segunda clave secreta que puede estar representada en forma de una segunda matriz M_2 de k líneas y n columnas. La invención descrita aquí tiene interés en caso de que las matrices secretas M_1 y M_2 de la primera y segunda entidad 1, 2 sean distintas, es decir en caso de que las entidades 1 y 2 no compartan una matriz secreta. En caso de que la primera y la segunda entidad compartan el conocimiento de una misma clave secreta representada por una matriz M, se aplican los procedimientos de cifrado y descifrado descritos en relación con las figuras 1a y 1b, por parte de la primera entidad, como entidad de cifrado, y por parte de la segunda entidad como entidad de descifrado. Las dos entidades utilizan entonces la misma matriz secreta.

Se supone que se desea proceder a la conversión de un mensaje en abierto x de r bits cifrado por la primera entidad 1 mediante cifrado probabilista simétrico por medio de su matriz secreta M_1, en un segundo mensaje cifrado a la atención de la segunda entidad 2. Dicho de otro modo, se desea que el segundo mensaje cifrado pueda ser descifrado por la segunda entidad 2 por medio de su matriz secreta M_2 y que el descifrado del segundo mensaje cifrado permita a la segunda entidad 2 obtener el mensaje en abierto x.

En una etapa previa E19 de cálculo del primer cifrado, la primera entidad 1 procede al cifrado del mensaje en abierto x de r bits, conforme al procedimiento de cifrado probabilista simétrico descrito en relación con la figura 1a. Al efecto, la entidad 1 codifica el mensaje x por medio de un código corrector de errores C de longitud m, de dimensión r y de

capacidad de corrección t. Se recuerda que si se añade a C(x) un número de errores inferior a t, el procedimiento de descodificación recupera el mensaje en abierto x. La entidad 1 obtiene asimismo un vector aleatorio a de k bits de una fuente S no representada en la figura 2, y un vector de ruido ε de n bits producido por una fuente B no representada en la figura 2. La entidad 1 calcula entonces el primer cifrado y_1 mediante cifrado de la palabra de código C(x) por medio de la matriz secreta M_1 parametrada mediante el vector aleatorio a, y añadiendo el ruido ε al valor obtenido. Dicho de otro modo, la primera entidad calcula $y_1 = C(x) \oplus a.M_1 \oplus \varepsilon$.

En una etapa E20 de envío del primer cifrado, la primera entidad 1 envía a la entidad de conversión 3 el primer cifrado y_1, acoplado al vector aleatorio a.

En una etapa de recepción E21, la unidad de conversión 3 recibe de la primera entidad 1 el primer mensaje cifrado acoplado al vector aleatorio (y_1, a).

En una etapa E22 de cálculo del segundo cifrado, la entidad de conversión 3 calcula un segundo cifrado y_2 destinado a ser descifrado por la segunda entidad 2 por medio de su matriz secreta M_2. La entidad de conversión 3 extrae el vector aleatorio a del par recibido. El segundo cifrado y_2 se calcula añadiendo al primer cifrado y_1 el producto entre el vector aleatorio a, en forma de vector línea de k bits, con una matriz de conversión M_{12} que representa una clave secreta propia de la entidad de conversión 3. Dicho de otro modo, $y_2 = y_1 \oplus a \cdot M_{12}$. El papel de esta etapa E21 es cifrar el primer cifrado y_1. Se habla habitualmente de transcifrado para esta operación consistente en cifrar un valor ya cifrado. La matriz de conversión M_{12} es memorizada por la entidad de conversión 3 en una memoria no representada en la figura 2. La matriz de conversión M_{12} ha sido previamente calculada, por ejemplo, por una entidad de confianza no representada en la figura 2, a la que la primera y la segunda entidad han transmitido su clave secreta respectiva. La matriz de conversión M_{12} es calculada por la entidad de confianza añadiendo la matriz M_1 de la primera entidad 1 a la matriz M_2 de la segunda entidad 2. De este modo, $M_{12} = M_1 \oplus M_2$, donde $\oplus$ representa una suma bit a bit, o una operación de O EXCLUSIVO.

En una etapa E23 de envío, la entidad de conversión 3 envía a la segunda entidad 2 el segundo cifrado acoplado al vector aleatorio a (y_2, a).

