(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 357 053**

(51) Int. Cl.:
G01S 13/78 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **02292172 .0**
(96) Fecha de presentación : **03.09.2002**
(97) Número de publicación de la solicitud: **1291672**
(97) Fecha de publicación de la solicitud: **12.03.2003**

(54) Título: **Procedimiento y dispositivo para generar varios canales en un sistema de tipo IFF.**

(30) Prioridad: **07.09.2001 FR 01 11618**

(45) Fecha de publicación de la mención BOPI:
15.04.2011

(45) Fecha de la publicación del folleto de la patente:
15.04.2011

(73) Titular/es: **THALES**
173, boulevard Haussmann
75008 Paris, FR

(72) Inventor/es: **Martin, Jean-Claude**

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

La presente invención se refiere a un procedimiento y un dispositivo para generar o crear canales o modos de interrogación en un sistema de tipo IFF (Identification Friend or Foe en inglés) que utilizan formas de onda de espectro extendido.

La invención se aplica especialmente en los sistemas de identificación IFF empleados en el campo de la aviación militar que funcionan con el Modo 5. El modo 5 es un modo de interrogación/respuesta cifrado que utiliza una forma de onda definida en la parte V del acuerdo de normalización de la OTAN, el STANAG 4193 y un algoritmo de cifrado propio. La figura 2 recuerda la estructura de esta forma de onda.

En la continuación de la descripción, se designa con la expresión “canal”, un modo de interrogación/respuesta cifrado aplicado en los sistemas de identificación IFF por pregunta/respuesta utilizando el Modo 5 pero con algoritmos de cifrado diferentes.

Cuando varios algoritmos de cifrado o también, para un mismo algoritmo de cifrado, cuando se utilizan claves de cifrado diferentes simultáneamente, no existe actualmente ningún medio para diferenciar los mensajes.

Un interrogador elige interrogar con un algoritmo de cifrado dado A o con claves específicas (Algo A). Un contestador no sabe con qué algoritmo o qué clave se han cifrado los mensajes que recibe.

Se pueden presentar entonces diversos casos:

- Si el contestador no está equipado más que con el algoritmo A, descifrará el mensaje de interrogación y contestará.
- Si el contestador no está equipado más que con el algoritmo B (Algo B) diferente del algoritmo A, no podrá responder a las interrogaciones pero su calculador criptográfico se utilizará para intentar descifrar el mensaje con el algoritmo A.
- Cuando el respondedor está equipado con algoritmos A y B, tendrá que tratar los mensajes con los dos algoritmos, bien en paralelo, bien en serie, si los plazos de tratamientos lo permiten. Responderá con el algoritmo que habrá dado un mensaje de interrogación comprensible y válido.

La patente francesa FR 2 632 421 se refiere a sistemas de identificación del tipo IFF modo 4. La invención consiste en modificar el preámbulo del mensaje de identificación IFF modo 4 efectuando una modulación por inversión de fase de algunos de los impulsos del preámbulo de este mensaje.

La idea de la presente invención consiste, especialmente, en crear canales independientes que permiten tener simultáneamente varios tipos de algoritmos de cifrado o carias claves diferentes para un mismo algoritmo de cifrado y que permiten al sistema tratar los mensajes sin tener que recurrir a tratamientos paralelos o en serie. El sistema tiene la posibilidad de reconocer los diferentes mensajes sea cual sea el algoritmo de cifrado o las claves de cifrado utilizados y determinar el algoritmo a usar para descifrar las interrogaciones y las respuestas.

Para esto, los símbolos de preámbulo del mensaje de interrogación se modulan y el contestador al detectar la modulación del preámbulo sabe qué algoritmo o qué clave se han utilizado.

Las interrogaciones realizadas con un algoritmo A no perturban un contestador que no está equipado con el algoritmo A. De hecho, los dos modos de interrogación/respuesta, algoritmo A y algoritmo B, aplicados en el sistema interrogador-contestador se ignoran y no se perturban. Esto evita de hecho tratamiento adicionales y ocupaciones intempestivas de los calculadores.

La invención se refiere a un procedimiento de interrogación/contestador en un sistema de comunicación de tipo IFF (Modo 5) que comprende un interrogador y un contestador, caracterizado porque comprende:

- respecto del interrogador al menos una etapa de modulación de los impulsos de un mensaje de interrogación utilizando una función de modulación elegida entre una familia casi ortogonal:
- respecto del contestador, al menos una etapa de detección de la función de modulación utilizada para el preámbulo y de determinación del algoritmo para la descodificación de las informaciones contenidas en el mensaje.

