MINISTERIO DE INDUSTRIA
REGISTRO DE LA PROPIEDAD INDUSTRIAL

ESPAÑA

(19) ES (11) (21) NUMERO 464814 (10) A1

(22) FECHA DE PRESENTACION

PATENTE DE INVENCION

(30) PRIORIDADES:

(31) NUMERO	(32) FECHA	(33) PAIS
77 16.098	26 de Mayo de 1.977	Francia

(47) FECHA DE PUBLICIDAD	(51) CLASIFICACION INTERNACIONAL	(62) PATENTE DE LA QUE ES DIVISIONARIA
	G 06 K	

(54) TITULO DE LA INVENCION

" SISTEMA DE TRATAMIENTO DE INFORMACIONES PROTEGIENDO EL SECRETO DE INFORMACIONES CONFIDENCIALES "

(71) SOLICITANTE (S) La sociedad Anónima Francesa:
COMPAGNIE INTERNATIONALE POUR L'INFORMATIQUE CII-HONEYWELL BULL

DOMICILIO DEL SOLICITANTE

96, Avenue Gambetta 75960 PARIS CEDEX 20 (Francia)

(72) INVENTOR (ES)

Georges, Jean, Louis Giraud.

(73) TITULAR (ES)

(74) REPRESENTANTE

DON FRANCISCO GARCIA CABRERIZO

N/Ref.: O.G. 33507/J.M.
S/Ref.: DFJF/PI/ND/771912019.

UNE A-4 MOD. 3106

Concedido el Registro de acuerdo con los datos que figuran en la presente descripción y según el contenido de la Memoria adjunta.

UTILICESE COMO PRIMERA PAGINA DE LA MEMORIA

20 JUL. 1978

Entre este tipo de sistemas, se distingue un primer ejemplo en el que el sistema comprende una máquina de tratamiento de datos unida a un dispositivo de transmisión de informaciones por el que un operador puede comunicarse con la máquina. La misma comprende un dispositivo auxiliar en el que es memorizada una información confidencial predeterminada, llamada clave, que condiciona el acceso a la máquina. No se autoriza un diálogo entre un operador y la máquina más que si el código confidencial conservado por el operador es reconocido como idéntico a la clave.

Un segundo ejemplo es el de los sistemas que utilizan tarjetas de crédito y/O de débito. En este caso, el dispositivo auxiliar está constituido por una tarjeta personal, conservada por un operador, en la que es memorizada la clave personal. El acceso a la máquina es reservado a todo usuario de la tarjeta que conozca el código confidencial idéntico a la clave. Solamente si el dispositivo de transmisión de informaciones detecta esta identidad, el usuario de la tarjeta puede tener acceso a las informaciones confidenciales contenidas en la máquina.

En estos dos tipos de ejemplo cuando un operador quiere dialogar confidencialmente con una máquina, comienza introduciendo, generalmente en un teclado, el código confidencial que, una vez reconocido como idéntico a la clave, le permite enviar otras informaciones por el mismo teclado y el dispositivo de transmisión intermediario entre el operador y la máquina. En el caso del primer ejemplo dado más arriba, un defraudador, en posesión del código confidencial, puede tener también acceso directamente a la máquina inscribiendo el código en el teclado. En el caso de

un sistema que utilice tarjetas de crédito, el defraudador debe peseer además la tarjeta en la que está memorizada la clave correspondiente al código confidencial que posee. Se impone una doble protección en este último caso. En efecto, si un defraudador consigue sustraer una tarjeta es preciso obrar de manera que no pueda leer la clave memorizada en - la misma. Por otra parte es preciso evitar que pueda interceptar el código confidencial conservado por el legítimo - posesor de la tarjeta cuando lo inscribe el mismo en el teclado (que es un dispositivo público) en el curso de una - operación precedente de iniciación de diálogo con la máquina.

La detección de identidad del código confidencial inscrito por un usuario y de la clave memorizada en la tarjeta conservada por el mismo se realiza por comparación - del código con la clave. Una solución consiste en efectuar esta comparación colocando un comparador en el dispositivo de transmisión de informaciones conectado localmente con - un teclado. Esta solución tiene el inconveniente de permitir a un defraudador la posibilidad de interceptar la clave en el momento en que la misma es leída para ser comparada con el código inscrito por un usuario en el teclado. - Otra solución que ha sido hecha posible por la evolución de la tecnología de los circuitos integrados consiste en incluir el comparador en la misma tarjeta que la memoria que contiene la clave. Se evita así toda interceptación durante la lectura de la memoria, no estando ya la misma físicamente separada del comparador como en el caso precedente.

Sin embargo esta última solución no elimina el - riesgo de una interceptación durante la transferencia del

código inscrito en el teclado hasta el comparador. En efecto, el teclado, implantado al nivel del dispositivo de transmisión, está pues físicamente separado de la tarjeta en la que se encuentra el comparador.

La invención propone una solución para proteger el secreto del código confidencial en los sistemas de tratamiento de la información.

Un sistema de tratamiento de informaciones de acuerdo con la invención es del tipo que comprende una máquina de tratamiento de informaciones provista de un dispositivo de transmisión de informaciones y de un dispositivo auxiliar, comprendiendo el dispositivo auxiliar medios de memorización permanente de una clave y medios de comparación de esta clave con un código confidencial, permitiendo el código confidencial predeterminado dar un acceso exclusivo a la máquina por el dispositivo de transmisión de informaciones, estando caracterizado porque el dispositivo auxiliar comprende una pluralidad de elementos de contacto unidos respectivamente por una conexión integrada con los medios de comparación, estando concebida la pluralidad para engendrar, por contacto exterior al dispositivo auxiliar, un conjunto de informaciones elementales que constituyen un código confidencial comparable con dicha clave.

