(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 696 513**

(51) Int. CI.:

H04L 9/00 (2006.01)
H04L 9/08 (2006.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **06.09.2010 E 10175467 (9)**

(97) Fecha y número de publicación de la concesión europea: **15.08.2018 EP 2317689**

(54) Título: **Sistema criptográfico para realizar cálculos y procesamiento de señales seguros directamente en datos encriptados en entornos no confiables**

(30) Prioridad:

04.09.2009 US 240177 P
04.09.2009 US 240179 P
04.09.2009 US 240181 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.01.2019

(73) Titular/es:

GRADIANT-CENTRO TECNOLOXICO DE TELECOMUNICACIÓNS DE GALICIA (100.0%)
Lagoas Marcosende s/n
36310 Vigo, ES

(72) Inventor/es:

TRONCOSO PASTORIZA, JUAN RAMON;
COMESAÑA ALFARO, PEDRO y
PÉREZ GONZÁLEZ, FERNANDO

(74) Agente/Representante:

CONTRERAS PÉREZ, Yahel

DESCRIPCIÓN

Sistema criptográfico para realizar cálculos y procesamiento de señales seguros directamente en datos encriptados en entornos no confiables

CAMPO TÉCNICO

Las formas de realización divulgadas se refieren a procedimientos y sistemas de criptografía. Específicamente, se relacionan con sistemas criptográficos para la ejecución de operaciones directamente en datos encriptados.

ANTECEDENTES

En la sociedad moderna, los datos digitales sobre individuos se pueden encontrar de manera relativamente fácil en las redes de comunicación, especialmente en Internet. Aunque el público respalda los avances de las últimas décadas en las redes digitales, la naturaleza sensible de estos datos motiva el aumento de una preocupación creciente sobre la disponibilidad pública de datos personales y el procesamiento realizado en los mismos. Por ejemplo, en Europa, esta preocupación se ha reflejado en una serie de Directivas que tratan de la protección de los datos personales de las personas. La Directiva 95/46/CE se refiere a la protección de las personas con respecto al tratamiento de datos personales y la libre circulación de dichos datos, siendo los datos personales cualquier información relacionada con una persona física identificada o identificable. Una de las ideas principales de esta Directiva es que los sistemas de procesamiento de datos deben respetar los derechos y libertades fundamentales, especialmente el derecho a la privacidad. Se han propuesto leyes y directivas similares con respecto a la privacidad de la información en los EE.UU y en otros países desarrollados. Éstas incluyen privacidad en Internet, privacidad médica, privacidad financiera, privacidad en la aplicación de la ley y privacidad política.

Actualmente hay numerosos procedimientos disponibles para proporcionar seguridad en una base de datos que contiene datos destinados a mantenerse privados con respecto a terceros. Este problema se resuelve mediante procedimientos de autenticación segura. Estos procedimientos se utilizan ampliamente para proteger la seguridad de bases de datos que contienen datos médicos, financieros y de otro tipo. Se puede añadir un nivel adicional de seguridad mediante la encriptación de todos los datos contenidos en la base de datos segura y transmitidos desde y hacia la base de datos segura durante operaciones de carga/subida o descarga/bajada. Esto es especialmente útil cuando los datos se deben transmitir a través de un medio potencialmente inseguro, tal como las redes informáticas. Sin embargo, incluso en estos sistemas de seguridad aumentada, en algún momento los datos encriptados son des-encriptados por un usuario autorizado para realizar las tareas necesarias de análisis de datos. Por ejemplo, en el caso de la investigación médica, el sistema de gestión segura de datos clínicos que contiene los datos clínicos encriptados y series temporales fisiológicas correspondientes a un estudio, investigación o ensayo clínico en particular requieren que el investigador autorizado des-encripte los datos para realizar el análisis matemático, procesamiento de señales y análisis estadístico necesarios con el fin de generar los resultados del estudio. Existen situaciones en las que este escenario convencional no cumple con los requisitos de seguridad, es decir, para analizar y procesar los datos encriptados, dichos datos no deberían ser des-encriptados en primera instancia (es decir, los datos se deben mantener encriptados en todo momento). Hay situaciones en las que los datos deben ser completamente privados, incluso para los investigadores, los administradores clínicos y los administradores del sistema. Esto se puede deber a razones puramente de privacidad o a consideraciones de investigación. Por ejemplo, ciertos estudios pueden requerir que los científicos e investigadores no puedan ver en absoluto los datos y que las hipótesis y los procedimientos de análisis sean seleccionados a priori. Con el fin de conseguir esto, se necesitan procedimientos para realizar operaciones y cálculos matemáticos típicos que incluyen técnicas de análisis estadístico, procedimientos algebraicos, procedimientos de procesamiento de señales y otras operaciones de cálculo directamente en los conjuntos de datos encriptados. Actualmente, la disponibilidad de dichos procedimientos seguros y sistemas criptográficos es limitada.

Los protocolos criptográficos convencionales tratan el problema de proteger cierta información privada con respecto a una tercera parte no autorizada que de otro modo podría modificar o tener acceso a la información. En el escenario de procesamiento seguro, en el que la privacidad se debe preservar no solo contra un tercero no autorizado, sino también contra las partes que procesan los datos, no hay sistemas o procedimientos disponibles que se puedan usar en escenarios del mundo real en términos tanto de coste de cálculo como de complejidad de comunicación.

Hasta ahora, los protocolos eficientes presentados en el campo del procesamiento de señales en el dominio encriptado se han enfocado a operaciones lineales, como productos escalares y algoritmos no iterativos. Sin embargo, hay muchos algoritmos básicos necesarios para la mayoría de las aplicaciones de procesamiento de señales que son iterativas e involucran no solo productos escalares con valores conocidos, sino también productos entre dos secuencias desconocidas a priori. La ausencia de estos algoritmos supone la falta de una herramienta potente e irremplazable que permita casi cualquier aplicación de procesamiento de señales y la mayoría de tipos de procedimientos de análisis.

Actualmente no existe un sistema criptográfico práctico totalmente homomórfico, es decir, no existe un sistema criptográfico seguro que permita el cálculo homomórfico de adiciones y productos sin restricciones. Ha habido una contribución reciente de Gentry que presenta un sistema criptográfico basado en estructuras ideales (ideal lattices) con des-encriptación arrancable (bootstrappable), y se ha demostrado que consigue un homomorfismo completo. Sin embargo, los autores de este procedimiento admiten que hacer que el esquema sea práctico sigue siendo un problema abierto.

Por el momento no hay ningún sistema criptográfico disponible que sea capaz de realizar cálculos como resolver sistemas de ecuaciones lineales sin imponer ninguna restricción a los coeficientes de la matriz. Estos sistemas criptográficos son un elemento de desarrollo fundamental necesario para desarrollar e implementar sistemas criptográficos más complejos capaces de realizar un procesamiento de señales, cálculos y análisis avanzados directamente en datos encriptados.

RESUMEN

Los anteriores y otros objetos se consiguen por medio del conjunto de reivindicaciones adjunto.

Según una forma de realización, el sistema propuesto involucra un sistema criptográfico (o criptosistema) para la ejecución de operaciones directamente en datos encriptados, es decir, un sistema diseñado para abordar el problema del procesamiento eficiente de señales en entornos no confiables, en el que no solo el canal de comunicación entre las partes no es seguro, sino que tampoco se puede confiar en las partes que realizan el cálculo.

Las formas de realización divulgadas incluyen un sistema criptográfico implementado en al menos un sistema informático digital con uno o más procesadores o hardware tales como FPGA para realizar cálculos, análisis y procesamiento de señales seguros directamente en datos encriptados en entornos no confiables. Según una forma de realización básica, el sistema criptográfico propuesto comprende: (a) al menos un protocolo seguro para realizar multiplicaciones de matrices en el dominio encriptado, y (b) al menos un protocolo seguro para resolver sistemas de ecuaciones lineales en el dominio encriptado. De acuerdo con una forma de realización particular, y sin limitación alguna, el sistema comprende una pluralidad de protocolos de preservación de la privacidad para resolver sistemas de ecuaciones lineales (SLE) basados directamente en cálculo homomórfico y compartición de secretos. Más específicamente, de acuerdo con una forma de realización particular, y sin limitación alguna, el sistema usa un protocolo en el que se resuelven sistemas de ecuaciones lineales de forma segura mediante eliminación directa de Gauss usando un protocolo seguro sin imponer ninguna restricción a los coeficientes de la matriz. En una forma de realización alternativa, el sistema usa un protocolo con el que se resuelven sistemas de ecuaciones lineales de forma segura e iterativa sin imponer ninguna restricción a los coeficientes de la matriz. Alternativamente, de acuerdo con otra forma de realización, el sistema usa un protocolo iterativo seguro con el que se resuelven sistemas de ecuaciones lineales e inversiones de matriz de forma segura e iterativa sin imponer ninguna restricción a los coeficientes de la matriz en base a un protocolo iterativo sustancialmente equivalente a un protocolo seguro de Newton.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Se ilustran formas de realización divulgadas a modo de ejemplo, y no a modo de limitación, en las figuras de los dibujos adjuntos.

La figura 1 muestra un diagrama de bloques para ilustrar el sistema criptográfico de acuerdo con una forma de realización.

La figura 2 muestra un diagrama de bloques de alto nivel para ilustrar la operación del sistema criptográfico.

La figura 3 muestra un diagrama de bloques para ilustrar el protocolo seguro para resolver sistemas de ecuaciones lineales en el dominio encriptado de acuerdo con una forma de realización.

La figura 4 muestra un diagrama de bloques para ilustrar el protocolo seguro para resolver sistemas de ecuaciones lineales en el dominio encriptado de acuerdo con una forma de realización.

La figura 5 muestra un diagrama de bloques para ilustrar el protocolo seguro para resolver sistemas de ecuaciones lineales en el dominio encriptado de acuerdo con una forma de realización.

DESCRIPCIÓN DETALLADA

La figura 1 muestra un diagrama de bloques del sistema criptográfico 102 de acuerdo con una forma de realización. Las formas de realización divulgadas describen cómo realizar un sistema criptográfico 102 para realizar cálculos matemáticos, procesamiento de señales, procesamiento estadístico de señales, estadísticas y análisis de datos seguros directamente en datos encriptados 100 en entornos no confiables. Según una forma de realización, el sistema involucra un sistema criptográfico 102 para la ejecución de operaciones directamente sobre datos

encriptados 100, es decir, un sistema diseñado para abordar el problema del procesamiento eficiente de señales en entornos no confiables, en el que no solo el canal de comunicación entre partes es inseguro, sino que tampoco se puede confiar en las partes que realizan el cálculo.