La función de modulación o de ensanchamiento es por ejemplo una función de Walsh de 16 bits.

El procedimiento se aplica por ejemplo en un sistema de identificación que utiliza el Modo 5 con diferentes algoritmos de cifrado y/o claves diferentes y el Modo 4.

La invención se refiere también a un dispositivo para generar varios canales en un sistema de interrogación/respuesta de tipo IFF que comprende un interrogador y un contestador, caracterizado porque comprende:

- en un interrogador, un medio adaptado para modular los impulsos del preámbulo de un mensaje de interrogación Modo 5 con la ayuda de una función de modulación elegida entre una familia de funciones casi ortogonales,
- en un contestador, un medio adaptado para determinar la función de modulación de los impulsos del preámbulo el algoritmo para descodificar las informaciones contenidas en el mensaje.

El dispositivo se adapta por ejemplo para generar una función de modulación de tipo función de Walsh.

La presente invención presenta especialmente las siguientes ventajas:

- Los canales de transmisión obtenidos son diferentes según los algoritmos, lo cual permite al sistema reconocer automáticamente el algoritmo que debe utilizar para descifrar las interrogaciones y las respuestas,
- Varios sistemas pueden de este modo funcionar simultáneamente con algoritmos de cifrado diferentes sin generar una ocupación inútil de los sistemas presentes en el entorno,
- Las capacidades de cifrado de cada canal pueden aumentar variando la función de modulación utilizada, por ejemplo la función de Walsh en función del tiempo,
- Un transpondedor dado puede recibir simultáneamente sobre varios canales sin necesitar el tratamiento de todos los mensajes paralela o secuencialmente en cada canal,
- Al ser cada canal independiente, es posible definir mensajes específicos para un canal dado, lo cual aumenta las capacidades operativas de los sistemas,
- Al presentar la secuencia de Walsh como particularidad el hecho de ser específica de un algoritmo y asociada a las eventuales evoluciones del preámbulo, la invención ofrece una seguridad adicional al mensaje.
- El Modo de interrogación/respuesta Modo 4 aplicado en los sistemas IFF actuales, utiliza una forma de onda con un preámbulo de 4 impulsos sin ensanchamiento y corresponde a un canal según la invención.

Otras características y ventajas de la invención aparecerán mejor en la siguiente descripción ofrecida a título ilustrativo y en modo alguno limitativo respecto de las figuras anexas que representan:

- La figura 1 es un ejemplo de estructura de intercambio de mensajes de interrogación/respuesta en un sistema IFF,
- La figura 2 es la estructura de un mensaje de interrogación del Modo 5 sin modulación,
- La figura 3 es la estructura de un mensaje de interrogación del Modo 4,
- La figura 4 es un ejemplo de estructura del preámbulo del mensaje en Modo 5 modulado por ensanchamiento.

La figura 1 recuerda el principio de interrogación/respuesta en un sistema donde la interrogación se hace con un modo cifrado dado para un contestador del mismo modo cifrado por ejemplo.

Un sistema IFF que comprende un interrogador 1 asociado a un calculador 2 de criptografía, interroga un contestador 3 emitiendo un mensaje de interrogación M en modo 5 cuyo formato se detalla en la figura 2. el contestador 3 determina en qué Modo se interroga, por ejemplo, en modo 4 o en Modo 5, según un canal conocido con las claves correctas o no. Transmite a continuación el mensaje de interrogación M al calculador 4 de criptografía al cual se conecta. En el caso de una interrogación válida, transmite un mensaje de respuesta R al interrogador.

Un contestador 3 está por ejemplo equipado con una interfaz específica adaptada para responder en el modo de interrogación únicamente.

Se dan diferentes ejemplos de arquitectura de sistemas IFF por ejemplo en el documento cuyo título es “Secondary Surveillance Radar” de Michael C.Stevens, Editions Artech House, Boston, 1988.