Las características y ventajas de la invención se desprenderán más claramente de la descripción que sigue, hecha con referencia a las figuras anexas, en las que:

- La figura 1 es un esquema de principio del sistema de tratamiento de informaciones según la invención;

- La figura 2 es un primer ejemplo de realización del dispositivo auxiliar contenido en el sistema de la fi-

gura 1 según la invención;

- La figura 3a es un ejemplo de realización de un dispositivo de control de contacto asociado con el dispositivo auxiliar de la figura 2;

- La figura 3b es un ejemplo de realización de un circuito selector contenido en el dispositivo auxiliar de la figura 2;

- La figura 4 es un segundo ejemplo de realización del dispositivo auxiliar contenido en el sistema de la figura 1, según la invención;

- La figura 5 es un ejemplo de realización de un circuito de recuento contenido en el dispositivo auxiliar de la figura 4;

- La figura 6 es un cronograma de señales engendradas en el dispositivo auxiliar de la figura 4.

El sistema de tratamiento de informaciones según la invención comprende, en la figura 1, una máquina MA de tratamiento de datos, un dispositivo DT de transmisión de informaciones. El sistema comprende además, en la figura 1, un dispositivo auxiliar DA unido por dos salidas 10 y 11 respectivamente con dos entradas 12 y 13 del dispositivo DT. El dispositivo auxiliar DA comprende una memoria MCL en la que es memorizada una clave, predeterminada, constituyendo una aplicación propia del dispositivo auxiliar que la contiene. Un comparador Cp, del dispositivo DA, está unido con la memoria MCL por entradas 14 para comparar la clave CLE con una información codificada IC recibida por otras entradas 15 del comparador Cp, proveniente de un codificador CD.

El comparador Cp está concebido para engendrar -

en una primera salida una señal SV enviada a la salida 10 del dispositivo DA cuando la información IC recibida por las entradas 15 es idéntica a la clave CLE recibida por las entradas 14. Por una segunda salida del comparador Cp se transmite una señal SE a la salida 11 del dispositivo DA cuando la información IC es diferente de la clave CLE. Un conjunto de N conexiones integradas c1, c2, c3..., cN unen N elementos de contacto T1, T2, T3,... TN respectivamente con N entradas del codificador CD. La pluralidad 16 de N elementos de contacto está concebida para ser accesible desde el exterior del dispositivo auxiliar por un operador, pudiendo así inscribir el mismo en el codificador CD un código confidencial CC de n bitios por contacto sucesivamente con n elementos entre los N elementos de contacto, siendo el número n inferior o igual a N.

Un primer ejemplo de realización del dispositivo auxiliar DA, de la figura 1 está representado en la figura 2, así como un modo particular de realización de contacto con los elementos de la pluralidad 16, de las figuras 1 y 2, para la introducción de un código confidencial CC por un operador. El contacto es asegurado por la aplicación de una punta P unida eléctricamente a masa, pudiendo ser accesible cada elemento de contacto o "tecla" por una ventana prevista en el plástico, cuando el dispositivo auxiliar es, por ejemplo, una tarjeta de crédito. La pluralidad 16 de la figura 2 comprende 10 teclas: T0, T1, T2...T9, así como una tecla suplementaria VC que permite validar en la tarjeta sucesivamente los diferentes elementos del código confidencial inscrito por el operador. Así, por ejemplo, si el operador quiere introducir el código 2356, aplica la punta

P sobre la tecla VC después de haberla aplicado sobre cada una de las teclas T2, T3, T5 y T6. Un dispositivo de control DC está unido con la punta P. por medio de un cordón por el que circula normalmente una corriente eléctrica cada vez que se pone la punta en contacto con una tecla. Este dispositivo DC está concebido de una parte, para unir la punta a la masa y de otra parte para controlar que cada contacto ha sido establecido efectivamente con la tarjeta por la aplicación de la punta P. El control de contacto es realizado por ejemplo, bien sea por una señal sonora emitida por un elemento Bip, o bien por una señal luminosa emitida por un elemento de visualización VISU de la figura 2. El codificador CD de la figura 1 comprende 10 entradas, en la figura 2, unidas con las 10 teclas T0, T1, T2...T9, respectivamente por 10 conexiones integradas c0, c1, c2... c9. El codificador CD emite una información codificada Ie por 4 salidas unidas respectivamente con las entradas 20, 21, 22 y 23 de un registro tampón RT del dispositivo DA. La información Ie es engendrada por codificación de un elemento del código CC inscrito por el apriete de una de las teclas T0 a T9 con ayuda de la punta. Cada vez que el codificador CD está listo para emitir una nueva información Ie, emite una señal por una quinta salida que permite la vuelta a cero del registo RT por una entrada 24. La información Ie que, en el esquema de principio de la figura 1, es enviada al comparador Cp por entradas 15 en paralelo, es transmitida en la figura 2, por mediación de un circuito selector S, a una entrada 15' de un comparador Cpl que recibe uno por uno los 4 bitios que constituyen la información Ie. El circuito selector S está concebido para emitir, uno por uno, los -

cuatro bitios de la información Ie que recibe en paralelo por 4 entradas 25, 26, 27, 28, bajo el mando de un contador Cptl que envia señales sucesivamente a otras cuatro entradas 29, 30, 31 y 32 del circuito S. El contador Cptl es mandado por señales de reloj SHO recibidas por una entrada 33 del dispositivo DA. Estas señales SHO son emitidas, por ejemplo, por un circuito reloj no representado, contenido en la máquina MA de tratamiento de informaciones con la que está unido el dispositivo DA por mediación del dispositivo DT. El funcionamiento del contador Cptl es declarado válido por señales recibidas por una entrada 34 unida por una conexión integrada clO con la tecla VC, cada vez que la misma está en contacto con la punta P. Con fines de sincronización, el contador Cptl es utilizado igualmente para leer la clave CLE, bitio por bitio, en la memoria MCL de las figuras 1 y 2. El contador Cptl está unido por una quinta salida con una entrada 35 de un generador de dirección GA concebido para efectuar la lectura de la clave CLE, bitio por bitio, en la memoria MCL y enviar cada bitio a una entrada 14' del comparador Cpl. Al mismo tiempo el comparador Cpl recibe por una entrada 15' cada bitio de la información Ie enviada por el circuito selector S bajo el mando del comparador Cptl, respectivamente por señales recibidas sucesivamente en las entradas 29, 30, 31, 32. Si cada bitio de la clave CLE y de la información IC, constituida por un conjunto de n informaciones Ie, es idéntico, se envía una señal SV a la salida 10 del dispositivo DA, mientras que en caso de diferencia es enviada una señal SE a la salida 11.