De este modo, la segunda entidad 2 recibe, en una etapa E24 de recepción, el par (y_2, a), donde el segundo cifrado y_2 corresponde al cifrado de y_1 por medio de la matriz de conversión parametrada por el vector aleatorio a. Dicho de otro modo, $y_2 = y_1 \oplus a \cdot M_{12}$. Ahora bien, el primer cifrado y_1 se ha obtenido mediante cifrado probabilista simétrico del mensaje en abierto x por medio de la primera matriz secreta M_1 parametrada por el vector aleatorio a. De este modo, $y_1 = C(x) \oplus a \cdot M_1 \oplus \varepsilon$. Sabiendo además que la matriz de conversión M_{12} se ha obtenido a partir de la primera y la segunda matriz secreta M_1 y M_2 mediante una operación de O EXCLUSIVO, por lo que se verifica que:

$$y_2 = y_1 \oplus a \cdot M_{12} = C(x) \oplus a \cdot M_1 \oplus \varepsilon \oplus a \cdot M_1 \oplus a \cdot M_2 = C(x) \oplus a \cdot M_2 \oplus \varepsilon,$$

por lo que y_2 corresponde bien al cifrado probabilista simétrico del mensaje en abierto x por medio de la segunda matriz secreta M_2 parametrada mediante el vector aleatorio a. Por lo tanto, la segunda entidad 2 es capaz de descifrar el segundo cifrado y_2 por medio de su matriz secreta M_2, conforme al procedimiento de descifrado descrito en relación con la figura 1b, y de obtener el mensaje en abierto x.

En una etapa E25 de descifrado, la segunda entidad 2 extrae el vector aleatorio a del par recibido, y añade al segundo cifrado y_2 el resultado del producto entre el vector aleatorio a y la segunda matriz secreta M_2. En binario, esta operación corresponde a restar el resultado del producto $a \cdot M_2$ del vector y_2 recibido. Se observa que siendo y_2 igual a la palabra de código cifrada y con ruido, es decir $C(x) \oplus a \cdot M_2 \oplus \varepsilon$, el resultado de esta operación corresponde a la palabra de código únicamente con ruido, es decir $C(x) \oplus \varepsilon$. El resultado obtenido se descodifica a continuación con la ayuda del código corrector de errores C utilizado por la entidad 1 durante la etapa E19 de cifrado. El peso de Hamming del vector de ruido ε siendo inferior o igual a la capacidad de corrección t del código corrector de errores, la descodificación proporciona directamente el mensaje en abierto x.

En otro modo de realización de la invención, la matriz de conversión M_{12} es calculada por la primera entidad 1 o la segunda entidad 2. Por ejemplo, la primera y la segunda entidad 1, 2 se ponen de acuerdo para que la entidad 1 calcule la matriz de conversión M_{12} a partir de la primera matriz secreta M_1 que posee y de la segunda matriz secreta M_2 que le transmite la segunda entidad 2.

El procedimiento de conversión se describe aquí con una entidad de conversión 3 y dos entidades que se califica de terminales: una primera entidad 1 que cifra un mensaje en abierto x y una segunda entidad 2 que descifra el segundo cifrado y_2 calculado por la entidad de conversión 3 para obtener el mensaje en abierto x. Por supuesto, el procedimiento puede aplicarse para n entidades terminales, con $n > 2$. En este caso, serán n entidades anotadas 1, 2, …, n. Se calcula entonces (n-1) matrices de conversión M_{12}, M_{23}, M_{34}, …, M_{n-1n} que se transmiten a la entidad de conversión 3. Se observa en efecto que no es necesario calcular todas las matrices de conversión propias de todas las parejas de entidades (i, j). Por una parte, se observa el carácter simétrico de las matrices de conversión. En efecto, para un primer par de entidades (i, j), la matriz de conversión asociada M_{ij} es igual a la matriz de conversión

M_{ji} asociada al par de entidades (j, i). Por otra parte, es posible obtener una matriz de conversión para una pareja (i, j) con j>i+1, a partir de las matrices calculadas. En efecto, se observa que $M_{ij} = M_{i(i+1)} \oplus \ldots \oplus M_{(i+(j-i-1))j}$. Por ejemplo, $M_{13} = M_{12} \oplus M_{23}$.

A continuación, se describe la entidad de conversión 3 en relación con la figura 3.

La entidad de conversión 3 incluye una memoria 31 de almacenamiento de una clave secreta de conversión en forma de una matriz secreta M_{12}, un módulo de cálculo 32 de un segundo cifrado a partir de un primer cifrado. El módulo de cálculo 32 tiene acceso a la memoria 31.

