(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 669 994**

(51) Int. CI.:

F42D 1/055 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.08.2014 PCT/ZA2014/000040**

(87) Fecha y número de publicación internacional: **19.03.2015 WO15039147**

(96) Fecha de presentación y número de la solicitud europea: **26.08.2014 E 14843538 (1)**

(97) Fecha y número de publicación de la concesión europea: **04.04.2018 EP 3042148**

(54) Título: **Control selectivo de grupos de detonadores**

(30) Prioridad:

04.09.2013 ZA 201306625

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.05.2018

(73) Titular/es:

DETNET SOUTH AFRICA (PTY) LTD (100.0%)
AECI Place The Woodlands Woodlands Drive
Woodmead, ZA

(72) Inventor/es:

SCHLENTER, CRAIG CHARLES y
GOUNDEN, JONATHAN

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Control selectivo de grupos de detonadores.

Antecedentes de la invención

La presente invención se refiere al control selectivo de un detonador, o de un grupo de detonadores, en un sistema de voladura que incluye una pluralidad de los detonadores.

Cierto sistema de voladura utiliza las denominadas “claves inteligentes” las cuales contienen un identificador de grupo integrado que es exclusivo de un conjunto emparejado dado de claves. El identificador de grupo de claves acompaña a los mensajes de voladura en el sistema, y se valida para garantizar que las claves, que se están utilizando en el sistema, presentan identificadores coincidentes antes de permitir la voladura. El sistema también permite seleccionar un subconjunto de explosores, que deben participar en una voladura. Esto se realiza por medio de órdenes dirigidas a cada explosor con el fin de posibilitar la participación de ese explosor en actividades de voladura subsiguientes.

El documento US8385042 divulga un método de comunicación con un subgrupo de detonadores inalámbricos, que conlleva el envío de un identificador de grupo en un mensaje a los detonadores inalámbricos. A continuación, cada detonador debe verificar que el identificador de grupo transmitido coincide con un identificador que está almacenado internamente en el detonador. Se describe una técnica similar en el documento US2011/0174181 en el que un código identificador de transmisor debe coincidir con un código de receptor con el fin de iniciar un detonador.

El documento US7848078 divulga un método de comunicación con detonadores en el cual una señal de listado incluye codificación para garantizar que solamente un conjunto de detonador específico o un grupo específico de conjuntos de detonador reacciona a la señal. Esto se realiza usando diferentes frecuencias para la señal.

El documento WO2012/061850 describe una técnica en la que una orden de disparo se selecciona de manera específica, o se genera aleatoriamente, según se requiera. Este planteamiento permite lograr agrupamientos de detonadores seleccionando diferentes órdenes de disparo para diferentes grupos de detonadores. No obstante, otras órdenes de difusión general no se identifican como pertenecientes a un grupo específico.

El documento US2012/353203 presenta un sistema en el que una estructura de datos de seguridad, en comunicación con un explosor, contiene un identificador de sistema y un identificador de dispositivo. Esta técnica se puede usar para lograr un control selectivo de grupos de detonadores.

El documento WO 2012/149584 A1 describe un dispositivo de control destinado a usarse con un detonador. El dispositivo de control incluye una disposición sensora magnetorresistiva la cual, como respuesta a una señal inalámbrica predeterminada, produce una señal de control. Además, se proporcionan medios de procesador que extraen datos de la señal de control y que introducen los datos en un circuito de control del detonador.

El documento US 6.618.237 B2 divulga un conjunto electrónico de retardo de detonadores que tiene un detonador asociado que se puede preprogramar in situ con un retardo de tiempo y se puede instalar en una perforación para llevar a cabo una operación de voladura. En primer lugar, el conjunto se acopla a una unidad de programación para programar el retardo de tiempo deseado y, a continuación, a una unidad de voladura, por medio de un dispositivo de acoplamiento magnético en el conjunto electrónico de retardo y a un trayecto único de un hilo metálico conductor a través del dispositivo de acoplamiento magnético. El retardo de tiempo del programa y el conjunto de retardo electrónico se pueden comprobar doblemente con respecto a un enlace de comunicaciones inalámbricas entre el conjunto electrónico de retardo y la unidad de programación.