En la siguiente descripción y figuras se exponen ciertos detalles específicos para proporcionar una comprensión exhaustiva de las diversas formas de realización divulgadas. Ciertos detalles bien conocidos a menudo asociados con la informática y la tecnología de software no se exponen en la siguiente descripción para evitar oscurecer innecesariamente las diversas formas de realización divulgadas. Además, los expertos en la materia entenderán que pueden poner en práctica otras formas de realización sin uno o más de los detalles descritos a continuación. Aspectos de las formas de realización divulgadas se pueden implementar en el contexto general de instrucciones ejecutables por un sistema informático, tales como módulos de programa, que se ejecutan en un sistema informático, un servidor informático o un dispositivo que contiene un procesador. En general, los módulos o protocolos de programa incluyen rutinas, programas, objetos, componentes, estructuras de datos, etc. que realizan tareas particulares o implementan tipos de datos abstractos particulares. Aspectos de las formas de realización divulgadas también se pueden poner en práctica en entornos informáticos distribuidos en los que las tareas son realizadas por dispositivos de procesamiento remotos que están conectados a través de una red de comunicaciones. En un entorno informático distribuido, los módulos de programa se pueden ubicar en medios de almacenamiento locales y/o remotos que incluyen dispositivos de almacenamiento de memoria. Los expertos en la técnica apreciarán que, dada la descripción de los módulos que comprende las formas de realización divulgadas proporcionadas en esta especificación, es una cuestión rutinaria proporcionar sistemas de trabajo que funcionarán en una diversidad de tecnologías conocidas y comúnmente disponibles capaces de incorporar las características descritas en este documento.

Según una forma de realización divulgada, el sistema criptográfico 102 es implementado en un sistema informático digital con uno o más procesadores para realizar cálculos y procesamiento de señales seguros directamente en datos encriptados 100 en entornos no confiables, comprendiendo dicho sistema criptográfico 102: (a) al menos un protocolo seguro para realizar multiplicaciones de matrices en el dominio encriptado 104, y (b) al menos un protocolo seguro para resolver sistemas de ecuaciones lineales en el dominio encriptado 106. De acuerdo con una forma de realización particular, y sin limitación alguna, el sistema usa un protocolo en el que se resuelven sistemas de ecuaciones lineales de forma segura mediante eliminación directa de Gauss usando un protocolo seguro de multiplicación para generar directamente los resultados 112 de dichos cálculos matemáticos, procesamiento de señales, procesamiento estadístico de señales, estadísticas y análisis de datos seguros directamente en datos encriptados 100 en entornos no confiables. De acuerdo con otras formas de realización, el sistema criptográfico divulgado puede ser implementado en otro hardware además de un sistema informático digital que incluye microcontroladores, DSP, FPGA o ASIC, así como en firmware y software.

Las formas de realización divulgadas del sistema criptográfico 102 y protocolos de seguridad asociados tienen una utilidad específica y sustancial por sí mismas como sistemas y procedimientos para criptografía y cálculo seguro (encriptado), sino también en una diversidad de aplicaciones prácticas en diversos campos, que incluyen sistemas de gestión segura de datos clínicos, plataformas seguras habilitadas para entornos web para una colaboración que incluye datos de privacidad, sistemas seguros de aplicación de la ley, sistemas financieros seguros y sistemas militares seguros que implican la transmisión de datos encriptados para su procesamiento en tiempo real sin ser des-encriptados.

Según una forma de realización básica, el sistema criptográfico propuesto 102 comprende: (a) al menos un protocolo seguro para realizar multiplicaciones de matrices en el dominio encriptado 104, y (b) al menos un protocolo seguro para resolver sistemas de ecuaciones lineales en el dominio encriptado 106 en el que se resuelven sistemas de ecuaciones lineales de forma segura mediante eliminación directa de Gauss utilizando un protocolo seguro de multiplicación basado en cálculo homomórfico 108 y compartición de secretos 110 sin poner ninguna restricción sobre la naturaleza de los coeficientes de la matriz (es decir, los coeficientes de la matriz pueden ser números reales o números complejos).

A modo de ejemplo, y no a modo de limitación, las formas de realización del sistema criptográfico 102 divulgado se pueden usar para realizar análisis y procesamiento directos en datos clínicos, financieros, de seguridad nacional, militares, de cumplimiento de la ley y políticos encriptados sin la necesidad de des-encriptar dichos datos antes de realizar dicho análisis y procesamiento. Por ejemplo, según una forma de realización, el sistema criptográfico 102 divulgado se puede usar para realizar e implementar un sistema clínico seguro en el que todos los datos de pacientes, historia clínica, datos clínicos, datos fisiológicos y series de tiempo, datos bioquímicos y datos de terapia farmacológica están encriptados en todo momento para transmisión, gestión y colaboración entre investigadores y médicos seguras; y todas las operaciones, procesamientos y análisis estadísticos realizados sobre dichos datos se realizan en el dominio encriptado (es decir, con los datos encriptados en todo momento). Una forma de realización particular específica de dicho sistema seguro de gestión y análisis de datos clínicos comprende (a) al menos un protocolo seguro para realizar multiplicaciones de matrices en el dominio encriptado 104, y (b) al menos un protocolo

seguro para resolver sistemas de ecuaciones lineales en el dominio encriptado 106 además de los elementos bien conocidos que comprenden sistemas de gestión clínica. De acuerdo con una forma de realización más específica, dicho protocolo para resolver sistemas de ecuaciones lineales en dicho sistema seguro de gestión de datos clínicos se basa en una implementación directa de la eliminación de Gauss que usa un protocolo seguro.

La figura 2 muestra un diagrama de alto nivel para ilustrar la operación del sistema criptográfico de acuerdo con una forma de realización. En la forma de realización ilustrada, y sin limitación alguna, hay dos partes A 200 y B 220. La primera parte tiene una matriz encriptada [**A**] y un vector encriptado [**b**], así como la clave para producir encriptaciones usando una encriptación homomórfica 202. La parte B posee tanto la clave de encriptación como la clave de des-encriptación 216 para la misma encriptación homomórfica. El sistema criptográfico se usa en ambos extremos 206 y 212 con el fin de resolver de forma privada el sistema lineal de ecuaciones **A** · **x = b**. Este sistema criptográfico comprende un protocolo de comunicación entre ambos extremos 208 y 214 que define las operaciones realizadas y el formato de los números intercambiados con el fin de resolver de forma interactiva el sistema sin revelar ninguna información. Esta comunicación tiene lugar sobre cualquier canal de comunicación 210 (por ejemplo, un medio alámbrico o inalámbrico o un solo dispositivo). Después de la ejecución del protocolo, el sistema envía la solución **x** 204 y 218 al sistema lineal de ecuaciones **A** · **x = b**. Es importante tener en cuenta que tanto A como B puede representar una pluralidad de partes o entidades (no necesariamente una sola entidad).

La multiplicación segura de matrices (transformaciones lineales) y la resolución de sistemas lineales de ecuaciones en el dominio encriptado son bloques de construcción matemáticos fundamentales para resolver una gran diversidad de problemas que incluyen análisis de datos, análisis de series de tiempo, procesamiento digital de señales, procesamiento estadístico de señales, filtrado óptimo, filtrado adaptativo, comunicaciones digitales, codificación, encriptación, teoría de la información y cualquier otro problema que implique el método de mínimos cuadrados y la representación de señales en espacios vectoriales.

Aunque se describen formas de realización particulares, se entiende que, después de aprender las enseñanzas contenidas en esta descripción, serán evidentes modificaciones y generalizaciones para los expertos en la técnica sin apartarse del alcance de las formas de realización divulgadas.

A. Notación matemática.

En la descripción detallada se utiliza la siguiente notación matemática. La notación matemática se describe detalladamente en esta sección para ayudar a los expertos en la técnica a comprender, implementar y poner en práctica las formas de realización divulgadas.

En la descripción usamos indistintamente letras minúsculas para representar clases en un anillo $(Z_n,+,\cdot)$ y un representante de esa clase en el intervalo [0,n). ⌈.⌋ representa la función de redondeo de un número al entero más cercano.

Los vectores usados tienen tamaño L y se representan con letras minúsculas en negrita, mientras que las matrices se representan con letras mayúsculas en negrita. **A'** = $\{ai,j\}_{r,s}^{t,u}$ representa la sub–matriz de **A** de tamaño (t–r+1) × (u–s+1), definida por $a'_{i,j} = a_{i+r-1,j+s-1}$.

La encriptación de un número x es representada por [x], y el vector (matriz) formado por las encriptaciones del vector x (matriz **X**) es representado por [**x**] ([**X**]).

Las operaciones realizadas entre números encriptados y en claro se indican como si se hubieran realizado en claro; por ejemplo [**X**] · **b** representa la encriptación de [**X** · **b**].

En cuanto a los cálculos de complejidad, la complejidad de operaciones modulares básicas, como adiciones (A), productos (P) y exponenciaciones (X) se denotan con $Comp_A$, $Comp_P$, $Comp_X$, respectivamente, con una E de prefijo (es decir, EA, EP, EX) cuando se realizan bajo encriptación. El factor ct < 1 denota la relación entre el tamaño de un valor de texto en claro y el de un valor encriptado. Finalmente, el subíndice cm denota la complejidad de la comunicación, medida según el número de encriptaciones enviadas, mientras que cp indica complejidad de cálculo, con una indicación de la parte cuya complejidad es representada.

B. Técnicas empleadas según una forma de realización.

De acuerdo con una forma de realización, el sistema criptográfico 102 usa técnicas seguras de cálculo multi–parte que incluyen encriptación homomórfica y compartición de secretos.

De acuerdo con una forma de realización, el sistema criptográfico 102 hace uso de homomorfismos entre los grupos de texto en claro y texto encriptado, que permiten la ejecución de una determinada operación directamente en

valores encriptados, sin la necesidad de des-encriptación. Esto incluye un sistema criptográfico homomórfico RSA, con un homomorfismo multiplicativo, o Paillier con un homomorfismo aditivo. Los procedimientos implementados no se restringen al uso de un sistema criptográfico para los protocolos presentados, en la medida en que presenta un homomorfismo aditivo. En esta forma de realización, el sistema 102 usa una extensión de la encriptación de Paillier en su forma de umbral y de no umbral; es decir, una k fuera del sistema de encriptación de clave pública de umbral M es un sistema criptográfico en el que la clave privada se distribuye entre M partes, y al menos k de ellas son necesarias para la des-encriptación.

De acuerdo con una forma de realización, el sistema criptográfico 102 usa la compartición de secretos. En esta forma de realización, se divide un determinado valor (el secreto) entre varias partes, de modo que la cooperación entre varias de estas partes es necesaria para recuperar el secreto. Ninguna de las partes sola puede tener acceso al secreto. De acuerdo con una forma de realización, el esquema se basa en polinomios y la necesidad de k puntos con el fin de determinar completamente un polinomio de grado (k – 1). La forma de realización descrita usa la compartición de secretos para protocolos entre dos partes basados en funciones lineales, sin limitación, ya que cada parte puede representar una pluralidad de entidades. De acuerdo con una forma de realización, el sistema soporta el cálculo de sumas y productos directamente sobre las partes de la siguiente manera: 1) supóngase que Z_n es el dominio de los secretos; 2) luego, se define una parte de un secreto x como dos valores x_A y x_B, que son propiedad de sus respectivas partes, de modo que $x_A+x_B \equiv x \bmod n$; 3) en lo sucesivo, aleatorizar un valor encriptado x significa obtener una parte compartida y proporcionar la encriptación de la otra (a través de la adición homomórfica).