La figura 2 representa esquemáticamente el formato o la estructura del mensaje de interrogación del Modo 5. Está compuesto por un grupo de cuatro impulsos P_1, P_2, P_3, P_4 seguido de dos impulsos opcionales de mando ISLS de supresión de las interrogaciones en lóbulos secundarios y de un grupo D de impulsos de información compuesto por

impulsos modulados por ensanchamiento según leyes cifradas. Los impulsos del preámbulo se espacian de tal manera que, T_1 corresponde a la diferencia temporal entre los dos impulsos extremos P_1 y P_4, T_2 a la diferencia entre los impulsos P_4 y P_2 y T_3 a la diferencia entre los impulsos P_4 y P_3.

La figura 3 representa la estructura del Modo 4. Este mensaje se compone de un grupo de cuatro impulsos P_1, P_2, P_3 y P_4 seguido de un impulso P_5 de mando de supresión de las interrogaciones en los lóbulos secundarios (ISLS) y de un grupo de impulsos de información compuesto por 32 posiciones que pueden o no estar ocupadas por un impulso. Todos los impulsos y posiciones están espaciados por 2 µs y cada impulso dura 0,5 µs, por ejemplo. El grupo de información empieza 10 µs después del primer impulso P_1. En este grupo de 32 impulsos posibles, cuando posiciones de impulsos contiguos están libres se introduce en posiciones que corresponden a múltiplos impares de microsegundo de los impulsos anti-interferencia (All). El primero de estos impulsos puede ser de 9 µs de P_1.

La figura 4 representa esquemáticamente los impulsos del preámbulo modulados por funciones ortogonales o casi ortogonales o también funciones de Walsh conocidos por el experto en la técnica. Estas funciones se eligen de manera a crear canales de comunicación independientes. El valor de la secuencia de ensanchamiento se define con un objetivo de interoperabilidad. Las secuencias utilizadas se eligen con el fin de ser las más ortogonales posibles entre los diferentes canales.

El procedimiento comprende, por ejemplo, las siguientes etapas:

- modular los impulsos del preámbulo del mensaje de interrogación utilizando funciones de Walsh o funciones ortogonales o casi ortogonales con el fin de diferenciar los diferentes canales, y
- reconocer la secuencia de ensanchamiento del preámbulo del mensaje con el fin de determinar, por ejemplo automáticamente, el algoritmo a aplicar para la descodificación de las informaciones contenidas en el mensaje.

Para esta segunda etapa, el dispositivo según la invención comprende por ejemplo, un procesador provisto de una función de software o también una serie de correladores dispuestos en paralelo o en serie.

La modulación de los cuatro impulsos del preámbulo del mensaje de interrogación por funciones de Walsh de 16 bits permite generar canales distintos y utilizar en cada canal un algoritmo de cifrado diferente, utilizando cada canal una función diferente.

El procedimiento también puede comprender una etapa de gestión y de generación dinámica de los canales durante el funcionamiento del sistema de interrogación-respuesta. En función de las necesidades del sistema en interrogaciones-respuestas, es posible variar y adaptar los canales. El dispositivo está entonces equipado por ejemplo con un procesador provisto de un software.

En los sistemas relacionados con la invención, un interrogador elige por ejemplo interrogar en Modo 4 o en Modo 5 con una canal dado. El contestador se adapta para funcionar con uno o dos modos y uno o más canales simultáneamente.

Un ejemplo de realización de la invención se ofrece a continuación:

Del lado del interrogador:

La modulación de los impulsos del preámbulo del mensaje se realiza en función del canal elegido. El Modo 4 se considera como un canal sin modulación.

Del lado del contestador:

Según el estado de la técnica, la modulación de los impulsos del preámbulo se puede determinar de varias maneras, por muestreo de la señal, por correladores dispuestos en serie o en paralelo. La modulación de los impulsos del preámbulo determina el canal de recepción de las interrogaciones así como el algoritmo de descifrado a tener en cuenta. Esta información es corroborada por la información sobre las características de transmisión del canal, espaciado de los impulsos de preámbulo (T_1, T_2, T_3 en la figura 2) y ensanchamiento de los datos. Estos valores son en un instante dado específicos del canal elegido.

REIVINDICACIONES

1.- Procedimiento de interrogación/respuesta en un sistema de comunicación de tipo IFF Modo 5 que comprende un interrogador y un contestador, **caracterizado porque**

- respecto del interrogador al menos una etapa de modulación de los impulsos del preámbulo de un mensaje de interrogación utilizando una función de modulación elegida entre una familia de funciones casi ortogonales en función de la codificación de las informaciones contenidas en el mensaje,

- respecto del contestador, al menos una etapa de detección de la función de modulación utilizada para el preámbulo y de determinación del algoritmo para la descodificación de las informaciones contenidas en el mensaje.