El documento US 2006/0027121 A1 divulga un método y un aparato para controlar una operación de voladura que usa un equipo de control de voladura para iniciar una pluralidad de detonadores en un emplazamiento de una voladura. Está relacionado con el control de una operación de voladura, y se proporciona un sistema mediante el cual una identidad de un usuario, que maneja el equipo de voladura, se verifica antes de que se habilite un controlador de voladura para ejecutar una orden de voladura. En otras palabras, se lleva a cabo un proceso de validación sobre información y, si la información es validada, se permite un uso al menos parcial del equipo de control de voladura. Una señal de solicitud que contiene la información a validar se puede transmitir de forma inalámbrica. Se puede adoptar cualquier técnica apta para cifrar y firmar digitalmente el mensaje. Se pueden usar técnicas criptográficas de pares de claves pública/privada.

En un sistema inalámbrico de detonadores, basado en el uso de conjuntos de detonador inalámbricos, las comunicaciones se logran normalmente por medio de señales que se transmiten modulando un campo magnético. Las frecuencias de funcionamiento son bajas para garantizar una propagación eficaz de la señal a través del suelo. Consecuentemente, las velocidades de transferencia de datos son también bajas. Un circuito receptor en un conjunto de detonador se puede sintonizar con una frecuencia específica por medio de un

receptor de Q alta, pero esta técnica hace que el uso de frecuencias independientes, para lograr un control específico de cada grupo, sea poco práctico. Si un identificador de grupo adicional acompaña a cada mensaje, entonces las comunicaciones serían más lentas de lo deseable.

Un objetivo de la invención es proporcionar un método de control de un conjunto de detonador seleccionado, o de un grupo seleccionado de conjuntos de detonadores, que no requiera la transmisión de un identificador de grupo con cada orden específica de cada grupo, y que no requiera el uso de frecuencias independientes. Esto permite reducir la tara de comunicación.

Este objetivo se alcanza con un método de comunicación que presenta las características de la reivindicación 1.

Sumario de la invención

La invención proporciona un método de acuerdo con la reivindicación 1.

En cada conjunto de detonador en el que se lleva a cabo el proceso de descifrado se calcula un código de validación a partir del mensaje descifrado y este se compara con el código de validación anexado al mensaje. Si los códigos de validación coinciden, el mensaje se procesa de manera adicional.

El cifrado de mensajes, y la transmisión de mensajes cifrados desde la ubicación de control, se puede repetir para eliminar, en la medida de lo posible, errores que son el resultado de mensajes dañados o de otras fuentes.

La transmisión del mensaje cifrado se puede realizar usando técnicas inalámbricas. En una forma de la invención, la transmisión se efectúa modulando una señal magnética.

El disparo de cualquier grupo de conjuntos de detonador requiere únicamente que la clave de cifrado correspondiente a ese grupo específico esté presente en la ubicación de control. Si se va a disparar un grupo adicional de conjuntos de detonador, entonces la clave de cifrado correspondiente a ese grupo se cargaría en la ubicación de control, por ejemplo, desde un dispositivo de programación, según se desee. No obstante, es posible almacenar una pluralidad de claves de cifrado en la ubicación de control. En cierta medida esto resulta cómodo ya que permite disparar de manera sucesiva múltiples grupos de conjuntos de detonador, sin interrumpir el proceso de disparo para cargar una clave de cifrado adicional para cada grupo particular de conjuntos de detonador que se va a disparar.

Breve descripción de los dibujos

La invención se describe de manera adicional, a título de ejemplo, haciendo referencia a los dibujos adjuntos, en los cuales:

La Figura 1 representa esquemáticamente un sistema de voladura en el cual se implementa el método de la invención; y

la Figura 2 representa una serie de etapas que se llevan a cabo en la implementación del método de la invención.