C. Definiciones de protocolos y construcciones según una forma de realización.

De acuerdo con una forma de realización del sistema criptográfico 102, y sin limitación alguna, los protocolos se basan en dos partes, A y B, que usan ambas un sistema criptográfico homomórfico de forma aditiva en un escenario asimétrico, en el que A solo puede encriptar, pero B también posee la clave de des-encriptación, y puede realizar tanto encriptado como des-encriptado. Para el problema de resolver un sistema de ecuaciones lineales $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$, el sistema requiere que A posea una versión encriptada de la matriz del sistema [**A**], y del vector independiente [**b**].

De acuerdo con una forma de realización, y sin limitación alguna, el sistema de ecuaciones lineales puede tener **A** que es una matriz definida positiva o una matriz dominante estrictamente en diagonal. En este caso particular, se puede garantizar tanto una solución al sistema como la convergencia de los procedimientos estudiados, según se detalla más adelante.

Con respecto a los requisitos de privacidad, según una forma de realización, el sistema criptográfico 102 está especialmente adaptado para partes semi confiables, en el sentido de que se adhieren al protocolo establecido, pero pueden tener curiosidad acerca de la información que pueden obtener a partir de la interacción. En esta forma de realización, los protocolos se pueden demostrar como privados; informalmente, ambas partes A y B puede obtener solo la información filtrada de la solución al sistema, y no se filtra información de las etapas intermedias de los protocolos.

D. Motor y procedimiento de cálculo seguro para multiplicar matrices en el dominio encriptado.

Para multiplicar dos matrices encriptadas, puesto que no hay una operación de multiplicación en un sistema criptográfico homomórfico de forma aditiva, es necesario ejecutar un protocolo interactivo con el fin de realizar cada producto. De acuerdo con una forma de realización, los sistemas usan el siguiente procedimiento para la encriptación sin umbral.

De acuerdo con una forma de realización del protocolo seguro, y sin limitación alguna, se asume que existe un sistema criptográfico homomórfico de forma aditiva con texto plano en Z_n de modo que B puede des-encriptar y tanto A como B pueden encriptar. En esta forma de realización, A posee dos escalares encriptados [x1] y [x2] y quiere multiplicarlos bajo encriptación. Con el fin de hacer esto, según una forma de realización, A genera dos valores aleatorios r_1, $r_2 \in Z_n$, y los utiliza para ocultar ambos números, usando la suma homomórfica módulo-n que obtiene $[\mathbf{z}_1] = [\mathbf{x}_1]+r_1 \bmod n$, y $[\mathbf{z}_2] = [\mathbf{x}_2]+r_2 \bmod n$, y los envía a B.

De acuerdo con una forma de realización del procedimiento, debido a sus capacidades de des-encriptación, B puede obtener z_1 y z_2 en claro, multiplicarlos y re-encriptar el resultado $[z_1 \cdot z_2]$. B envía este producto encriptado a A, quien, a través de sumas homomórficas, puede obtener el resultado deseado, como

$$[\![x_1 \cdot x_2]\!] = [\![z_1 \cdot z_2]\!] - r_1 [\![x_2]\!] - r_2 [\![x_1]\!] - r_1 r_2.$$

De acuerdo con la forma de realización que involucra un sistema criptográfico homomórfico umbral, el procedimiento es análogo, con la excepción de que los valores aleatorios deben ser generados por ambas partes.

De acuerdo con la forma de realización que involucra un producto de una matriz L x M y un escalar, el protocolo es exactamente el mismo que en el caso de escalar–escalar, con L x M productos escalares en paralelo.

Según la forma de realización que involucra un producto matriz–matriz, todos los productos escalares se realizan usando el protocolo de producto escalar–escalar en paralelo, con solo una aleatorización por cada coeficiente de matriz, y las operaciones restantes son sumas, que se pueden realizar de forma homomórfica. De acuerdo con una forma de realización, con el fin de minimizar la complejidad de cálculo y comunicación, A puede dejar que B realice todas las adiciones parciales que B puede hacer en claro y A tendría que hacer de manera homomórfica.

Despreciando la complejidad de los algoritmos de generación de números aleatorios, la complejidad de todo el protocolo, cuando se multiplica una matriz L × M y una matriz M × N es

$$\mathrm{Comp}_{cmMULT}(L,M,N) = M\cdot(L+N) + L\cdot N$$

$$\mathrm{Comp}_{cpMULT,A}(L,M,N) = L\cdot N\cdot M\cdot(3\mathrm{Comp}_{EA} + 2\mathrm{Comp}_{EP})$$

$$\mathrm{Comp}_{cpMULT,B}(L,M,N) = M\cdot(L+N)\mathrm{Comp}_{Decrypt} + M\cdot L\cdot N\mathrm{Comp}_{P} + L\cdot N\cdot((M-1)\mathrm{Comp}_{A} + \mathrm{Comp}_{Encrypt}).$$

E. Motor y procedimiento de cálculo seguro para resolver ecuaciones lineales en el dominio encriptado.

La figura 3 muestra un diagrama de bloques del procedimiento directo para resolver sistemas de ecuaciones lineales en el dominio encriptado de acuerdo con una forma de realización. De acuerdo con una forma de realización, el sistema criptográfico 102 incluye un procedimiento para resolver sistemas de ecuaciones lineales directamente sobre los datos encriptados 100 (es decir, sin la necesidad de des-encriptar los datos). El procedimiento se basa en la eliminación de Gauss, utilizando el protocolo seguro de multiplicación para implementar las multiplicaciones necesarias. Debido a la falta de una operación de división bajo encriptación, según una forma de realización del procedimiento y sistema criptográfico 102, el vector resultado obtenido es escalado, pero los factores de escala son almacenados en un segundo vector **s**, de modo que se puede recuperar la solución después del des-encriptado a través de una división de componentes. El protocolo termina con dos vectores **x'** y **s**, que son la solución al sistema $x_i = \frac{x'_i}{s_i}$, i = 1,...., L.

A continuación se muestra una descripción detallada de los procedimientos para implementar los protocolos seguros para la resolución de sistemas de ecuaciones lineales de acuerdo con formas de realización particulares. En resumen, asúmase que L denota la dimensión de la matriz del sistema **A**. Para L–1 iteraciones, siendo k el número de la iteración ascendente de 1 a L–1, de acuerdo con una forma de realización, el sistema repite las siguientes etapas: A aleatoriza las encriptaciones de [$\mathbf{C}^{(k)}$] 300; A envía las encriptaciones aleatorizadas de [$\mathbf{C}^{(k)}$] a B 302; B calcula los productos [$\mathbf{D}^{(k)}$] y [$\mathbf{E}^{(k)}$], usando las encriptaciones recibidas 304; B envía [$\mathbf{D}^{(k)}$] y [$\mathbf{E}^{(k)}$] encriptados a A 306; A calcula [$\mathbf{G}^{(k)}$] y [$\mathbf{C}^{(k+1)}$], usando las encriptaciones recibidas 308. Entonces, A posee el vector de escala encriptado y lo envía a B 310. B des-encripta el vector de escala recibido y el valor de x'_L 312. B envía el vector de escala des-encriptado y x'_L a A 314. Entonces, para L–1 iteraciones, siendo k el número de la iteración descendente desde L–1 a 1, se repiten las siguientes etapas: A calcula el [x'_k] encriptado, utilizando los valores que A posee 316; A envía el [x'_k] encriptado a B 318; B des-encripta [x'_k] 320, B envía el x'_k des-encriptado a A 322. Después de estas operaciones, A y B calculan la solución **x** al sistema de ecuaciones lineales **A · x = b**, usando los valores que poseen 324.

Asúmase que $\mathbf{A} \in M_{L\times L}(\mathbb{Z})$ es una matriz definida positiva cuantificada simétrica, o una matriz dominante en diagonal, y que $\mathbf{b} \in \mathbb{Z}^L$ es un vector de columna cuantificado. La etapa de cuantificación Δ es tal que el valor absoluto de cada elemento cuantificado está limitado por encima por una constante T.

De acuerdo con una forma de realización, y sin limitación alguna, el procedimiento de protocolo seguro asume que B conoce la clave de des-encriptación de un sistema criptográfico homomórfico aditivo, y tanto A como B pueden producir encriptaciones usando este sistema criptográfico; A posee la matriz encriptada [**A**] y el vector encriptado de términos independientes [**b**]. Ambas partes participan en un protocolo interactivo con el fin de obtener la solución **x** al sistema lineal **A · x = b**. De acuerdo con una forma de realización, el protocolo se describe en detalle de la siguiente manera.

Siguiendo el algoritmo de eliminación de Gauss, llamamos $\mathbf{G}^{(0)}$ = **G** a la concatenación de **G** = [**A**|**b**]. El algoritmo se ejecuta en L–1 etapas. En cada etapa k, la matriz **G** es modificada para obtener un sistema equivalente $\mathbf{G}^{(k)}$ en el que la k-ésima incógnita no se encuentra en las últimas L–k ecuaciones.

Para la k-ésima etapa del algoritmo, los primeros k – 1 elementos de las L–k+1 últimas filas de $\mathbf{G}^{(k-1)}$ son cero; A posee una versión encriptada de los elementos distintos de cero de $\mathbf{G}^{(k-1)}$. El protocolo seguro procede de la siguiente manera:

1. A proporciona versiones encriptadas aleatorizadas de la sub–matriz $\mathbf{C}^{(k)}$ formada por las (L–k+2) últimas columnas de las (L–k+1) últimas filas de $\mathbf{G}^{(k-1)}$;

2. B, a través de la des-encriptación y re-encriptación, calcula los productos (aleatorios) de las (L–k) × (L–k+1) matrices $\mathbf{D}^{(k)}$ y $\mathbf{E}^{(k)}$, definidas como $\left[\mathrm{d}_{j,m}^{(k)}\right] = \left[\mathrm{c}_{1,m+1}^{(k)} \cdot \mathrm{c}_{j+1,1}^{(k)}\right]$ y $\left[\mathrm{e}_{i,j}^{(k)}\right] = \left[\mathrm{c}_{1,1}^{(k)} \cdot \mathrm{c}_{i+1,j+1}^{(k)}\right]$, y envía las encriptaciones aleatorizadas a A.

3. A des-aleatoriza las encriptaciones recibidas y, usando operaciones homomórficas, obtiene la siguiente iteración de **G**:

$$[\![\boldsymbol{G}^{(k)}]\!] = \left(\begin{array}{c|c} \{[\![g_{i,m}^{(k-1)}]\!]\}_{(1,1)}^{(k,L+1)} & \\ \hline \mathbf{0}_{L-k,k} & [\![\boldsymbol{F}^{(k)}]\!] \end{array} \right),$$

en la que [$\mathbf{F}^{(k)}$] es una matriz (L–k) × (L–k+1) con elementos $\left[\mathrm{f}_{i,m}^{(k)}\right] = \left[\mathrm{e}_{i,m}^{(k)}\right] - \left[\mathrm{d}_{i,m}^{(k)}\right]$.

Después de L–1 iteraciones, A tiene una matriz triangular superior encriptada anexada a un vector encriptado, [$\mathbf{G}^{(L-1)}$], que constituye un sistema con la misma solución que la original.