2.- Procedimiento según la reivindicación 1, **caracterizado porque** se utiliza como función de modulación una función de Walsh de 16 bits.

3.- Procedimiento según cualquiera de las reivindicaciones 1 y 2, **caracterizado porque** comprende una etapa de gestión dinámica de las funciones de modulación o de ensanchamiento y de programación de varios canales de transmisión de las interrogaciones IFF Modo 5.

4.- Aplicación del procedimiento según cualquiera de las reivindicaciones 1 a 3 en un sistema de identificación que utiliza el Modo 5 con diferentes algoritmos de cifrado y/o claves diferentes y el Modo 4.

5.- Dispositivo para generar varios canales en un sistema de interrogación/respuesta de tipo IFF que comprende un interrogador y un contestador, **caracterizado porque** comprende:

- en un interrogador, un medio adaptado para modular los impulsos del preámbulo de un mensaje de interrogación Modo 5 con la ayuda de una función de modulación elegida entre una familia de funciones casi ortogonales, en función de la codificación de las informaciones contenidas en el mensaje,

- en un contestador, un medio adaptado para determinar la función de modulación de los impulsos del preámbulo y el algoritmo para descodificar las informaciones contenidas en el mensaje.

6.- Dispositivo según la reivindicación 5, **caracterizado porque** comprende un dispositivo adaptado para generar una función de modulación de tipo función de Walsh.

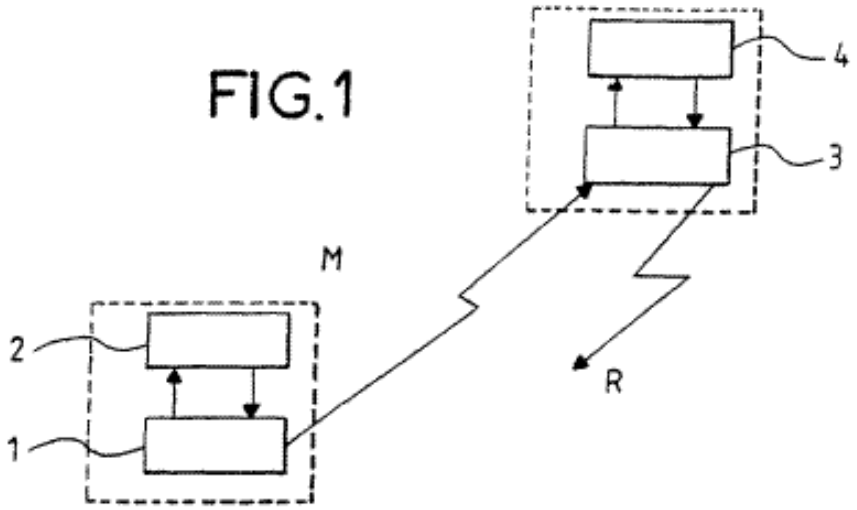
7.- Dispositivo según cualquiera de las reivindicaciones 5 y 6, **caracterizado porque** comprende uno o más correladores para determinar la función de ensanchamiento utilizada, dichos correladores se disponen en serie y/o en paralelo.

8.- Dispositivo según cualquiera de las reivindicaciones 5 y 6, **caracterizado porque** comprende un procesador adaptado para determinar la función de ensanchamiento.

9.- Dispositivo según cualquiera de las reivindicaciones 5 a 8, **caracterizado porque** comprende un procesador equipado con un software para administrar y generar varios canales elegidos en función de las necesidades de interrogaciones/respuestas

10.- Dispositivo según cualquiera de las reivindicaciones 5 a 9 **caracterizado porque** el contestador está equipado con una interfaz específica elegida en función del modo de interrogación.