Un ejemplo de realización del dispositivo de con

trol DC es dado en la figura 3a. Este dispositivo comprende un fotoacoplador PC1 conectado, por la entrada 36 con el cordón de la punta P de la figura 2, y con un transistor T1 unido a masa. Los elementos sonoro y de visualización Bip y VISU, de las figuras 2 y 3a están unidos con el fotoacoplador PC1 por dos monoestables CI1 y CI 2 del dispositivo DC. El monoestable CI2 está unido de una parte con los elementos Bip y VISU por dos inversores 37 y 38 y de otra parte con el transistor T1 por un inversor 39. Los dos monoestables CI1 y CI2 son vueltos a cero por una entrada 40 del dispositivo DC que está unido por ejemplo con un circuito común de vuelta a cero de la máquina MA. Cuando se aplica la punta P sobre una de las teclas del dispositivo DA, circula una corriente por el cordón y va a la masa a través del fotoacoplador PC1 y el transistor T1 que está saturado. Esta corriente es detectada por PC1 que envía un impulso negativo a la entrada del monoestable CI1 que, por unión con el monoestable CI1, permite saturar el transistor T1 unido por el inversor 39. Los elementos Bip y VISU, unidos respectivamente con las salidas Q y $\overline{Q}$ del monoestable CI2 son así activados alternativamente en caso de contacto establecido por la punta P o no.

El circuito selector S de la figura 2 comprende en la figura 3b, un conjunto de 4 puertas Y 41, 42, 43, 44, unidas por una primera entrada con las entradas 25, 26, 27, 28, respectivamente y por una segunda entrada con las entradas 29, 30, 31, 32 respectivamente. Las salidas de las 4 puertas Y están unidas respectivamente con cuatro entradas de una puerta O 45 cuya salida está unida con una salida 46 por la que el circuito S envía, bitio por bitio, la

información Ie a la entrada 15ª del comparador Cpl de la - figura 2. Así por señales enviadas del contador Cptl sucesivamente a las entradas 29, 30, 31, 32, los 4 bitios recibidos por las entradas 25, 26, 27, 28 son transmitidos sucesivamente por las puertas 41, 42, 43, 44, y la puerta 45, hacia la salida 46. El contador Cptl encargado de pilotar el circuito S para enviar secuencialmente los 4 bitios de la información Ie es puesto en funcionamiento por una primera señal recibida en su entrada 34, de la figura 2, cuando es puesta la tecla VC una primera vez a masa por el contacto de la punta.

En cada contacto de la punta con la tecla VC, el generador GA de la figura 2 es incrementado seguidamente en una unidad permitiendo así la lectura de los 4 bitios de la clave CLE inscrita en la memoria MCL.

Otro ejemplo de realización del dispositivo auxiliar DA de la figura 1 es dado en la figura 4. Comprende un registro R2, unido al codificador CD y con la pluralidad 16 de las teclas T0, T1, T2... T9 de la figura 2, un generador de dirección GA unido a la memoria MCL de las figuras 1, 2. El dispositivo DA comprende, además, un circuito comparador Cp2, un circuito de recuento Cpt2 y un circuito de sincronización SYN.

El apriete de las teclas permite cargar el codificador CD por las conexiones integradas (de las figuras 1, 2, 4) y enviar una información codificada IC, elemento por elemento Ie, por cuatro salidas 2^0, 2^1, 2^2, 2^3, del codificador a las entradas A, B, C, D, del registo R2. En una salida S del codificador CD se engendra un impulso de muestreo enviado a un retardador 50 del circuito SYN para mandar, -

por mediación de una puerta Y 51 y de una puerta O 52, unida a una entrada E del registro R2, la carga en este registro de la información Ie codificada por el circuito CD. los 4 bitios de la información Ie introducida en el registro R2 por las entradas A, B, C, D, son enviados seguidamente, uno por uno, a un comparador 53 del circuito comparador Cp2 bajo el mando de señales de reloj emitidas por la puerta Y 58. Las señales son engendradas en la salida $\overline{Q}$ de una báscula 54, entre cada apriete de la tecla VC que pone en 1 la salida Q de la báscula 54 a través de la báscula 55, cuando la báscula 54 recibe el frente posterior de un impulso de reloj SH_0. Las señales de reloj SH_0 recibidas en una entrada 56 del dispositivo DA, por medios que pueden ser idénticos a los de la figura 2 en la que las señales SH_0 son recibidas en la entrada 33, son transmitidas a la báscula 54 a través de un inversor 57. Una puerta Y 58 está unida por una primera entrada con la salida Q de la báscula 54, por una segunda entrada con la entrada 56 de las señales SH_0 y por una tercera entrada con una salida $\overline{Q}$ de una báscula 59, de modo que la puerta 58 transmita las señales SH_0 a una segunda entrada de la puerta O 52 cuando las salidas Q y $\overline{Q}$ de las básculas 54 y 59 se encuentran respectivamente en 1. La salida de la puerta 58, unida con la puerta O 52, está unida igualmente con una entrada 60 de un contador 61, contenido en el circuito Cpt2, del que una primera salida 62 está unida con las básculas 54 y 55 por medio de una puerta O 63 para volver estas básculas a cero por una señal RAZ engendrada cada 4 impulsos de reloj contados por el contador 61 y declarados válidos por la señal engendrada en la salida Q de la báscula 54. Además, la sa-