De acuerdo con una forma de realización, con el fin de resolver el sistema de ecuaciones lineales, ambas partes inician el proceso de sustitución inversa (back substitution) bajo encriptación, que consiste en L iteraciones: en cada iteración, se obtiene un elemento del vector **x**' y el correspondiente elemento del vector de escala **s**. A medida que son revelados en la salida y se necesitan para calcular los elementos subsiguientes de **x**', se pueden des-encriptar antes de la siguiente iteración con el fin de disminuir la complejidad reduciendo el número de protocolos de multiplicación necesarios. Para la primera etapa:

1. A envía $\{\left[\mathrm{g}_{i,i}^{(L-1)}\right]\}_{i=1}^{L}$ y $\left[\mathrm{g}_{L,L+1}^{(L-1)}\right]$.

2. B obtiene, mediante des-encriptación, el vector de escala **s**, con $s_i = \prod_{l=i}^{(L)} g_{l,l}^{(L-1)}$, y el valor $x'_L = g_{L,L+1}^{(L-1)}$, y los retorna a A.

En cada k-ésima etapa subsecuente, A calcula, usando operaciones homomórficas:

$$[\![x'_{L-k+1}]\!] = [\![g_{L-k+1,L+1}^{(L-1)}]\!] \cdot s_{L-k+2} - \sum_{l=L-k+2}^{L} [\![g_{L-k+1,l}^{(L-1)}]\!] \cdot x'_l \frac{s_l}{s_{L-k+2}},$$

y envía [x'$_{L-k+1}$] a B para obtener su des-encriptación.

Con esta forma de realización del protocolo, el sistema no divulga elemento alguno de la matriz original **A** ni de los vectores de términos independientes **b**. Además, cada etapa del protocolo se puede probar como segura con partes semi confiables, debido a la seguridad semántica del sistema criptográfico homomórfico subyacente, la seguridad de los protocolos de multiplicación usados y el hecho de que todos los valores no encriptados (además del resultado y el vector de escalado) al que cada parte puede acceder son aleatorios y no correlacionados. Sin embargo, el vector de escala revela la diagonal de la matriz triangular superior de un sistema equivalente, que proporciona información sobre los valores propios de la matriz original. Esta información afecta a los L elementos escalados fuera de $\frac{L(L+1)}{2}$.

Debe observarse que al tener los valores de la diagonal principal de la matriz triangular superior del sistema equivalente se obtiene la posibilidad de calcular su número de condición, o al menos, su límite

$$\kappa(\boldsymbol{U}) \geq \frac{\max_i(|u_{ii}|)}{\min_i(|u_{ii}|)}.$$

Por lo tanto, esta forma de realización descrita constituye una clara ventaja en términos de acondicionamiento y eficacia: antes de ejecutar el protocolo de sustitución inversa, las filas de $\mathbf{G}^{(L)}$ se pueden multiplicar por factores apropiados para reducir el número de condición y minimizar la propagación de un error debido al trabajo con una precisión de punto fijo. Además, el vector de factores multiplicativos s_i puede ser cuantificado de forma adecuada en claro para conseguir este mismo objetivo.

La forma de realización descrita del protocolo no limita el número N de sistemas de ecuaciones lineales que comparten la misma matriz del sistema **A** y con diferentes vectores de términos independientes $\mathbf{b}_i$ que se pueden

resolver en paralelo; todos los vectores $\mathbf{b}_i$ se pueden anexar a la matriz del sistema, formando una matriz $\mathbf{G}_{ext}$ de L × (L+N) y en cada etapa del protocolo anterior, se replican las operaciones que se deben realizar en la última columna de $\mathbf{G}^{(k)}$ para las últimas N columnas de $\boldsymbol{G}_{ext}^{(k)}$.

Cuando se resuelve un sistema $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$, el protocolo de eliminación de Gauss (GE) se realiza en (L–1) series de comunicación, con una complejidad total de

$$\begin{aligned}
\mathrm{Comp}_{cmGE} &= (L^3 + L^2 - 2) \\
\mathrm{Comp}_{cpGE,A} &= \frac{1}{3}\left(L^3 + 3L^2 + 2L - 6\right)\mathrm{Comp}_{Encrypt} + \ldots \\
&\quad \frac{1}{3}\left(2L^3 + 3L^2 + L - 6\right)\mathrm{Comp}_{EA} \\
\mathrm{Comp}_{cpGE,B} &= \frac{1}{3}\left(L^3 + 3L^2 + 2L - 6\right)\mathrm{Comp}_{Decrypt} + \ldots \\
&\quad \frac{2}{3}\left(L^3 - L\right)\left(\mathrm{Comp}_{Encrypt} + \mathrm{Comp}_{P}\right).
\end{aligned}$$

El protocolo de sustitución inversa (BS) se realiza en L series de comunicación, con una complejidad total de

$$\begin{aligned}
\mathrm{Comp}_{cmBS} &= 2L \cdot (1 + ct) \\
\mathrm{Comp}_{cpBS,A} &= \frac{1}{2}(L^2 + L - 2)\mathrm{Comp}_{EP} + \frac{1}{2}(L^2 - L)\mathrm{Comp}_{EA} \\
\mathrm{Comp}_{cpBS,B} &= 2L\mathrm{Comp}_{Decrypt}.
\end{aligned}$$

De acuerdo con una forma de realización, los coeficientes de la matriz **A** del sistema son versiones cuantificadas de los coeficientes de valor real, con una etapa de cuantificación Δ. Además, el valor absoluto de los coeficientes cuantificados está limitado por un entero T > 0. Entonces, es posible estimar el valor de T necesario para encajar todas las operaciones realizadas dentro de un cifrado que puede representar números enteros en el rango [0,n) sin problemas de redondeo.

Para la primera parte del protocolo de acuerdo con una forma de realización (la eliminación segura y directa de Gauss), cada iteración multiplica dos números que se obtuvieron en la iteración anterior y los suma, con lo que el límite anterior se eleva al cuadrado y se duplica:

$$|t_1|, |t_2|, |t_3|, |t_4| < T \Rightarrow |t_1 \cdot t_2 - t_3 \cdot t_4| < 2T^2.$$

En esta forma de realización, todos los elementos de la k-ésima fila de la $\mathbf{G}^{(L-1)}$ resultante son limitados por $(2^{2^{k-1}-1})T^{2^k}$, y constituyen la representación de sus equivalentes de valor real, cuantificados por $\Delta^{2^{k-1}}$. Por lo tanto, el cifrado debe ser tal que $n > (2^{2^{k-1}-1})T^{2^k}$ con el fin de encajar todos los números implicados en este protocolo. Esto significa que el tamaño de bit del módulo del cifrado debe crecer exponencialmente con la dimensionalidad del sistema, lo que da como resultado una escalabilidad baja.

Para la segunda parte del protocolo según esta forma de realización, después de la revelación de los elementos de la diagonal, se pueden volver a cuantificar para hacerlos relativos a la escala más baja y disminuir los requisitos de tamaño de bit del cifrado; pero en el peor de los casos, sin volver a cuantificar los factores de escala, el mayor número presente después de ejecutar todo el protocolo es $2^{2^L - L - 1}T^{2^{1+L}-4}$. Esto también restringe el tamaño del cifrado.

F. Motor de cálculo seguro y protocolo iterativo para resolver ecuaciones lineales en el dominio encriptado.

La figura 4 muestra un diagrama de bloques de un procedimiento ilustrativo para resolver sistemas de ecuaciones lineales iterativamente en el dominio encriptado de acuerdo con una forma de realización. De acuerdo con una forma de realización, el sistema criptográfico 102 incluye un procedimiento (protocolo) iterativo para resolver sistemas de ecuaciones lineales directamente en los datos encriptados 100 (es decir, sin la necesidad de des-encriptar los datos). De acuerdo con una forma de realización presentada en este documento solo con fines ilustrativos, y no a modo de limitación, el sistema criptográfico incluye un procedimiento iterativo para resolver sistemas de ecuaciones lineales según se describe a continuación. Asúmase que L denota la dimensión de la matriz **A** del sistema. A oculta la encriptación de la diagonal principal de [**A**] a través de la adición homomórfica 400. A envía estas encriptaciones a B 402, para que B pueda des-encriptar una parte compartida de la diagonal principal de [**A**] 404. Entonces, A y B calculan, a través de protocolos de multiplicación paralelos seguros, la matriz diagonal encriptada [ɣ$\mathbf{D}^{-1}$] y el factor ɣ 406. A y B, utilizando el protocolo seguro de multiplicación, pueden calcular encriptaciones de la matriz modificada [ɣ**M**] y el vector modificado [ɣ**c**] 408. Después de esto, A y B terminan con partes compartidas de [ɣ**M**] 410. A realiza la primera iteración del protocolo usando operaciones homomórficas 412, obteniendo [$\mathbf{x}'_1$] = [ɣ$\mathbf{x}^{(1)}$]. Luego, para cada iteración, siendo k el número de la iteración actual, ambas partes siguen el siguiente procedimiento: A y B ejecutan el protocolo de producto seguro sobre [ɣ**M**] y [$\mathbf{x}'_k$] 414; usando el resultado de la operación anterior, A calcula

homomórficamente la encriptación de [$\mathbf{x}'_{k+1}$] 416. Después de cada iteración o después de un número predefinido de iteraciones, se verifica una condición de detención 418. Cuando se cumple la condición de detención 418, el protocolo se detiene, y A envía el [$\mathbf{x}'_k$] encriptado a B para su des-encriptación 420, y ambas partes obtienen el resultado $\mathbf{x}^{(k)}$ 422.

De acuerdo con una forma de realización, la forma general de procedimientos iterativos estacionarios para resolver sistemas de ecuaciones lineales es

$$\boldsymbol{x}^{(k+1)} = \boldsymbol{M} \cdot \boldsymbol{x}^{(k)} + \boldsymbol{c}.$$

De acuerdo con una forma de realización, y sin limitación alguna, la matriz del sistema se descompone en **A** = **D**(**L**+**I**+**U**), una matriz diagonal **D**, una matriz triangular inferior **L** y una matriz triangular superior **U**, teniendo tanto **L** como **U** ceros en sus diagonales principales. Entonces, **M** = –(**L**+**U**) y **c** = $\mathbf{D}^{-1}$ **b**. Nos referimos a esta forma de realización como el procedimiento de Jacobi, la forma de realización de Jabobi, el protocolo de Jacobi o el protocolo seguro de Jacobi debido a la naturaleza de la descomposición de la matriz y el procedimiento iterativo para resolver el sistema de ecuaciones lineales. Como las divisiones no son compatibles homomórficamente, la iteración anterior no se puede implementar directamente. Por lo tanto, de acuerdo con esta forma de realización, se simula la división multiplicando cada fila de **A** por los elementos diagonales de las filas restantes, lo que resulta en multiplicar la matriz **M** del procedimiento de Jacobi por un factor escalar $\gamma = \prod_{i=1}^{L} a_{ii}$.

$$\boldsymbol{A}' = -\gamma \boldsymbol{D}^{-1} \cdot (\boldsymbol{A} - \boldsymbol{D}) = \gamma \boldsymbol{M}.$$

De acuerdo con la forma de realización de Jacobi, el factor γ se propaga en cada iteración del algoritmo:

$$\gamma^k \boldsymbol{x}^{(k)} = -\gamma \boldsymbol{D}^{-1} (\boldsymbol{A} - \boldsymbol{D}) \cdot \gamma^{k-1} \boldsymbol{x}^{(k-1)} + \gamma^k \boldsymbol{D}^{-1} \boldsymbol{b}.$$

De acuerdo con una forma de realización, el protocolo iterativo seguro asume que B puede des-encriptar y tanto A como B pueden encriptar con un esquema homomórfico aditivo, y que A posee encriptaciones de [**A**] y [**b**] con este sistema homomórfico. Con el fin de permitir un cálculo eficiente, se ejecuta el siguiente protocolo:

1. A puede ocultar la diagonal principal de [**A**] y enviarla a B.

2. B la des-encripta, terminando ambas partes con partes compartidas aditivas de los elementos en la diagonal $\{a_{ii}\}$.