Descripción de la forma de realización preferida

La Figura 1 de los dibujos adjuntos ilustra un sistema de voladura 10 que incluye una unidad de control 12, típicamente un explosor en una ubicación de comunicaciones. El explosor está conectado directamente, o usando técnicas inalámbricas, a un bucle 20 que rodea una pluralidad de perforaciones 22 las cuales se han formado en el suelo en un banco de voladura. Cada perforación alberga un conjunto de detonador inalámbrico 24. La comunicación en el sistema es unidireccional, es decir, únicamente desde el explosor a los conjuntos de detonador, y se efectúa modulando un campo magnético el cual se establece energizando el bucle 20. Este aspecto se aporta únicamente a título de antecedentes.

En el método de la invención, las comunicaciones a través de la interfaz inalámbrica entre el explosor y los conjuntos de detonador se logra por medio de señales cifradas. Se fija una clave de cifrado individualmente para cada conjunto de detonador antes de la comunicación de grupo selectiva con los conjuntos de detonador. Cada clave se fija según cualquier manera adecuada. Por ejemplo, se puede utilizar un dispositivo portátil para programar una clave de cifrado en un conjunto de detonador antes de colocar el detonador en un barreno respectivo. Esta es una forma cómoda y fiable de vincular las claves cifradas con los conjuntos de detonador. Alternativamente, para transmitir una clave exclusiva, asociada a un conjunto de detonador, a ese detonador, se pueden utilizar técnicas inalámbricas de corto alcance u otras técnicas de comunicación.

La misma clave de cifrado exclusiva se carga y almacena en cada conjunto de detonador del cual se requiere que pertenezca a un grupo definido de conjuntos de detonador.

Grupos diferentes de conjuntos de detonador están asociados a claves exclusivas respectivas diferentes que son distintas de las claves usadas para otros grupos de conjuntos de detonador. La clave que se asocia a un grupo específico de conjuntos de detonador que van a ser disparados es almacenada y usada por el explosor. Si se va a disparar de manera sucesiva una pluralidad de grupos de conjuntos de detonador, entonces las claves de cifrado respectivas para estos grupos se almacenan, de manera preferente, simultáneamente, para su uso por el explosor.

Para comunicarse con un grupo seleccionado de conjuntos de detonador, se usa una clave de cifrado que está almacenada en una ubicación de control, la cual puede ser fija o móvil, y que está asociada de manera exclusiva a los conjuntos de detonador de ese grupo, con el fin de cifrar un mensaje. A continuación, el mensaje cifrado se difunde de manera general a todos los conjuntos de detonador. El mensaje cifrado se recibe en cada conjunto de detonador, y la clave de cifrado respectiva, almacenada previamente en dicho conjunto de detonador, se usa para implementar un proceso de descifrado. Este proceso únicamente se puede llevar a cabo de manera satisfactoria si la clave correcta para el descifrado del mensaje cifrado está disponible en ese conjunto de detonador.

La Figura 2 ilustra varias etapas en la implementación del método de la invención.

Una unidad de memoria 30 asociada al explosor 12 contiene una pluralidad de claves de cifrado K1... a KN. Cada clave de cifrado es exclusiva y distinta de las otras claves. Cada clave de cifrado está asociada a un conjunto de detonador 24 distinto, o a un grupo distinto de los conjuntos de detonador, en el sistema de voladura. Tal como se indica, en cada conjunto de detonador se carga según cualquier forma adecuada una clave de cifrado durante el establecimiento del sistema de voladura. De este modo, cada clave K1... a KN está vinculada a solamente un conjunto de detonador, o vincula entre sí un conjunto particular de conjuntos de detonador en un grupo definido.