La entidad de conversión incluye además:

- una unidad de procesamiento 33, o “CPU” (del inglés “Control Processing Unit”),

- una memoria volátil 34 o “RAM” (para “Random Access Memory) empleada para cargar instrucciones de código, ejecutarlas, almacenar variables, etc.

En funcionamiento, se proporciona un primer cifrado y_1 (no representado en la figura 3) a la entrada del módulo de cálculo 32, que produce a la salida un segundo cifrado y_2 (no representado en la figura 3).

La memoria 31 está destinada a almacenar la matriz secreta M_{12} utilizada para calcular el segundo cifrado y_2 a partir del primer cifrado y_1. La matriz secreta M_{12} se calcula previamente a partir de las matrices secretas M_1 y M_2 de las entidades. Las matrices M_1 y M_2 son por ejemplo matrices de Toeplitz. Por definición, se trata de matrices cuyos coeficientes en una diagonal descendiente de izquierda a derecha son las mismas. Por lo tanto, la matriz de conversión M_{12} obtenida a partir de las dos matrices secretas de las entidades mediante un O EXCLUSIVO entre estas dos matrices es asimismo una matriz de Toeplitz. De este modo, el conjunto de coeficientes de la matriz de conversión M_{12} pueden deducirse únicamente de los coeficientes de la primera línea y de la primera columna de la matriz. Asimismo, es suficiente con almacenar únicamente los coeficientes de la primera línea y la primera columna de la matriz de conversión para disponer del conjunto de coeficientes de la matriz de conversión.

Por lo tanto, la memoria 31 puede almacenar únicamente los coeficientes de la primera línea y los coeficientes de la primera columna de la matriz de conversión M_{12}. La utilización de la matriz de Toeplitz permite limitar la capacidad de almacenamiento necesaria para almacenar los coeficientes de la matriz de conversión M_{12}.

El módulo de cálculo 32 está adaptado para:

- calcular el producto del vector aleatorio a tomado en forma de un vector línea de k bits, con la matriz secreta M_{12}, es decir el producto $a \cdot M_{12}$,

- añadir el primer cifrado y_1 recibido a la entrada del módulo al resultado del producto $a \cdot M_{12}$.

El módulo de cálculo proporciona por lo tanto a la salida el cifrado de y_1 por medio de la matriz de conversión M_{12}, es decir $y_1 \oplus a \cdot M_{12}$.

Los distintos módulos se comunican gracias a un bus de comunicación.

El módulo de cálculo 32 aplica la etapa E22 de cálculo del segundo cifrado.

En un modo particular de realización de la inversión, la entidad de conversión 3 incluye asimismo:

- un módulo 35 de recepción (en trazo discontinuo en la figura 3), adaptado para recibir de una primera entidad el primer cifrado y_1,

- un módulo 36 de emisión (en trazo discontinuo en la figura 3), adaptado para enviar a una segunda entidad el segundo cifrado y_2 obtenido a la salida del módulo de cálculo 32.

En este ejemplo de realización, el módulo 35 de recepción está conectado de entrada al módulo de cálculo 32, el cual está conectado de salida al módulo 36 de emisión.

El módulo 35 de recepción aplica la etapa E21 de recepción.

El módulo 36 de emisión aplica la etapa E23 de emisión.

En un ejemplo de realización, en el que la entidad de conversión 3 recibe la matriz de conversión M_{12}, el módulo 35 de recepción está asimismo adaptado para recibir de una entidad tercera la matriz de conversión M_{12} y memorizarla en la memoria 31.

Los módulos 32, 34 y 35 son preferiblemente módulos de software que incluyen instrucciones de software para ejecutar las etapas del procedimiento de la invención.

Pueden almacenarse en un mismo ordenador de una red o en ordenadores distintos que garantizan las funciones de la entidad de conversión.

Por lo tanto, la invención se refiere asimismo:

- a programas de ordenador que incluyen instrucciones para la aplicación del procedimiento de conversión, cuando dichos programas son ejecutados por un procesador;

- a un soporte de grabación legible por un ordenador, en el que está grabado el programa de ordenador descrito anteriormente.

Los módulos de software pueden almacenarse en o transmitirse mediante un soporte de datos. Este puede ser un soporte material de almacenamiento, por ejemplo un CD-ROM, un disquete magnético o un disco duro, o bien un soporte de transmisión como una señal o una red de telecomunicaciones.