3. Con estas partes compartidas, ambas partes pueden calcular de forma segura partes compartidas de la matriz diagonal $(\gamma \boldsymbol{D}^{-1})_{jj} = \prod_{i=1, i\neq j}^{L} a_{ii}$, a través de $\lceil \log_2(L-1) \rceil$ series de protocolos de multiplicación seguros en paralelo. También pueden calcular el valor de γ y divulgarlo para su uso en las siguientes etapas del protocolo.

4. A puede calcular luego la encriptación de [γ**M**] = [-$\gamma\mathbf{D}^{-1}$]·[**A**-**D**] y [γ**c**]= [-$\gamma\mathbf{D}^{-1}$]·[**b**], invocando el protocolo seguro de multiplicación.

5. Entonces, A envía a B una versión oculta y encriptada de [γ**M**], que B des-encripta para uso en la siguientes iteraciones.

Después de estas etapas iniciales, en la primera iteración del protocolo seguro, ambas partes acuerdan un vector inicial $\mathbf{x}^{(0)}$ y A calcula, a través de adiciones y multiplicaciones homomórficas, la encriptación de [$\gamma\mathbf{x}^{(1)}$] = [γ**M**] · $\mathbf{x}^{(0)}$+[γ**c**].

Para cada iteración posterior, A calcula la encriptación de γ · [γ^{k-1}**c**], y a continuación ambas partes utilizan el protocolo seguro de multiplicación y adiciones homomórficas con el fin de obtener el vector para la etapa siguiente

$$[\![\boldsymbol{x}'_k]\!] = [\![\gamma^k \boldsymbol{x}^{(k)}]\!] = [\![\gamma \boldsymbol{M}]\!] \cdot [\![\gamma^{k-1} \boldsymbol{x}^{(k-1)}]\!] + \gamma \cdot [\![\gamma^{k-1} \boldsymbol{c}]\!].$$

Debe observarse que la matriz [γ**M**] no tiene que ser comunicada en cada iteración, ya que su versión oculta ha sido almacenada por B en la etapa inicial. Por lo tanto, solo se envían dos vectores por cada iteración entre A y B.

Después de cada iteración, el factor γ multiplica el resultado; por lo tanto, después de una serie de etapas, el cifrado no podrá admitir el número escalado, y el protocolo deberá detenerse. Debe observarse que el factor acumulado no es solo γ, sino también la etapa de cuantificación Δ utilizada para la cuantificación inicial de los coeficientes tanto de la matriz **A** del sistema como del vector **b** para convertirlos en enteros para que puedan ser encriptados. Este factor también se debe tener en cuenta cada vez que γ multiplica el vector **c**, para que los vectores agregados homomórficamente sean cuantificados con el mismo factor de escala.

De acuerdo con una forma de realización, cada etapa del protocolo de acuerdo con esta forma de realización puede ser probada como segura con partes semi confiables, debido a la seguridad semántica del sistema criptográfico

subyacente, la seguridad del protocolo de multiplicación y el hecho de que los valores no encriptados que ve cada parte son aleatorios y no correlacionados.

La complejidad de la parte inicial (inicial de Jacobi, JI) del protocolo es

$$\mathrm{Comp}_{cmJI} = 3L^2 + 2L\lceil \log_2(L-1)\rceil - 3L + 5 + ct$$

$$\mathrm{Comp}_{cpJI,A} = (5L^2 + 4L\lceil \log_2(L-1)\rceil - 5L + 8)\mathrm{Comp}_{EA} + (L^2 + L\lceil \log_2(L-1)\rceil - L + 2)2\mathrm{Comp}_{EP}$$

$$\mathrm{Comp}_{cpJI,B} = (L^2 + L\lceil \log_2(L-1)\rceil - L + 2)\left(\mathrm{Comp}_{Decrypt} + \mathrm{Comp}_P + \mathrm{Comp}_{Encrypt}\right) + (L^2 - L + 1)\mathrm{Comp}_{Decrypt}.$$

La primera iteración (J1) no involucra ninguna interacción, y A incurre en una complejidad de cálculo $\mathrm{Comp}_{cpJ1,\,A} = L^2(\mathrm{Comp}_{EP}+\mathrm{Comp}_{EA})$.

La complejidad de cada una de las iteraciones posteriores de este protocolo (J) es la siguiente

$$\mathrm{Comp}_{cmJ} = 2L$$

$$\mathrm{Comp}_{cpJ,A} = (3L^2 - 2L)\mathrm{Comp}_{EA} + (2L^2 - L)\mathrm{Comp}_{EP} + L\mathrm{Comp}_{EA}$$

$$\mathrm{Comp}_{cpJ,B} = L\left(\mathrm{Comp}_{Decrypt} + \mathrm{Comp}_{Encrypt}\right) + (L^2 - L)\mathrm{Comp}_P + (L^2 - 2L)\mathrm{Comp}_A.$$

Después de un número de iteraciones, o bien la solución puede ser revelada, o se puede obtener una métrica de error para determinar si se ha alcanzado la convergencia. Si bien la elección de esta métrica de error es arbitraria, una posibilidad de acuerdo con una forma de realización es restar homomórficamente $[\mathbf{x}^{(k)}] - [\mathbf{x}^{(k-1)}]$, y des-encriptar el resultado o realizar L comparaciones encriptadas en paralelo con un umbral predeterminado.

Según una forma de realización, y sin limitación alguna, los coeficientes de la matriz **A** del sistema son versiones cuantificadas de los coeficientes de valor real, con una etapa de cuantificación Δ, de modo que su valor absoluto cuantificado está limitado por un entero $T > 0$.

Para la primera parte de la forma de realización descrita del protocolo iterativo, en el que se calculan el factor γ y la matriz $\gamma\mathbf{D}^{-1}$, γ es el número más alto que el sistema tendrá que representar, y está limitado por T^L; el límite para los elementos de $\gamma\mathbf{D}^{-1}$ es T^{L-1}. Además, dado que γ es revelado en la siguiente etapa, puede constituir un límite más preciso para los coeficientes encriptados de $\gamma\mathbf{D}^{-1}$. Un límite para el valor absoluto de los coeficientes de $\gamma\mathbf{M}$ y de $\gamma\mathbf{c}$ es $\min(T^L, \gamma T)$.

De acuerdo con una forma de realización particular, el límite al que están sujetos los elementos del primer vector $\mathbf{x}^{(1)}$ es $L \cdot T^{L+1}$.

En cada iteración, el límite anterior es multiplicado por $L \cdot T^L$, lo que significa que el límite para los elementos de la k-ésima iteración es $L^k \cdot T^{k\cdot L+1}$, es decir, el tamaño de bit necesario del cifrado es lineal tanto en la dimensión del sistema como en el número máximo de iteraciones que se pueden realizar sin errores. Además, la etapa de cuantificación de los elementos de $\mathbf{x}^{(k)}$ será Δ^{kL}.

Cuando se trata de algoritmos iterativos tales como la forma de realización que se presenta en este documento, es necesario determinar si el algoritmo puede converger o no antes de aplicar el algoritmo. En el caso general de procedimientos iterativos estacionarios, la condición necesaria y suficiente para su convergencia con un vector inicial arbitrario $\mathbf{x}^{(0)}$ es que $\max_i |\lambda_i(\mathbf{M})| < 1$, en el que $\lambda_i(\mathbf{M})$ son los valores propios de **M**. En esta forma de realización particular, $\mathbf{M} = -\mathbf{D}^{-1} \cdot (\mathbf{A} - \mathbf{D})$. Asúmase que **A** es una matriz estrictamente dominante en diagonal con coeficientes limitados $|a_{ij}| \leq T$. Según el teorema de Ostrowski, los valores propios de **M** se encuentran en la unión de L discos

$$\mathcal{L}_1 \triangleq \bigcup_{i=1}^{L} \{z \in \mathbb{C} : |z - m_{ii}| \leq \min\{R_i, C_i\}\},$$

en el que $m_{ii} = 0$, $m_{ij} = a_{ij} / a_{ii}$, $i \neq j$, y

$$R_i = \sum_{j=1, j\neq i}^{L} |m_{ij}|,$$
$$C_i = \sum_{j=1, j\neq i}^{L} |m_{ji}|.$$

Como **A** es dominante estrictamente diagonalmente, $\sum_{j=1,j\neq i}^{L}|a_{ij}| < |a_{ii}|$ => $R_i < 1$. Por lo tanto, es posible limitar los módulos de los valores propios de **M** como

$$|\lambda_i(\boldsymbol{M})| < 1.$$

En consecuencia, la forma de realización de Jacobi divulgada siempre converge para matrices estrictamente dominantes diagonalmente, y no es necesario el test de convergencia.

G. Protocolo iterativo seguro para realizar inversiones de matrices y resolver sistemas de ecuaciones en base a un protocolo iterativo.

La figura 5 muestra un diagrama de bloques ilustrativo de la operación del sistema criptográfico. Asúmase que L denota la dimensión de la matriz **A** del sistema. A y B acuerdan una matriz inicial $\mathbf{X}^{(0)}$ 500 que cumple los criterios de convergencia. Para la primera iteración, A calcula homomórficamente la encriptación de la matriz $\mathbf{X}^{(1)}$ 502. Para cada iteración posterior, siendo k el número de la iteración actual, ambas partes ejecutan las siguientes etapas: A y B usan el protocolo seguro de multiplicación para obtener la matriz encriptada $\mathbf{Q}^{(k)}$ 504; A y B usan el protocolo seguro de multiplicación con el fin de obtener la matriz encriptada $\mathbf{X}^{(k+1)}$ 506. Después de cada iteración o después de un número predefinido de iteraciones, se verifica una condición de detención 508. Cuando se cumple la condición de detención 508, el protocolo se detiene, y A envía la $[\mathbf{X}^{(k)}]$ encriptada a B para su des-encriptación 510, y ambas partes obtienen la $\mathbf{X}^{(k)}$ resultante 512.