Supóngase que un mensaje 32 se va a dirigir solamente a aquellos conjuntos de detonador del grupo que están asociados a la clave K1. En la ubicación de control, al mensaje se le anexa un código de validación 34. El código de validación, que puede ser una CRC, una suma de comprobación, una firma o un valor *hash*, según los requisitos, está destinado a proporcionar unos medios para monitorizar la integridad del mensaje cuando el mismo es transmitido, y para validar que el proceso de descifrado es satisfactorio, es decir, que el descifrado se realiza usando la clave asociada correcta. La combinación resultante 36 del mensaje y el código de validación se cifra en una etapa 40, con la clave K1. Esto produce un mensaje cifrado 42.

Posteriormente, el mensaje cifrado 42 se transmite a los conjuntos de detonador en el sistema. En esta solicitud, el mensaje 42 se transmite modulando un campo magnético que es establecido por el bucle 20 (etapa 44).

Cada conjunto de detonador 24 puede recibir cada mensaje modulado y transmitido (etapa 46). A continuación, se intenta un proceso de descifrado 48 usando una clave 50, la cual está asociada al conjunto de detonador. En este ejemplo, cada conjunto de detonador del grupo de destino tiene la clave almacenada K1. Los otros conjuntos de detonador tienen claves diferentes. En cada detonador, se usa la clave almacenada respectiva 50 en el proceso de descifrado 48. Después de esto, se vuelve a calcular (52) el código de validación basándose en el contenido del mensaje descifrado, y el mismo se compara, en una etapa 54, con el código de validación 34 que se usó en el punto de control y que acompañaba al mensaje recibido. Si la comparación no es satisfactoria, entonces no se lleva a cabo ninguna actividad adicional en ese conjunto de detonador con respecto al mensaje transmitido (etapa 56). Si la validación es satisfactoria, entonces se efectúa un proceso adicional (etapa 60) del mensaje, de manera que la instrucción contenida en el mensaje se puede ejecutar en el conjunto de detonador.

Debido a diversos factores, pueden producirse errores de transmisión que afecten a la integridad de la combinación transmitida de código de validación y mensaje. Por este motivo, el proceso antes mencionado se repite con el fin de reducir la probabilidad de aparición de errores cuando se implementa el sistema de voladura. Este es un aspecto importante, dado que la invención normalmente encuentra aplicación en un sistema en el que los conjuntos de detonador en el sistema no tienen la capacidad de transmitir señales de retorno a la unidad de control.

De este modo, la invención se basa en el uso de claves de cifrado exclusivas cada una de las cuales está asociada a un grupo definido de conjuntos de detonador. Se hace un uso selectivo de las claves de cifrado, según se requiera, con el fin de cifrar mensajes en una ubicación de control, y los mensajes cifrados se envían a todos los conjuntos de detonador. Consecuentemente, no es necesario transmitir un identificador de grupo con cada orden específica de cada grupo, para permitir que el grupo de destino responda a la orden.

El uso de un código de validación independiente no es estrictamente necesario. En sistemas típicos, a los mensajes ya les acompañan códigos de integridad de mensaje para garantizar su integridad, y estos códigos se pueden usar en el contexto del proceso de validación según se ha descrito en la presente. De esta manera, al mensaje no se le añaden datos adicionales, y no se incurre en ninguna tara de mensajería adicional.

En el proceso antes mencionado se puede aplicar una modificación en una situación en la que el número de posibles mensajes transmitidos N constituya un subconjunto pequeño del número de posibles codificaciones de mensajería M. Si N es significativamente menor que M, entonces, con un alto grado de probabilidad, un descifrado con una clave incorrecta no produciría un mensaje aparentemente válido N. En esta situación, no sería necesario ningún código de validación de mensajes. En su lugar, una determinación de que el mensaje descifrado es parte del conjunto N es suficiente para validar el mensaje y la clave con un alto grado de fiabilidad.