REIVINDICACIONES

1. Procedimiento de conversión, mediante una entidad de conversión, de un primer cifrado (y_1) en un segundo cifrado (y_2), correspondiendo el primer cifrado al resultado de un cifrado probabilista simétrico de un elemento de mensaje en abierto (x) por medio de una primera matriz secreta (M_1) parametrada mediante un vector aleatorio (a), correspondiendo el segundo cifrado (y_2) al resultado de un cifrado probabilista simétrico del elemento de mensaje en abierto por medio de una segunda matriz secreta (M_2) parametrada mediante el vector aleatorio, caracterizado por el hecho de que el procedimiento incluye una etapa de:

- cálculo (E22) del segundo cifrado (y_2) mediante cifrado del primer cifrado por medio de una matriz secreta de conversión (M_{12}) en función de la primera y la segunda matriz secreta, y parametrada mediante el vector aleatorio (a).

2. Procedimiento de conversión según la reivindicación 1, que incluye una etapa de:

- recepción (E21) del primer cifrado (y_1) acoplado al vector aleatorio (a) procedente de una primera entidad (1),

- envío (E23) del segundo cifrado (y_2) acoplado al vector aleatorio (a) con destino a una segunda entidad (2).

3. Procedimiento según la reivindicación 1, en el que la matriz secreta de conversión (M_{12}) se calcula mediante una operación de O EXCLUSIVO entre la primera y la segunda matriz secreta ($M_1 \oplus M_2$).

4. Procedimiento según la reivindicación 1, en el que la matriz de conversión (M12) es una matriz de Toeplitz.

5. Procedimiento según la reivindicación 2, en el que la matriz de conversión se obtiene por parte de la entidad de conversión ante una entidad de confianza que calcula la matriz de conversión por medio de la primera y la segunda matriz secreta transmitidas por la primera y la segunda entidad respectivamente.

6. Procedimiento de transmisión de un elemento de mensaje en abierto (x) en forma cifrada entre una primera y una segunda entidad, que incluye una etapa de:

- cifrado (E19) por parte de la primera entidad por medio de un cifrado probabilista simétrico del mensaje en abierto, por medio de una primera matriz secreta (M_1), parametrada mediante un vector aleatorio (a), con objeto de obtener un primer cifrado (y_1),

- envío (E20) del primer cifrado acoplado al vector aleatorio, a una entidad de conversión,

- conversión (E22) por la entidad de conversión del primer cifrado (y_1) en un segundo cifrado (y_2) según el procedimiento definido en la reivindicación 1,

- envío (E23) por parte de la entidad de conversión a la segunda entidad del segundo cifrado acoplado al vector aleatorio,

- recepción (E24) por la segunda entidad del segundo cifrado acoplado al vector aleatorio,

- descifrado (E25) por la segunda entidad del segundo cifrado (y_2) por medio de una segunda matriz secreta (M_2) mediante descifrado probabilista simétrico.

7. Entidad de conversión (3) adecuada para convertir un primer cifrado en un segundo cifrado, correspondiendo el primer cifrado al resultado de un cifrado probabilista simétrico de un elemento de mensaje en abierto (x) por medio de una primera matriz secreta (M_1) parametrada mediante un vector aleatorio (a), correspondiendo el segundo cifrado (y_2) al resultado de un cifrado probabilista simétrico del elemento de mensaje en abierto por medio de una segunda matriz secreta (M_2) parametrada mediante el vector aleatorio, incluyendo la entidad de conversión:

- medios (32) de cálculo del segundo cifrado, adecuados para calcular el segundo cifrado mediante cifrado del primer cifrado recibido por medio de una matriz secreta de conversión (M_{12}) en función de la primera y la segunda matriz secreta, y parametrada mediante el vector aleatorio (a).

8. Entidad de conversión según la reivindicación 7, que incluye, además:

- medios (35) de recepción adaptados para recibir el primer cifrado acoplado a un vector aleatorio (a),

- medios (36) de envío adaptados para enviar el segundo cifrado (y_2) acoplado al vector aleatorio (a).

9. Sistema de conversión adecuado para convertir un primer cifrado en un segundo cifrado, correspondiendo el primer cifrado al resultado de un cifrado probabilista simétrico de un elemento de mensaje en abierto (x) por medio

de una primera matriz secreta (M_1) parametrada mediante un vector aleatorio (a), correspondiendo el segundo cifrado (y_2) al resultado de un cifrado probabilista simétrico del elemento de mensaje en abierto por medio de una segunda matriz secreta (M_2) parametrada mediante el vector aleatorio, incluyendo el sistema:

- una entidad de conversión según la reivindicación 7,

- una entidad de confianza adecuada para calcular la matriz de conversión (M_{12}) a partir de las matrices secretas (M_1, M_2).