lida de la puerta 58 está unida con una primera entrada de una puerta Y 64, unida por una segunda entrada con la misma salida $\overline{Q}$ de la báscula 59 que la tercera entrada de la puerta 58. Así, la señal engendrada en la salida de la puerta 64 permite el mando del generador GA por una entrada 65, de modo que cada uno de los 4 bitios de un elemento de la clave CLE, contenida en la memoria MCL, sea direccionado en sincronismo con los 4 bitios de una información Ie, emitidos sucesivamente en la salida del registro R2. Cada bitio enviado por la salida 66 de la memoria MCL al comparador 53 es comparado con un bitio enviado por una salida Q_D del registro R2 por la sincronización asegurada por el circuito SYN unido a la tecla VC, a la salida S del codificador CD, con dos entradas E y H del registro R2, al circuito de recuento Cpt2, al generador GA, así como al circuito comparador Cp2. Cada secuencia de comparación de los 4 bitios de un elemento de la clave CLE con los 4 bitios de la información Ie (resultante de la codificación de un elemento del código CC inscrito por un operador) termina en el momento enque el contador 61, que ha contado 4 impulsos, engendra una señal en la salida 62. Se observará que una señal INIT, recibida por una entrada 67 del dispositivo DA permite inicializar el dispositivo a su puesta en funcionamiento, volviendo a cero las básculas 54 y 55 del circuito SYN, la báscula 59 del circuito Cpt2, así como las otras tres básculas 68, 69 y 70 contenidas en el circuito comparador Cp2, al igual que el contador 61.

Si los bitios comparados provenientes de la memoria MCL y del registro R2 son idénticos, no hay señal engendrada a la salida del comparador 53 y la báscula 68 perma-

nece a cero. Si los bitios son diferentes, la salida del comparador 53 engendra una señal que pone la báscula 68 en 1 en el frente ascendente de una señal de reloj SH_0 transmitida por la puerta 58. En un ejemplo de realización, el contador 61 está concebido para engendrar una señal en una salida 71 cada 16 impulsos declarados válidos por la puerta 58; correspondiendo el intervalo de tiempo por definición a un período de control durante el cual se comprueba por el dispositivo DA si el código CC es efectivamente el que da acceso a la máquina. Una señal de la salida 71, unida a la báscula 59, permite ponerla en 1 y, por la salida Q de esta báscula, poner en 1 la báscula 69 que engendra entonces una señal SV en su salida Q, enviada a la salida 10 del dispositivo DA. En caso de error detectado por el comparador 53, el mismo envía una señal a la báscula 68 que pone la báscula 70 en 1, de modo que sea enviada una señal SE, engendrada en la salida Q de la báscula 70, a la salida 11 del dispositivo DA.

El contador 61 de la figura 4 comprende, en la figura 5, un contador elemental 80 con 4 salidas, Q_A, Q_B, Q_C, Q_D. El contador 80 es mandado por la entrada 60 unida a la puerta 58 de la figura 4 y vuelto a cero por la señal INIT recibida en la entrada 67 del dispositivo DA de la figura 4. La señal INIT sirve igualmente para la vuelta a cero de una báscula 81 por medio de una puerta O 82, que está además unida con la salida de una puerta NO-Y (NI) 83 por la que es engendrada la señal en la salida 71 del contador 61 de las figuras 4 y 5. La báscula 81 es vuelta así a cero por la puerta 82 en la iniciación del dispositivo DA y al final de cada período de control en el curso del cual

ha sido contado un número determinado de impulsos de reloj SH_0, o sea 16 por ejemplo. La puerta 89 emite una señal en su salida en presencia de una señal de reloj SH_0 en la entrada 60 transmitida por un inversor NO-Y (NI) 85. La puerta 85 tiene su salida unida con la salida 62 del comparador 61, de las figuras 4 y 5, a la que envía una señal en ausencia de señales en su primera entrada unida con el inversor 84, con otras dos entradas unidas respectivamente con las salidas Q_A y Q_B del contador 80 por medio de dos inversores 86 y 87, y con una cuarta entrada unida a una puerta O 88. La condición, en ausencia de señal en las cuatro entradas de la puerta 85, es cumplida cuando el contador 80 ha contado 4 impulsos de reloj SHO, en cuyo caso se engendra una señal en las salidas Q_A y Q_B del contador 80 solamente. Cuando el contador 80 ha contado 16 impulsos, se engendra una señal en las 4 salidas Q_A, Q_B, Q_C, Q_D, pero en este caso, el contador 80 no engendra señal en una quinta salida 89, de modo que la báscula 81 con la que está unida esta salida es puesta a cero. Siendo puesta a cero la báscula 81 al cabo de 16 impulsos, la salida Q de esta báscula no envía más señales a la puerta 38 de una parte, ni a la puerta 83 de otra parte. Así, cada 4 impulsos, se engendra solamente una señal en la salida de la puerta 85 y, cada 16 impulsos, se engendra una señal en la salida de las puertas 85 y 83.

La figura 6 es un cronograma de señales engendradas en el dispositivo DA de la figura 4, en caso de ser pulsadas las teclas T9, T2, T3, T4. La pulsación de la tecla T9 provoca la generación de impulsos en las salidas 2^0 y 2^3 del codificador CD, de las figuras 2 y 4. La pulsa

ción de la tecla T2 permite engendrar un impulso en la salida 2^1. La pulsación de la tecla T3 permite engendrar un impulso en la salidas 2^0 y 2^1, mientras que por la tecla T4 es engendrado un impulso en la salida 2^2 del codificador CD. Así, un código confidencial CC introducido en el dispositivo DA por la pulsación sucesiva de las teclas T9, T2, T3, T4, por ejemplo, es codificado en una información IC resultante de la codificación sucesiva de cada elemento del código CC. El codificador CD de la figura 4 envía sucesivamente al registro R2 los códigos elementales correspondientes a la pulsación de la tecla T9 indicado por C9 en la figura 6; representando C2, C3, C4 los códigos almacenados sucesivamente en el registro R2 que resultan de la pulsación de las teclas T2, T3, T4. La pulsación de la tecla VC permite validar el almacenamiento de cada código elemental en el registro R2, tal como el código C9, por un impulso enviado a la entrada H del registro R2 de la figura 4 está, como se indica por la figura 6, en retraso con relación al impulso que constituye el código que es declarado válido por la misma, o sea C9 por ejemplo. Los impulsos de reloj SH_0 destinados a la sincronización de los diferentes elementos del dispositivo DA por el circuito SYN de la figura 4, están indicados en la figura 6. Del mismo modo, son indicados los impulsos engendrados en la salida Q de las básculas 55 y 54 respectivamente de la figura 4, el primero en sincronismo con el impulso resultante de la pulsación de la tecla VC, mientras que el segundo presenta un desplazamiento en el tiempo con relación al primero. Estando unida la salida Q de la báscula 54, en la figura 4, con la puerta 58 por la que es mandado el contador 61, este último