Hay casos en los que, en lugar de o además de solucionar un sistema de ecuaciones lineales, también se necesita la inversa de la matriz del sistema, como el caso de análisis de regresión en estadística. Para estas aplicaciones, se debe invertir la matriz **A** del sistema. De acuerdo con una forma de realización, los sistemas criptográficos incluyen un protocolo seguro para realizar la ejecución de un procedimiento iterativo. Nos referimos a esta forma de realización como la forma de realización de Newton, protocolo iterativo de Newton o procedimiento de Newton, indistintamente. De acuerdo con una forma de realización, una iteración de este procedimiento tiene la siguiente expresión

$$\boldsymbol{X}^{(k)} = \boldsymbol{X}^{(k-1)} \cdot \left(2\boldsymbol{I} - \boldsymbol{A}\boldsymbol{X}^{(k-1)}\right),$$

en la que $\mathbf{X}^{(k)}$ convergerá a A^{-1}.

De acuerdo con una forma de realización, el protocolo seguro para el protocolo seguro de Newton ejecuta una iteración inicial con un valor inicial acordado $\mathbf{X}^{(0)}$, realizada únicamente con operaciones homomórficas. Luego, las siguientes iteraciones utilizan el protocolo seguro de multiplicación y las sumas homomórficas. Cada iteración necesita dos series de comunicación:

1. La primera para calcular $[\mathbf{Q}^{(k)}] = [\mathbf{A}] \cdot [\mathbf{X}^{(k-1)}]$,

2. La segunda para calcular $[\mathbf{X}^{(k)}] = [\mathbf{X}^{(k-1)}] \cdot (2\mathbf{I} - [\mathbf{Q}^{(k)}])$.

De acuerdo con una forma de realización, el resultado es multiplicado después de cada iteración por la etapa de cuantificación de los enteros utilizados, de modo que después de un número suficientemente alto de iteraciones, el protocolo se detiene.

El protocolo es demostrablemente seguro con partes semi confiables debido a la seguridad semántica del sistema criptográfico, y la seguridad de los protocolos de multiplicación compuestos secuencialmente.

La complejidad de las formas de realización divulgadas se evalúa como sigue. La primera etapa involucra solo una serie de interacción, y su complejidad es determinada por

$$\mathrm{Comp}_{cmNEWI} = \mathrm{Comp}_{cmMULT}(L, L, L)$$
$$\mathrm{Comp}_{cpNEWI,A} = \mathrm{Comp}_{cpMULT,A}(L, L, L) + L^3\mathrm{Comp}_{EP} + (L^3 - L^2 + L)\mathrm{Comp}_{EA}$$
$$\mathrm{Comp}_{cpNEWI,B} = \mathrm{Comp}_{cpMULT,B}(L, L, L).$$

La complejidad de cada una de las siguientes iteraciones de este protocolo es la siguiente

$$\mathrm{Comp}_{cmNEW} = 2\mathrm{Comp}_{cmMULT}(L, L, L)$$

$$\mathrm{Comp}_{cpNEW,A} = 2\mathrm{Comp}_{cpMULT,A}(L, L, L) + L\mathrm{Comp}_{EA}$$

$$\mathrm{Comp}_{cpNEW,B} = 2\mathrm{Comp}_{cpMULT,B}(L, L, L).$$

Asúmase que los elementos de la matriz **A** se cuantifican con una etapa de cuantificación Δ, y su valor absoluto está limitado por T > 0. Entonces, los elementos de la matriz que resultan de la primera iteración del protocolo están limitados por L^2T^3+2T. Para cada una de las siguientes iteraciones, se actualiza el límite $T^{(k-1)}$ como $T^{(k)}=(T^{(k-1)})^2 \cdot T \cdot L^2+2 \cdot K$. Por lo tanto, el orden del límite después de m iteraciones es $O(T^{2^{m+1}-1} \cdot L^{2^{m+1}-2})$, es decir, el tamaño de bit del cifrado es exponencial en el número de iteraciones.

La convergencia de la forma de realización descrita del protocolo iterativo seguro de Newton es asegurada siempre que la matriz inicial $\mathbf{X}^{(0)}$ satisfaga $||\mathbf{AX}^{(0)} - \mathbf{I}|| < 1$. Dado que el vector inicial es elegido por ambas partes, éste puede ser tal que se cumpla esta condición, dados los límites en los elementos de **A** y los límites en los valores propios obtenidos mediante la aplicación del teorema de Ostrowski.

H. Extensión a sistemas con elementos complejos según una forma de realización.

El protocolo presentado en la sección anterior no impone ninguna restricción a los coeficientes de matriz. Se puede usar tanto para coeficientes reales no restringidos como para coeficientes complejos. En esta sección explicamos cómo se puede implementar el protocolo en el caso de coeficientes complejos.

Por conveniencia, y sin pérdida de generalidad, se elige una representación binomial para números complejos; la encriptación de un número complejo [x] es determinada por el par $[x] \triangleq ([R\{x\}], [I\{x\}])$, es decir, el par de encriptaciones de sus partes real e imaginaria.

De acuerdo con una forma de realización, la operación de adición compleja se puede realizar a través de dos adiciones reales; por lo tanto, se puede realizar homomórficamente entre dos números complejos encriptados como dos adiciones reales homomórficas. Con respecto al producto complejo, cuando involucra un factor conocido y un número encriptado, también se puede realizar homomórficamente como cuatro multiplicaciones homomórficas y dos adiciones homomórficas. Cuando hay dos factores encriptados involucrados, se realiza a través de cuatro protocolos de multiplicación escalar (real) en paralelo y dos adiciones homomórficas.

Por lo tanto, el protocolo de multiplicación de matrices descrito en la sección anterior funciona en números complejos adoptando la representación compleja encriptada propuesta, y sustituyendo las adiciones y productos reales por sus operaciones complejas correspondientes. Como resultado, se duplica la complejidad de la comunicación, se multiplica por cuatro el número de productos realizados, y se duplica el número de adiciones realizadas. Para el protocolo seguro de resolución de sistemas de ecuaciones lineales, las modificaciones necesarias son esencialmente las mismas, siendo los factores de escala involucrados también complejos. Debemos señalar que las hipótesis sobre la matriz del sistema que se impusieron para garantizar la convergencia de los algoritmos se mantienen inalteradas cuando se trata de sistemas con coeficientes complejos, ya que son hipótesis generales no restringidas a sistemas con coeficientes reales.

Aunque se han descrito formas de realización particulares, se entiende que, después de aprender las enseñanzas contenidas en esta descripción, para los expertos en la técnica serán evidentes modificaciones y generalizaciones sin apartarse del alcance de las formas de realización divulgadas. Se observa que los ejemplos anteriores han sido proporcionados meramente con el propósito de explicación y de ningún modo deben interpretarse como limitativos. Aunque el sistema se ha descrito con referencia a diversas formas de realización, se entiende que las palabras que se han utilizado en este documento son palabras de descripción e ilustración, en lugar de palabras limitantes. Además, aunque el sistema se ha descrito en el presente documento con referencia a medios, materiales y formas de realización particulares, no se pretende que las formas de realización se limiten a los detalles divulgados en este documento; más bien, el sistema se extiende a todas las estructuras, procedimientos y usos funcionalmente equivalentes, tales como los que están dentro del alcance de las reivindicaciones adjuntas. Los expertos en la técnica, que tienen el beneficio de las enseñanzas de esta especificación, pueden efectuar numerosas modificaciones a las mismas y se pueden hacer cambios sin apartarse del alcance de las formas de realización divulgadas en sus aspectos.

REIVINDICACIONES

1. Un sistema criptográfico (102), que comprende:
una memoria configurada para almacenar instrucciones ejecutables por un sistema informático; y
al menos un procesador de hardware configurado para ejecutar dichas instrucciones ejecutables por un sistema informático que cuando se ejecutan hacen que el procesador realice multiplicaciones de matrices en un dominio encriptado (104) y resuelva sistemas de ecuaciones lineales en el dominio encriptado (106) usando un protocolo iterativo seguro basado en protocolos de preservación de la privacidad basados en cálculo homomórfico (108) y compartición de secretos (110), siendo implementado dicho protocolo iterativo seguro como un procedimiento iterativo estacionario y siendo sustancialmente equivalente a una matriz iterativa de actualización de Jacobi;
en el que dicho protocolo iterativo seguro comprende calcular las partes compartidas de una diagonal de una matriz del sistema (400 – 406), calcular una matriz modificada encriptada y un vector modificado encriptado (408), calcular un vector de salida encriptado (414 – 416) en base a cálculo homomórfico (108) y compartición de secretos (110), y des-encriptar los elementos de dicho vector de salida (422);
por lo que dicho sistema criptográfico (102) es capaz de realizar cálculos seguros, procesamiento de señal y análisis de datos directamente en datos encriptados (100) en entornos no confiables sin la necesidad de des-encriptar dichos datos encriptados (100).

2. Un producto de programa informático que comprende instrucciones ejecutables por un sistema informático, que, cuando son ejecutadas por un procesador de hardware, hacen que el procesador de hardware realice un procedimiento criptográfico que comprende:
realizar multiplicaciones de matrices en un dominio encriptado (104); y
resolver sistemas de ecuaciones lineales en el dominio encriptado (106) usando un protocolo iterativo seguro basado en protocolos de preservación de privacidad basados en cálculo homomórfico (108) y compartición de secretos (110), siendo implementado dicho protocolo iterativo seguro como un procedimiento iterativo estacionario y siendo sustancialmente equivalente a una matriz iterativa de actualización de Jacobi;
en el que dicho protocolo iterativo seguro comprende calcular las partes compartidas de una diagonal de una matriz del sistema (400 – 406), calcular una matriz modificada encriptada y un vector modificado encriptado (408), calcular un vector de salida encriptado (414 – 416) en base a cálculo homomórfico (108) y compartición de secretos (110), y des-encriptar los elementos de dicho vector de salida (422);
por lo que dicho sistema criptográfico (102) es capaz de realizar cálculos seguros, procesamiento de señal y análisis de datos directamente en datos encriptados en entornos no confiables sin la necesidad de des-encriptar dichos datos encriptados (100).