REIVINDICACIONES

1. Método de comunicación con por lo menos un conjunto de detonador que se selecciona de entre una pluralidad de conjuntos de detonador (24) en un sistema de voladura (10) que incluye una unidad de control (12) que está conectada, directamente o usando técnicas inalámbricas, a un bucle (20) que rodea una pluralidad de perforaciones (22), conteniendo cada una de ellas un conjunto de detonador inalámbrico (24), incluyendo el método las etapas siguientes:

1) proporcionar una pluralidad de claves de cifrado, estando cada clave de cifrado (50) asociada únicamente a un conjunto de detonador (24) seleccionado, o a un grupo seleccionado de conjuntos de detonador, en la pluralidad de conjuntos de detonador;

2) almacenar cada clave de cifrado (50) en el conjunto de detonador (24) seleccionado, o en el grupo seleccionado de conjuntos de detonador, al cual está asociada únicamente la clave de cifrado;

3) almacenar por lo menos una de dichas claves de cifrado (50) en una unidad de memoria (30) asociada a la unidad de control (12);

4) en la unidad de control (12), cifrar un mensaje (32) para formar un mensaje cifrado (42) destinado solamente a un conjunto de detonador (24) seleccionado, o a un grupo seleccionado de conjuntos de detonador, usando la respectiva clave de cifrado (50) que está asociada únicamente al conjunto de detonador (24) seleccionado o al grupo seleccionado de conjuntos de detonador;

5) transmitir el mensaje cifrado (42) a la pluralidad de conjuntos de detonador modulando una señal magnética que se establece energizando el bucle (20);

6) recibir dicho mensaje cifrado (42) en cada conjunto de detonador (24);

7) en cada conjunto de detonador (24), llevar a cabo un proceso de descifrado (48) sobre el mensaje recibido (42) usando la clave de cifrado (50) que está asociada únicamente al conjunto de detonador (24) para producir un mensaje descifrado;

8) validar (54) el mensaje descifrado; y

9) después de un proceso de validación satisfactorio, procesar adicionalmente el mensaje descifrado;

caracterizado por que, en la etapa 4, el mensaje (32) y el código de validación (34) anexado se cifran para producir el mensaje cifrado (42), y por que en cada conjunto de detonador (24), en el cual se lleva a cabo el proceso de descifrado (48), se calcula un código de validación (52) a partir del mensaje descifrado y este se compara con el código de validación (34), y si los códigos de validación (52/34) coinciden, el mensaje descifrado se procesa adicionalmente en una etapa (60).

2. Método según la reivindicación 1, que incluye la etapa, si surgen errores de mensajes dañados o de otras fuentes, de repetir por lo menos las etapas 5 a 8 para eliminar los errores.

3. Método según la reivindicación 1, que incluye la etapa, si aparecen errores como resultado de mensajes dañados o de otras fuentes, de repetir el cifrado de los mensajes (etapa 4), y la transmisión de mensajes cifrados (42) desde la unidad de control (12) para eliminar los errores.

4. Método según cualquiera de las reivindicaciones 1 a 3, en el que, en la etapa 3, una pluralidad de dichas claves de cifrado (K1... a KN) está almacenada en la unidad de memoria 30.

5. Método según cualquiera de las reivindicaciones 1 a 4, en el que, en la etapa 1, se usa un dispositivo portátil para programar la respectiva clave de cifrado (50), que está asociada a un conjunto de detonador (24) dado, en el conjunto de detonador (24) antes de que el conjunto de detonador sea colocado en un respectivo barreno.