después de haber contado 4 impulsos de reloj, a partir del frente anterior de los impulsos Q 54 (en la figura 6), engendra un impulso en la salida 62 por medio de lo cual se produce la vuelta a cero de las básculas 54 y 55, correspondiente al frente posterior de los impulsos Q 55 y Q 54. Correspondiendo cada impulso Q 54 a 4 impulsos de reloj SH_0 dados como válidos por la pulsación de la tecla VC, es al cabo de 4 impulsos Q 54 cuando son así declarados válidos 16 impulsos de reloj SH_0, generando un impulso en la salida 7I del contador 61 de la figura 4. Se engendra así un impulso en la salida Q de la báscula 59 para declarar válido el resultado de la comparación de la información IC, es decir del código confidencial introducido por las teclas, con la clave CLE, y permitir la emisión bien sea de una señal SV, o bien de una señal SE en las salidas 10 y 11 del dispositivo DA. Los impulsos de reloj transmitidos por la salida de la puerta 64 de la figura 4 son reagrupados por 4, en la figura 6, según el mando de los impulsos engendrados en la salida Q de la báscula 54. Estas secuencias de 4 impulsos enviadas al generador de dirección GA permiten la lectura de los 4 bitios de la clave CLE en memoria MCL de la figura 4, bitio por bitio, durante 4 secuencias. La comparación de los bitios se realiza en el comparador 53 al ritmo de 4 impulsos de reloj.

En el caso de la figura 6 en que se pulsa sucesivamente las teclas T9, T2, T3, T4, para formar el código CC, cada código, es decir C9, C2, C3, C4, es comparado con uno de los 4 elementos de la clave CLE en el curso de las 4 secuencias de 4 impulsos de reloj declarados válidos por 4 pulsaciones de la tecla VC. En la figura 6 se da un ejem

plo que muestra un impulso engendrado en la salida del comparador 53 en caso de detección de error y la señal engendrada en la salida Q de la báscula 68 en este caso. La señal SE resultante no aparece en la salida Q de la báscula 70, de la figura 4, más que en el momento de la validación por la señal engendrada a la salida Q de la báscula 59, cuando el contador 61 ha contado 16 impulsos de reloj SH_0.

La invención tal como ha sido descrita, según dos ejemplos de realización no limitativos, presenta un interés especial en el caso de su aplicación a sistemas que utilizan tarjetas de crédito y/o de débito. El fraude que puede resultar de una interceptación en el momento de la inscripción de un código confidencial en un teclado ordinario queda excluido en este caso debido a la conexión integrada en la tarjeta entre la pluralidad de teclas que sirven de teclado y el comparador. Por otra parte, pueden darse pequeñas dimensiones a la pluralidad de teclas para evitar toda interceptación visual, permitiendo no obstante al poseedor legítimo de la tarjeta distinguir suficientemente las teclas unas de otras y aplicar una punta sobre una de ellas sin contacto con una tecla vecina.

N O T A

La Patente de invención que se solicita por veinte años para España, de acuerdo con la vigente Legislación, deberá recaer sobre: " SISTEMA DE TRATAMIENTO DE INFORMACIONES PROTEGIENDO EL SECRETO DE INFORMACIONES CONFIDENCIALES ", con Prioridad de la Demanda de Patente en Francia nº 77 16.098 de fecha 26 de Mayo de 1.977, según las características esenciales de las siguientes:----------

REIVINDICACIONES

1.- Sistema de tratamiento de informaciones protegiendo el secreto de informaciones confidenciales que comprende una máquina de tratamiento de informaciones provista de un dispositivo de transmisión de informaciones y de un dispositivo auxiliar, comprendiendo el dispositivo auxiliar unos medios de memorización permanente de una clave y medios de comparación de esta clave con un código confidencial, permitiendo el código confidencial predeterminado dar acceso exclusivo a la máquina por el dispositivo de transmisión de informaciones, caracterizado porque el dispositivo auxiliar comprende una pluralidad de elementos de contacto unidos respectivamente por una conexión integrada en los medios de comparación, estando concebida la pluralidad para engendrar, por contacto exterior, un conjunto de informaciones elementales que constituyen un código confidencial comparable con dicha clave.

2.- Sistema de tratamiento de informaciones protegiendo el secreto de informaciones confidenciales según la reivindicación,/ caracterizado porque la pluralidad de elementos de contacto está unida con dichos medios de comparación por medio de un codificador que comprende un número de entradas igual al número de elementos de contacto de la pluralidad, estando conectadas las entradas del codificador con los elementos de contacto de la pluralidad respectivamente por dichas conexiones integradas.

3.- Sistema de tratamiento de informaciones protegiendo el secreto de informaciones confidenciales según la reivindicación, 2 caracterizado porque unos medios de contacto exterior al dispositivo auxiliar permiten poner -

en contacto eléctrico sucesivamente elementos determinados de la pluralidad con las entradas correspondientes del codificador, el codificador está concebido para engendrar sucesivamente en un número determinado de salidas, una serie de conbinaciones de bitios, siendo cada combinación una de las informaciones elementales que constituyen el código confidencial introducido en el dispositivo auxiliar por contacto exterior con dichos elementtos determinados sucesivamente.

4.- Sistema de tratamiento de informaciones protegiendo el secreto de informaciones confidenciales según la reivindicación 3, caracterizado porque la pluralidad de elementos de contacto comprenden un elemento de contacto suplementario, comprendiendo además el dispositivo auxiliar unos medios de sincronización mandados por contacto exterior con dicho elemento suplementario.