10. Programa de ordenador destinado a ser instalado en una memoria de una entidad intermediaria, que incluye instrucciones para la aplicación de las etapas del procedimiento de conversión según una de las reivindicaciones 1 a 5, cuando el programa se ejecuta mediante un procesador.

11. Soporte de datos en el que se graba el programa de ordenador según la reivindicación 10.

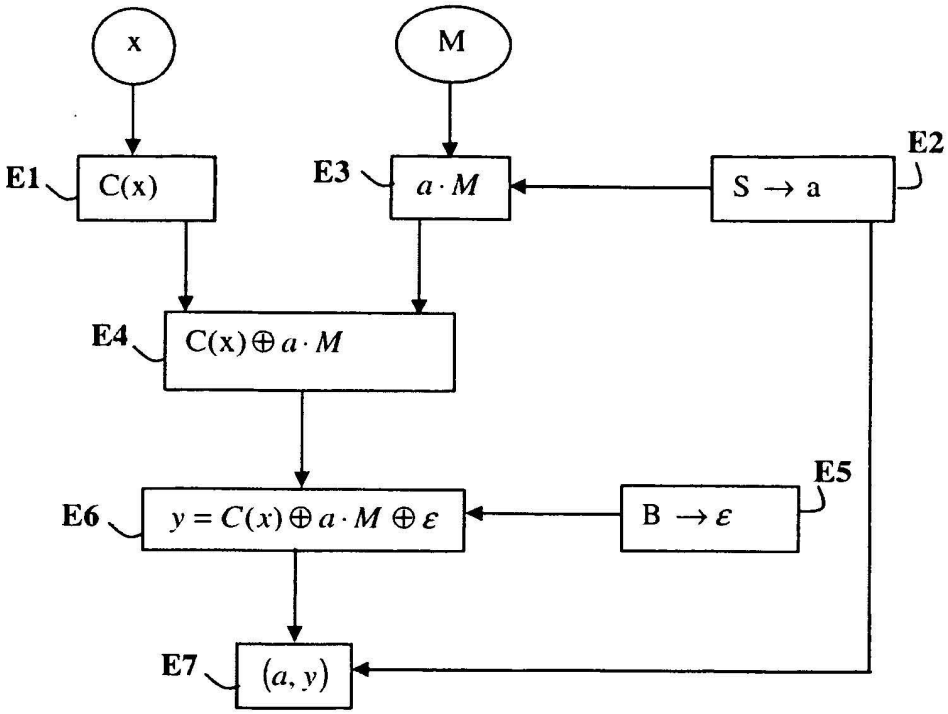

Figura 1a

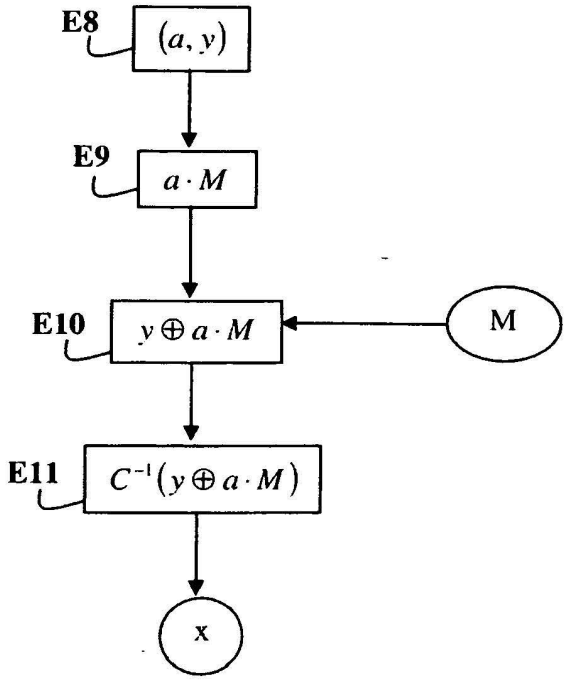

Figura 1b

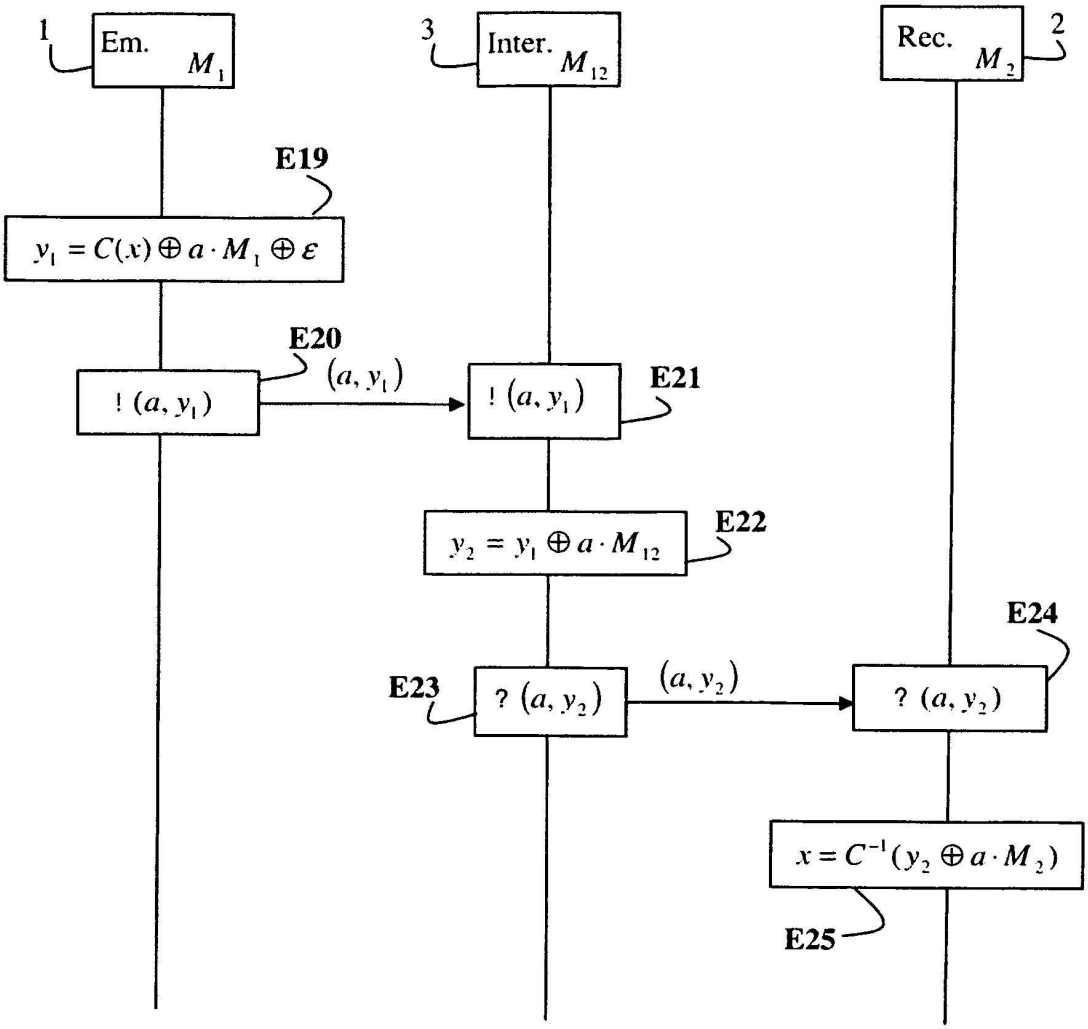

Figura 2

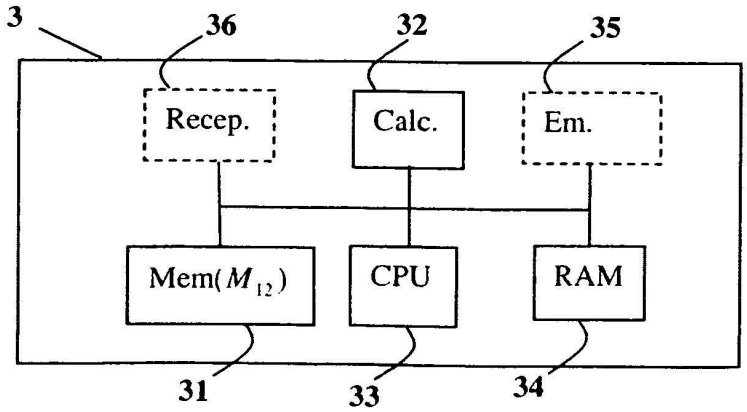

Figura 3