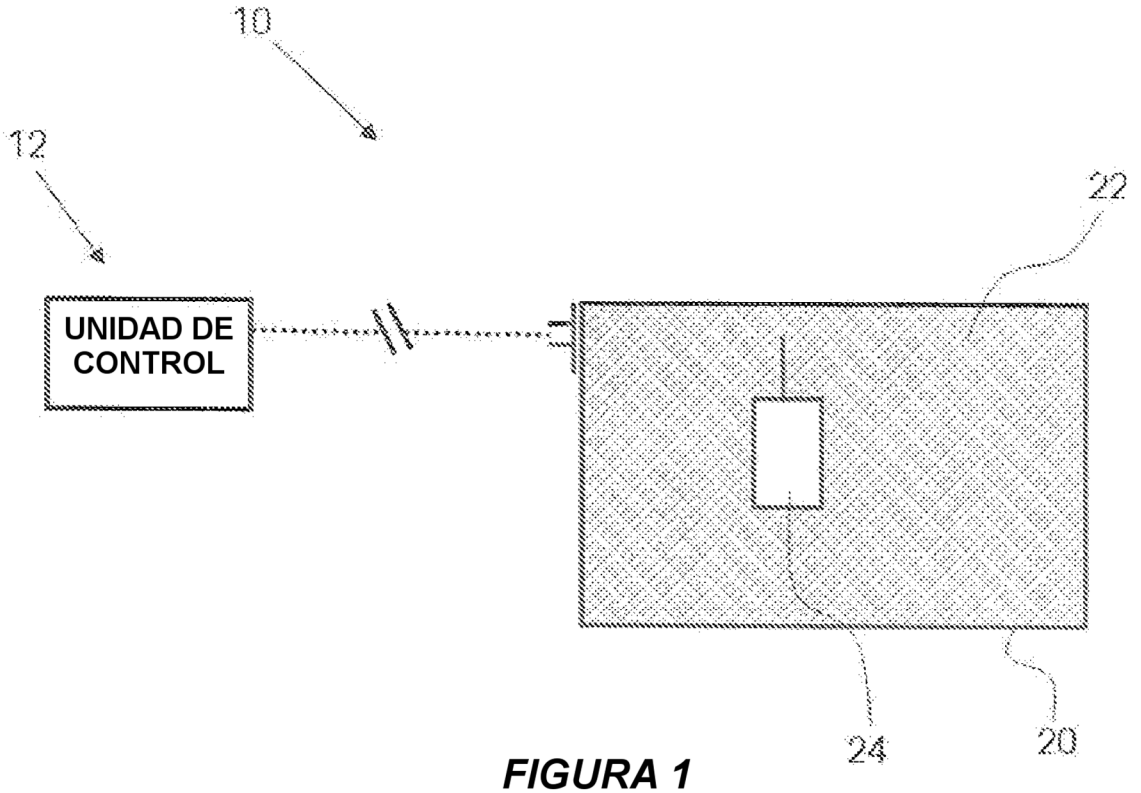
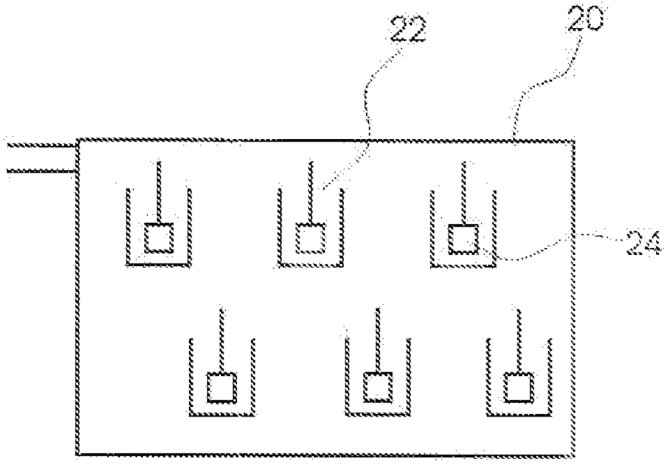