5.- Sistema de tratamiento de informaciones protegiendo el secreto de informaciones confidenciales según la reivindicación 4, caracterizado porque el dispositivo auxiliar comprende, además, un registro tampón unido por entradas al codificador y por al menos una salida en los medios de comparación y un circuito de recuento concebido para funcionar según un ritmo determinado por un circuito reloj, exterior al dispositivo auxiliar con el que está unido, estando unido este circuito de recuento de una parte con dichos medios de sincronización y de otra parte con los medios de memorización de la clave de modo que la lectura de la clave en los medios de memorización sea realizada en sincronismo con la del registro tampón para la comparación del código confidencial con la clave por los medios

de comparación.

6.- Sistema de tratamiento de informaciones protegiendo el secreto de informaciones confidenciales según la reivindicación 5, caracterizado porque dichos medios de comparación comprenden unos medios discriminadores concebidos para engendrar una primera señal de validación de acceso a la máquina por una primera salida unida al dispositivo de transmisión de informaciones, y una segunda señal de error que impide el acceso a la máquina por una segunda salida unida al dispositivo de transmisión de informaciones.

7.- " SISTEMA DE TRATAMIENTO DE INFORMACIONES - PROTEGIENDO EL SECRETO DE INFORMACIONES CONFIDENCIALES "

Según queda sustancialmente descrito en la presente memoria que consta de Diecinueve hojas escritas a - máquina por una sola cara y acompañada de dibujos.

Madrid. 6 DIC. 1977

COMPAGNIE INTERNATIONALE POUR L' INFORMATIQUE CII-HONEYWELL BULL

P.P.

FRANCISCO GARCIA CABRERIZO,
P.P.

Firmado: M.ª Dolores Jorquera

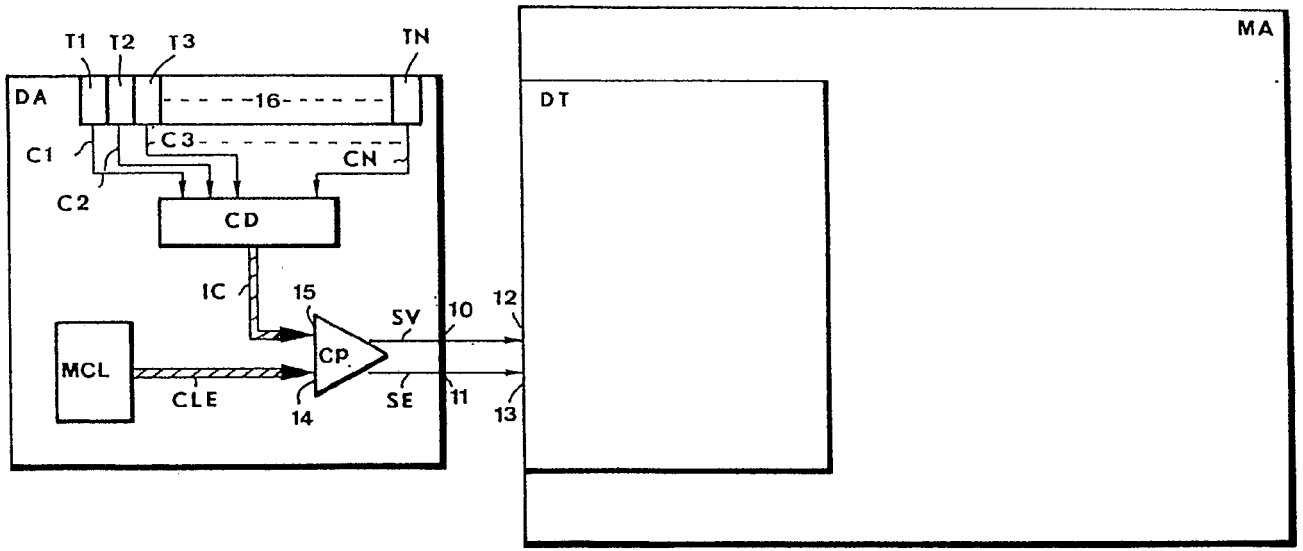


FIG. 1

Madrid
P.P.