FIG.1



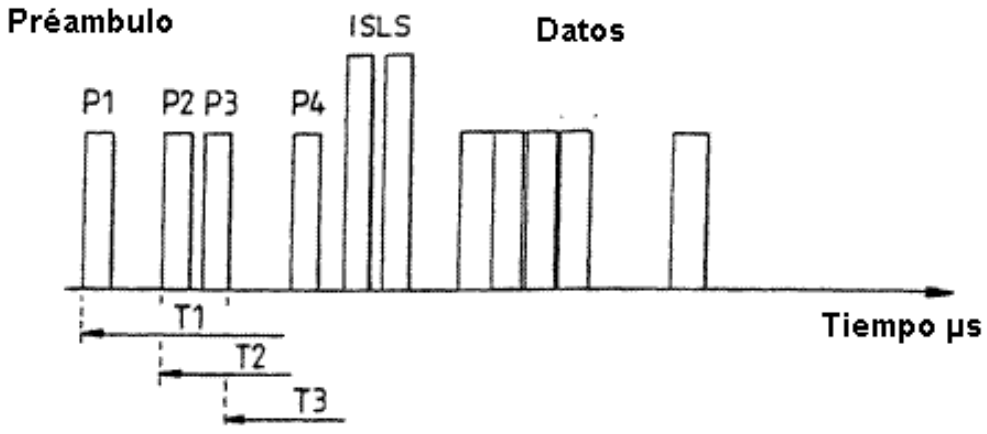


FIG.2

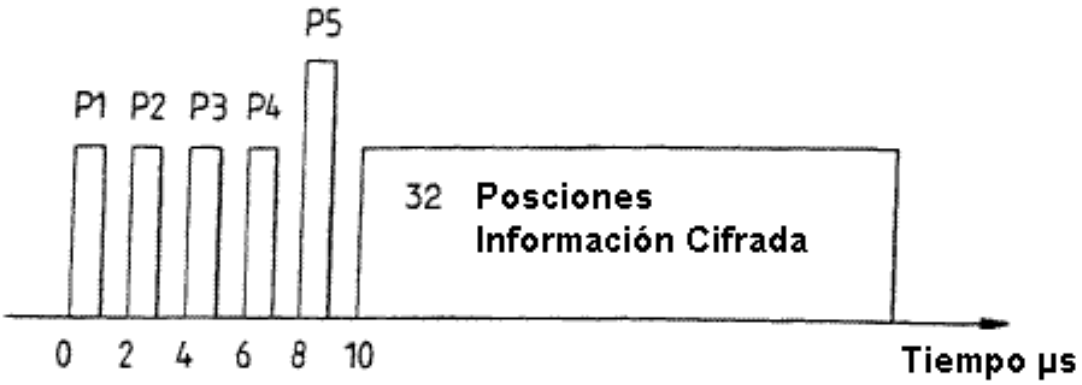
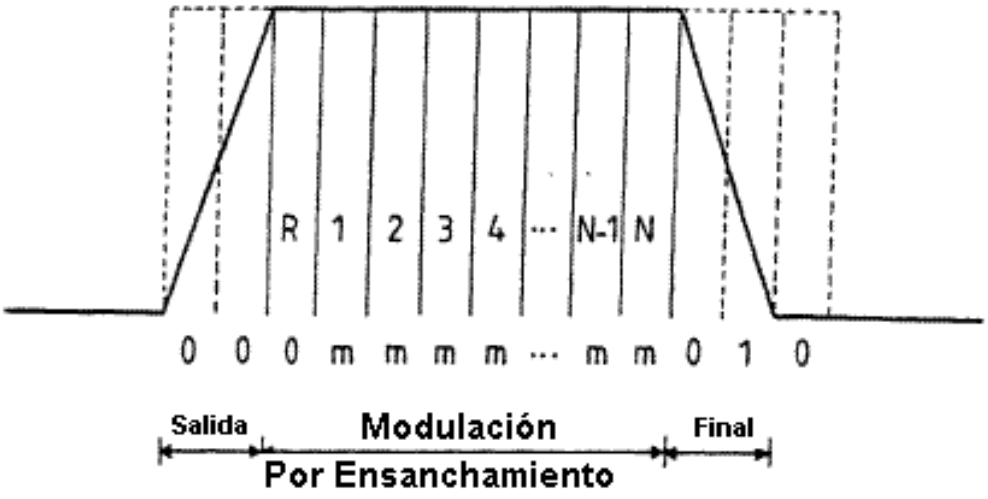

P5
P1 P2 P3 P4
32 Posciones
Información Cifrada
0 2 4 6 8 10
Tiempo µs

FIG.3


R 1 2 3 4 ··· N-1 N
0 0 0 m m m m ··· m m 0 1 0
Salida
Modulación
Por Ensanchamiento
Final