FIGURA 1



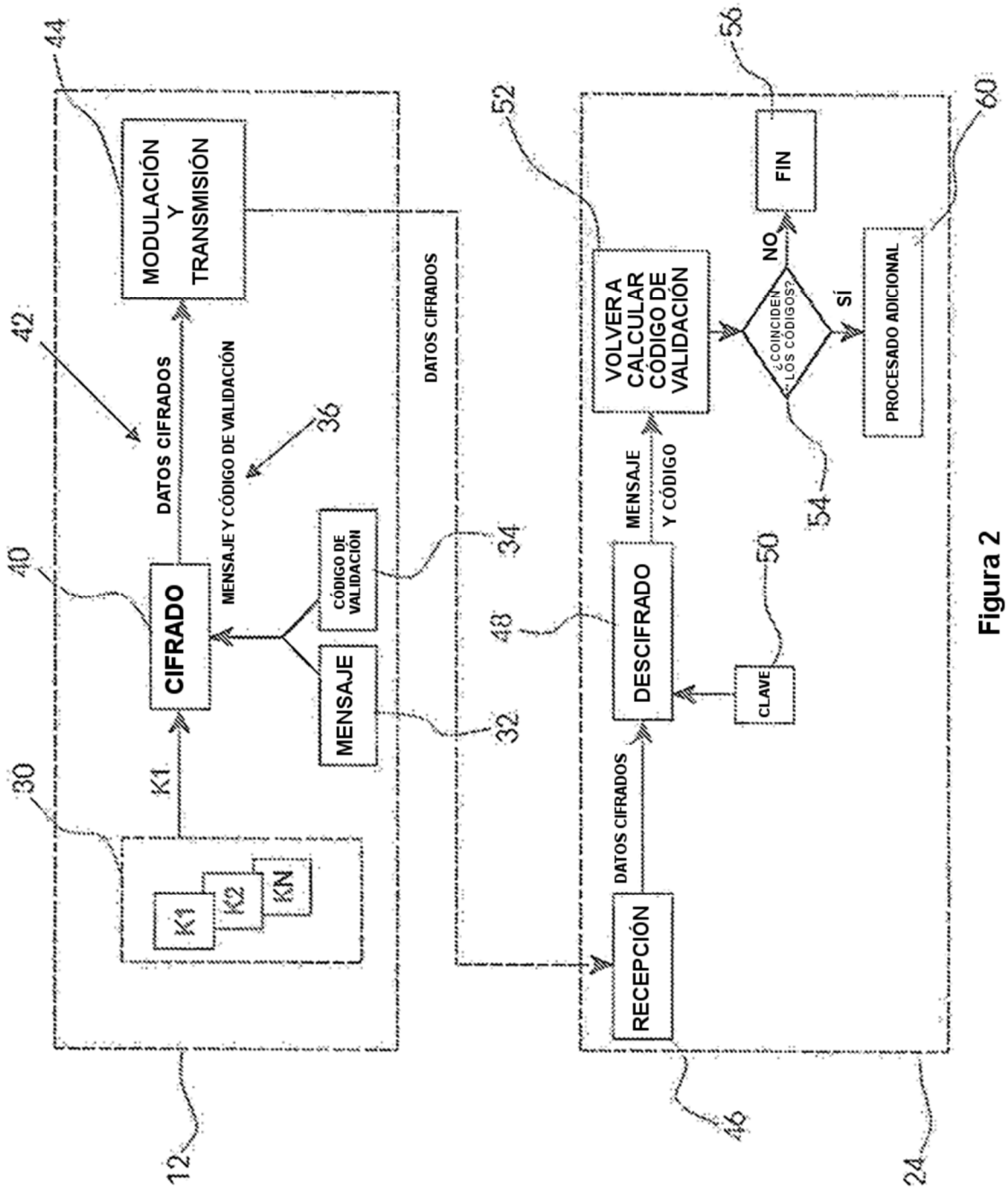

12
24
30
K1
K2
KN
40
CIFRADO
K1
42
DATOS CIFRADOS
MENSAJE Y CÓDIGO DE VALIDACIÓN
36
CÓDIGO DE VALIDACIÓN
MENSAJE
32
34
44
MODULACIÓN Y TRANSMISIÓN
DATOS CIFRADOS
46
RECEPCIÓN
DATOS CIFRADOS
48
DESCIFRADO
50
CLAVE
MENSAJE Y CÓDIGO
52
VOLVER A CALCULAR CÓDIGO DE VALIDACIÓN
54
¿COINCIDEN LOS CÓDIGOS?
NO
SÍ
56
FIN
60
PROCESADO ADICIONAL

Figura 2