Compagnie Internationale pour l'Informatique Cii-Honeywell Bull

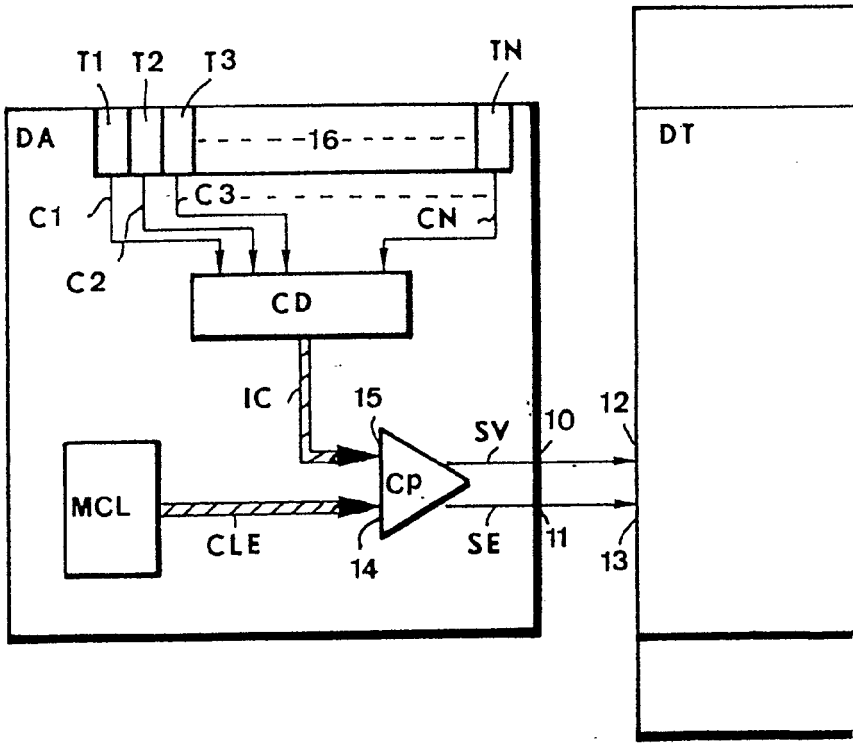


FIG. 1

Bull

6 Hojas Hoja 1

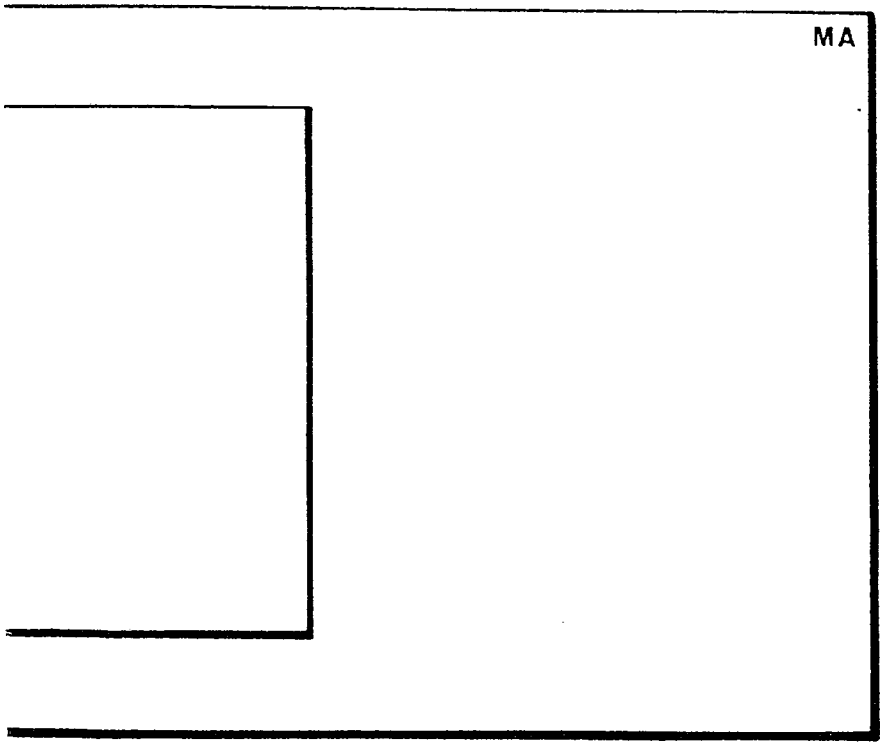


FIG. 1

Madrid 5 DIC. 1977

P.P.

FRANCISCO [illegible] CABRERIZO

P.P. [illegible]

[illegible] Dolores Jerquera

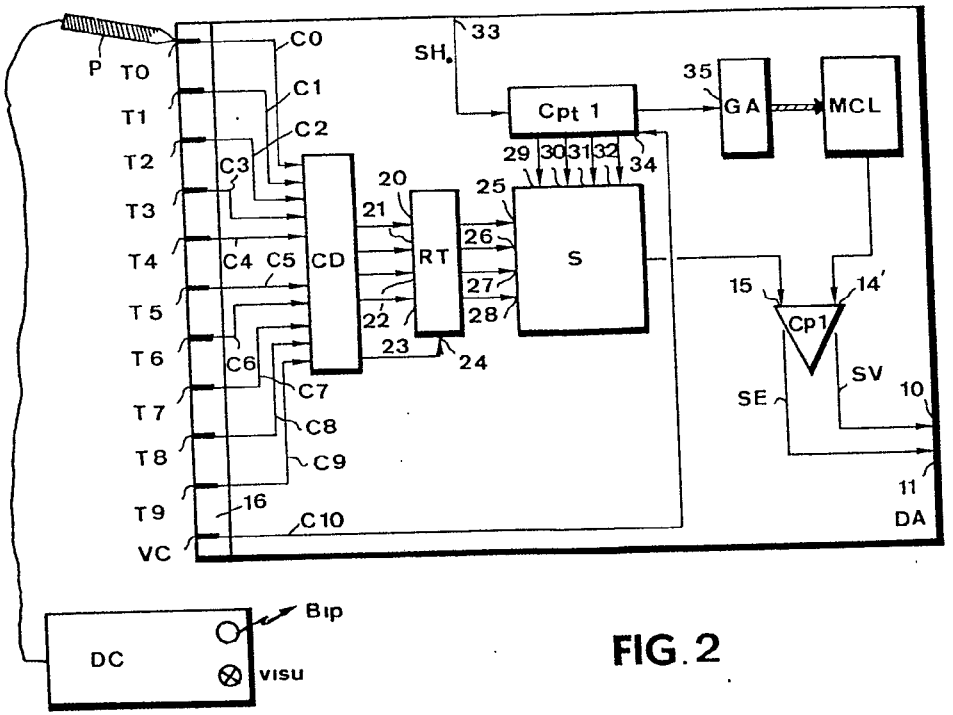
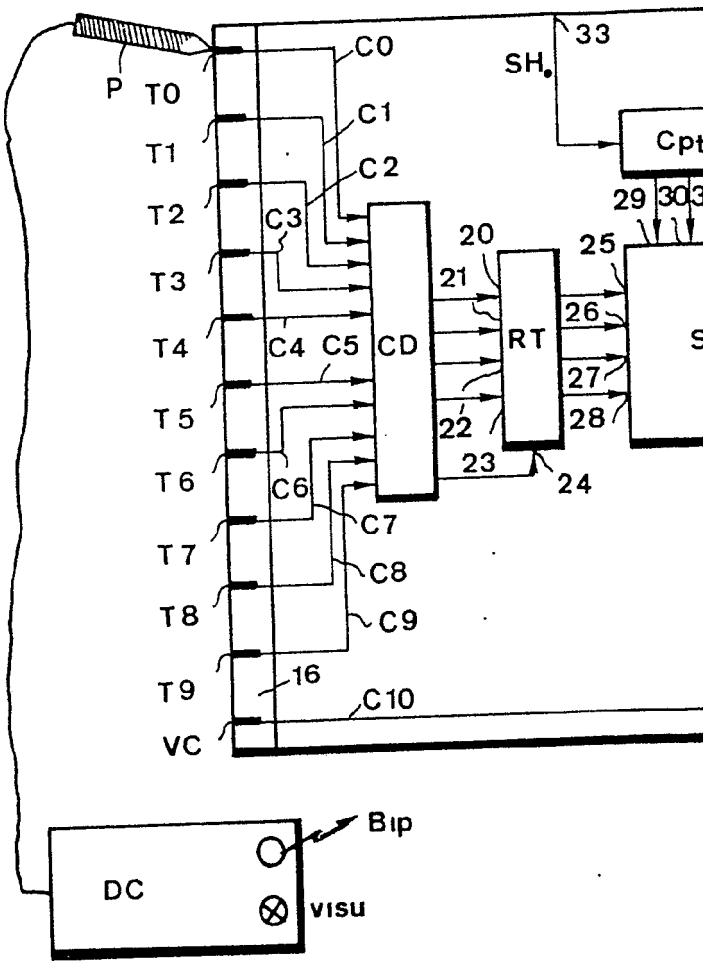