3. El producto de programa informático según la reivindicación 2, incorporado en un medio de almacenamiento.

4. El producto de programa informático según la reivindicación 2, transportado por una señal de transmisión.

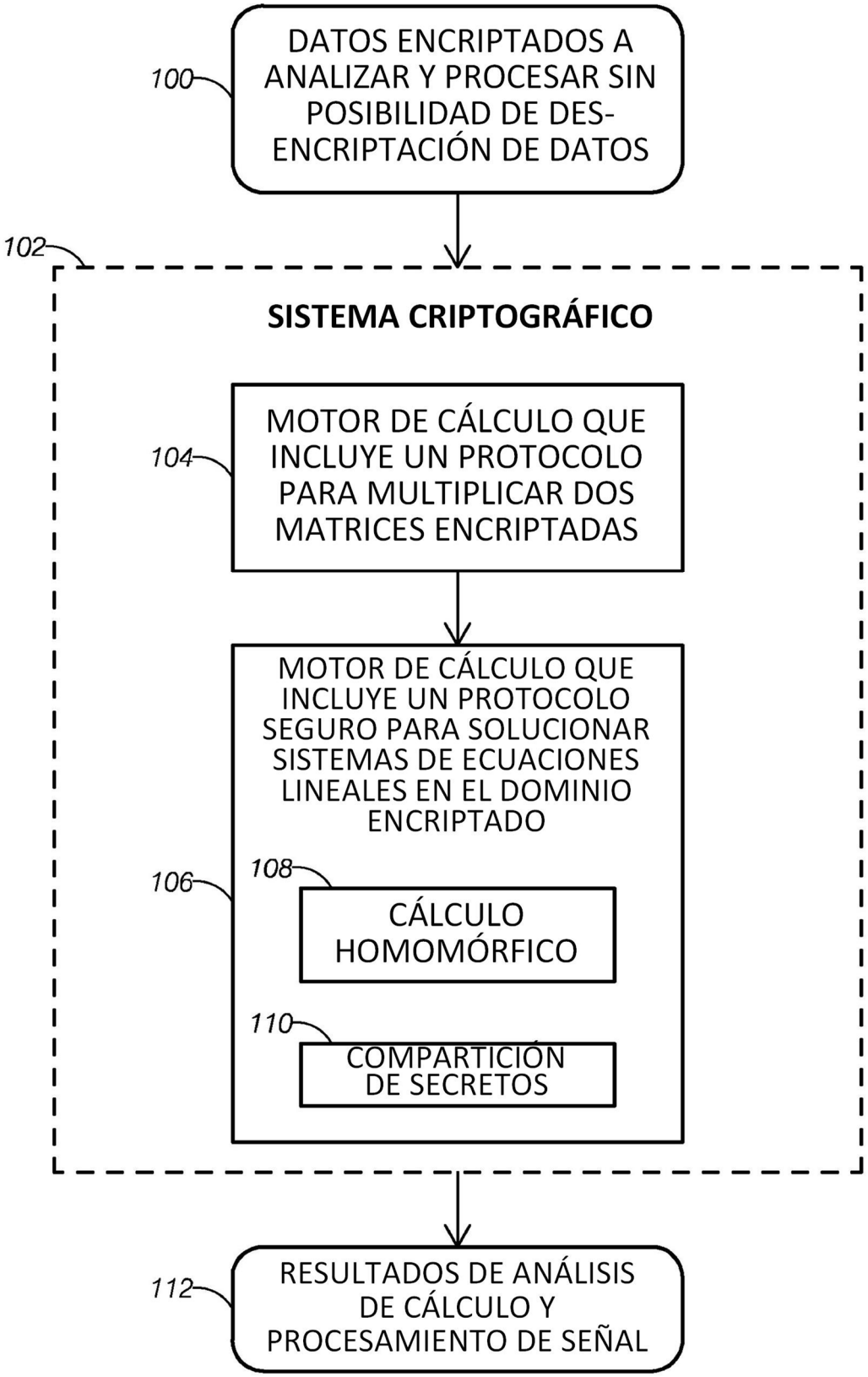
DATOS ENCRIPTADOS A ANALIZAR Y PROCESAR SIN POSIBILIDAD DE DES-ENCRIPTACIÓN DE DATOS
100
102
SISTEMA CRIPTOGRÁFICO
MOTOR DE CÁLCULO QUE INCLUYE UN PROTOCOLO PARA MULTIPLICAR DOS MATRICES ENCRIPTADAS
104
MOTOR DE CÁLCULO QUE INCLUYE UN PROTOCOLO SEGURO PARA SOLUCIONAR SISTEMAS DE ECUACIONES LINEALES EN EL DOMINIO ENCRIPTADO
106
108
CÁLCULO HOMOMÓRFICO
110
COMPARTICIÓN DE SECRETOS
RESULTADOS DE ANÁLISIS DE CÁLCULO Y PROCESAMIENTO DE SEÑAL
112

FIG.1

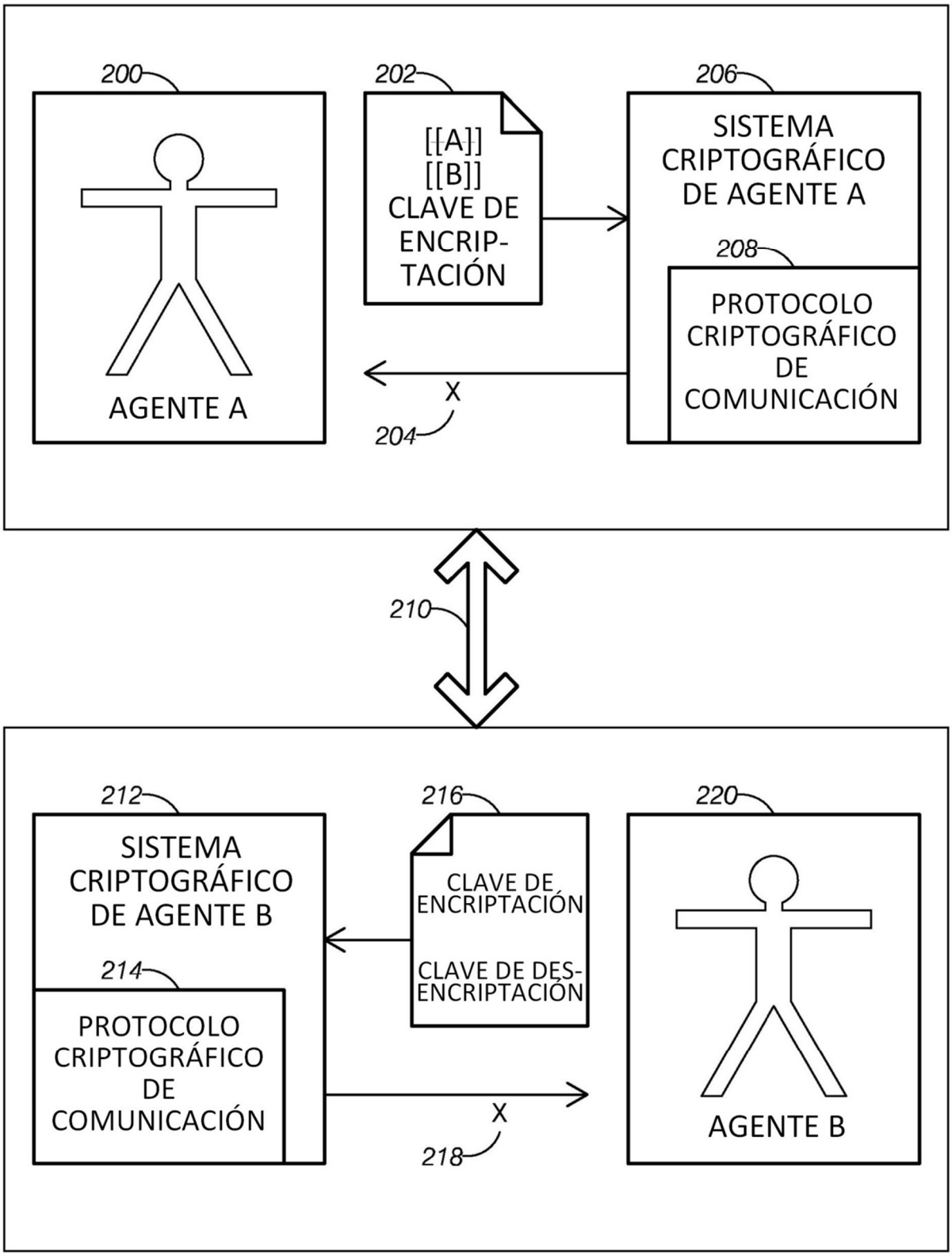
200
AGENTE A
202
[[A]]
[[B]]
CLAVE DE ENCRIP-TACIÓN
X
204
206
SISTEMA CRIPTOGRÁFICO DE AGENTE A
208
PROTOCOLO CRIPTOGRÁFICO DE COMUNICACIÓN
210
212
SISTEMA CRIPTOGRÁFICO DE AGENTE B
214
PROTOCOLO CRIPTOGRÁFICO DE COMUNICACIÓN
216
CLAVE DE ENCRIPTACIÓN
CLAVE DE DES-ENCRIPTACIÓN
X
218
220
AGENTE B

FIG.2

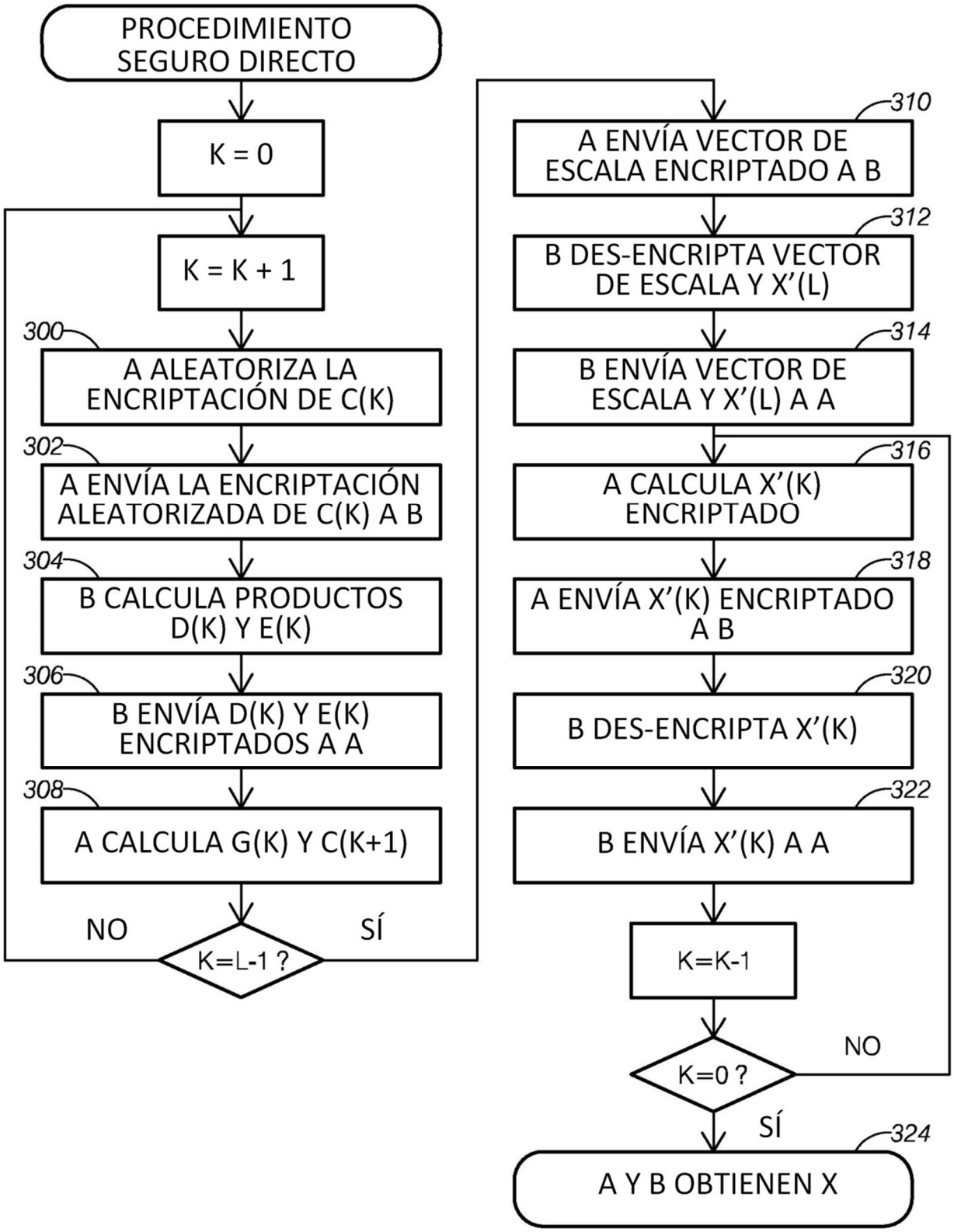
PROCEDIMIENTO SEGURO DIRECTO
K = 0
K = K + 1
300
A ALEATORIZA LA ENCRIPTACIÓN DE C(K)
302
A ENVÍA LA ENCRIPTACIÓN ALEATORIZADA DE C(K) A B
304
B CALCULA PRODUCTOS D(K) Y E(K)
306
B ENVÍA D(K) Y E(K) ENCRIPTADOS A A
308
A CALCULA G(K) Y C(K+1)
NO
K=L-1 ?
SÍ
310
A ENVÍA VECTOR DE ESCALA ENCRIPTADO A B
312
B DES-ENCRIPTA VECTOR DE ESCALA Y X'(L)
314
B ENVÍA VECTOR DE ESCALA Y X'(L) A A
316
A CALCULA X'(K) ENCRIPTADO
318
A ENVÍA X'(K) ENCRIPTADO A B
320
B DES-ENCRIPTA X'(K)
322
B ENVÍA X'(K) A A
K=K-1
K=0 ?
NO
SÍ
324
A Y B OBTIENEN X

FIG.3

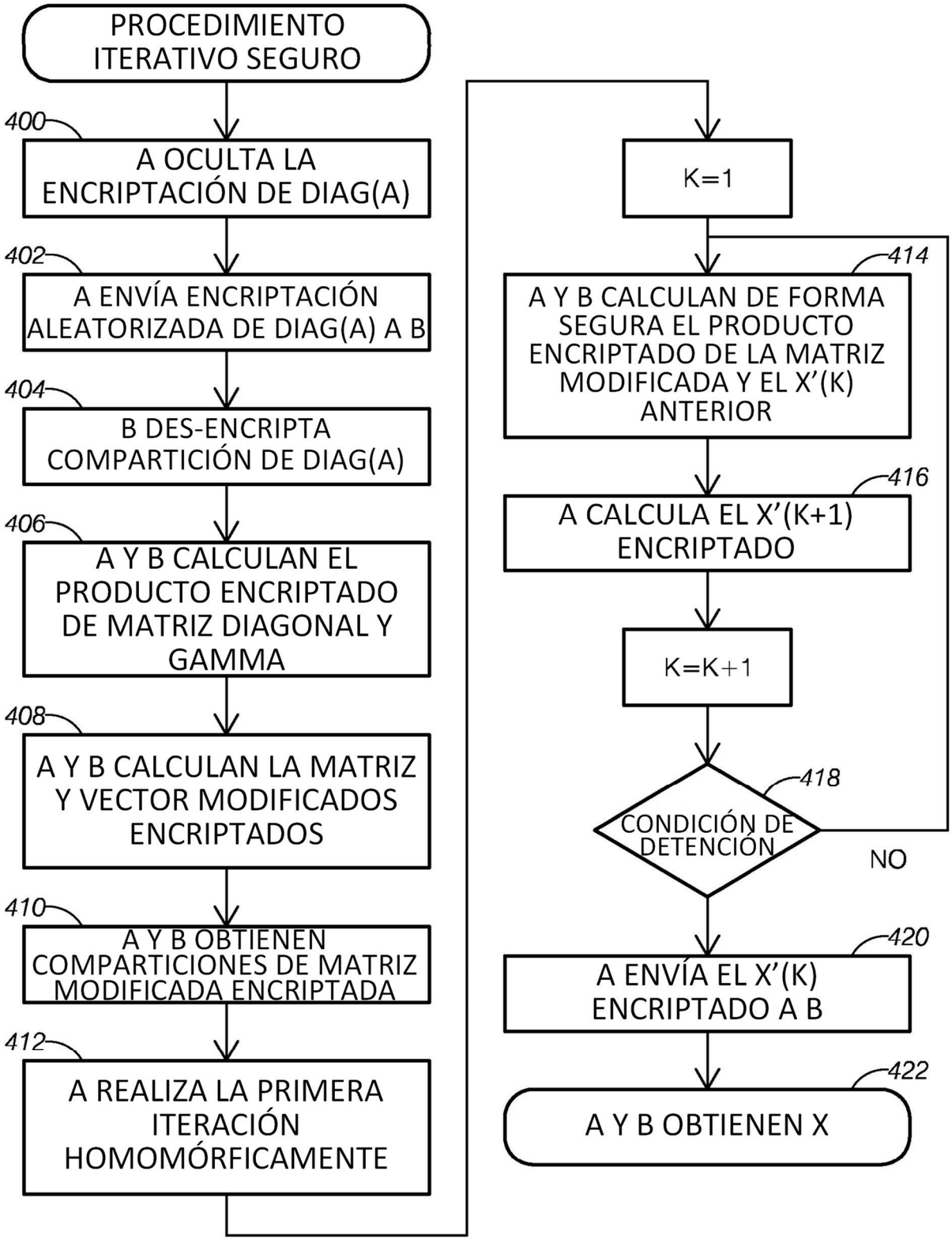
PROCEDIMIENTO ITERATIVO SEGURO
400
A OCULTA LA ENCRIPTACIÓN DE DIAG(A)
402
A ENVÍA ENCRIPTACIÓN ALEATORIZADA DE DIAG(A) A B
404
B DES-ENCRIPTA COMPARTICIÓN DE DIAG(A)
406
A Y B CALCULAN EL PRODUCTO ENCRIPTADO DE MATRIZ DIAGONAL Y GAMMA
408
A Y B CALCULAN LA MATRIZ Y VECTOR MODIFICADOS ENCRIPTADOS
410
A Y B OBTIENEN COMPARTICIONES DE MATRIZ MODIFICADA ENCRIPTADA
412
A REALIZA LA PRIMERA ITERACIÓN HOMOMÓRFICAMENTE
K=1
414
A Y B CALCULAN DE FORMA SEGURA EL PRODUCTO ENCRIPTADO DE LA MATRIZ MODIFICADA Y EL X'(K) ANTERIOR
416
A CALCULA EL X'(K+1) ENCRIPTADO
K=K+1
418
CONDICIÓN DE DETENCIÓN
NO
420
A ENVÍA EL X'(K) ENCRIPTADO A B
422
A Y B OBTIENEN X

FIG.4

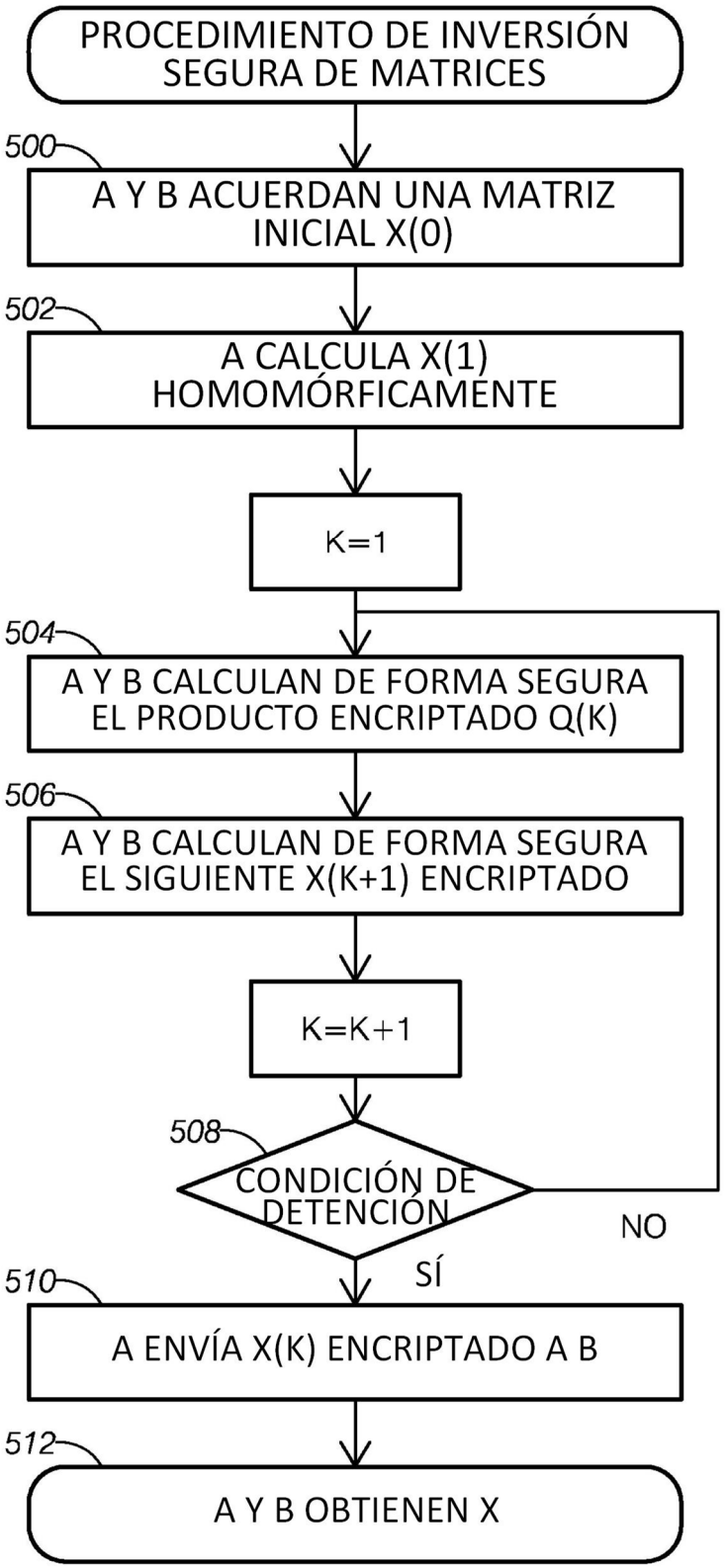
PROCEDIMIENTO DE INVERSIÓN SEGURA DE MATRICES
500
A Y B ACUERDAN UNA MATRIZ INICIAL X(0)
502
A CALCULA X(1) HOMOMÓRFICAMENTE
K=1
504
A Y B CALCULAN DE FORMA SEGURA EL PRODUCTO ENCRIPTADO Q(K)
506
A Y B CALCULAN DE FORMA SEGURA EL SIGUIENTE X(K+1) ENCRIPTADO
K=K+1
508
CONDICIÓN DE DETENCIÓN
NO
SÍ
510
A ENVÍA X(K) ENCRIPTADO A B
512
A Y B OBTIENEN X

FIG.5