FIG. 2

Madrid, ...
P.P.

FRANCISCO GARCIA CABRERIZO
P. P.

Fdo.: Mª Dolores Jorquera


P
T0
T1
T2
T3
T4
T5
T6
T7
T8
T9
VC
C0
C1
C2
C3
C4
C5
C6
C7
C8
C9
C10
16
CD
RT
SH
33
Cpt
20
21
22
23
24
25
26
27
28
29
30
DC
Bip
visu

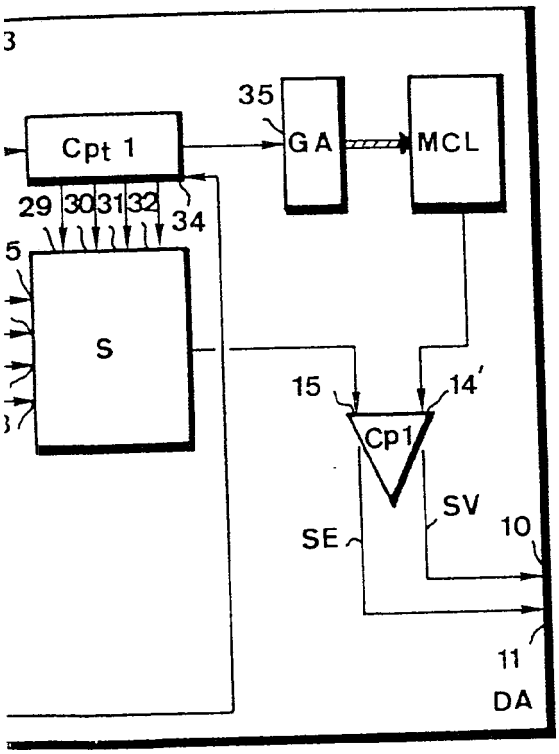


FIG. 2

Madrid,

P.P.

FRANCISCO GARCIA CABRERIZO,
P. P.

madc: M.ª Dolores Jorquera

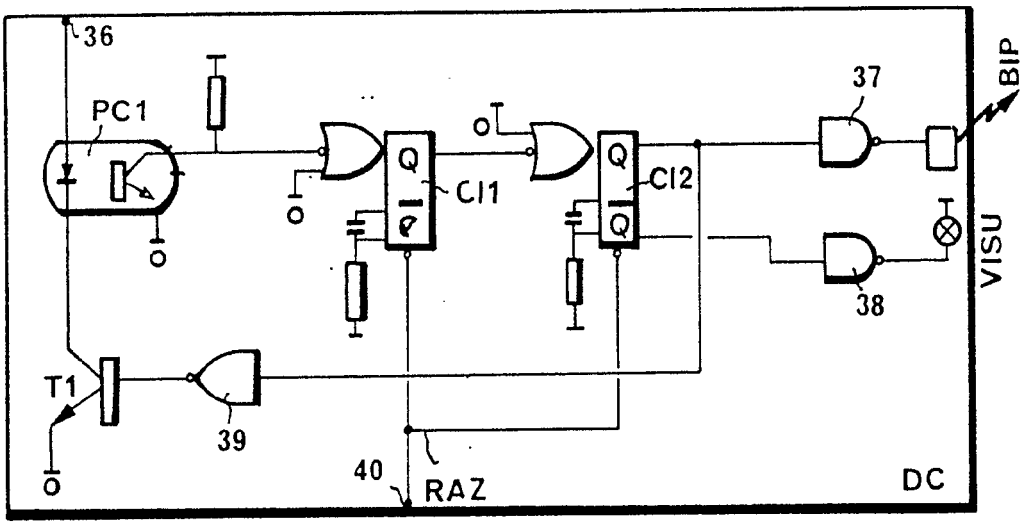


FIG.3a

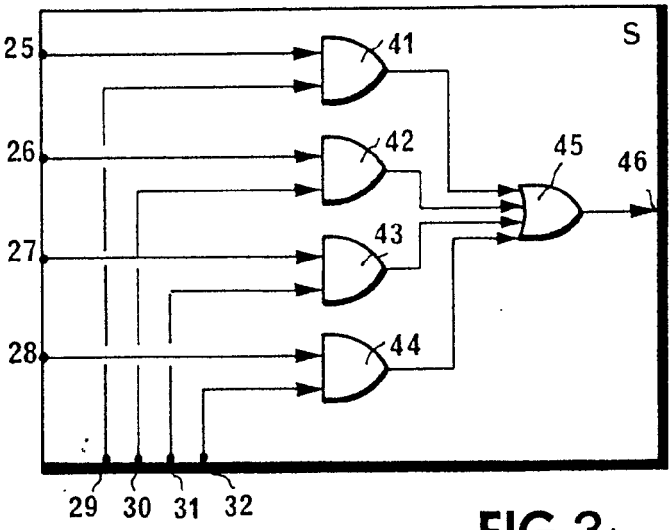


FIG.3b

6 DIC. 1977

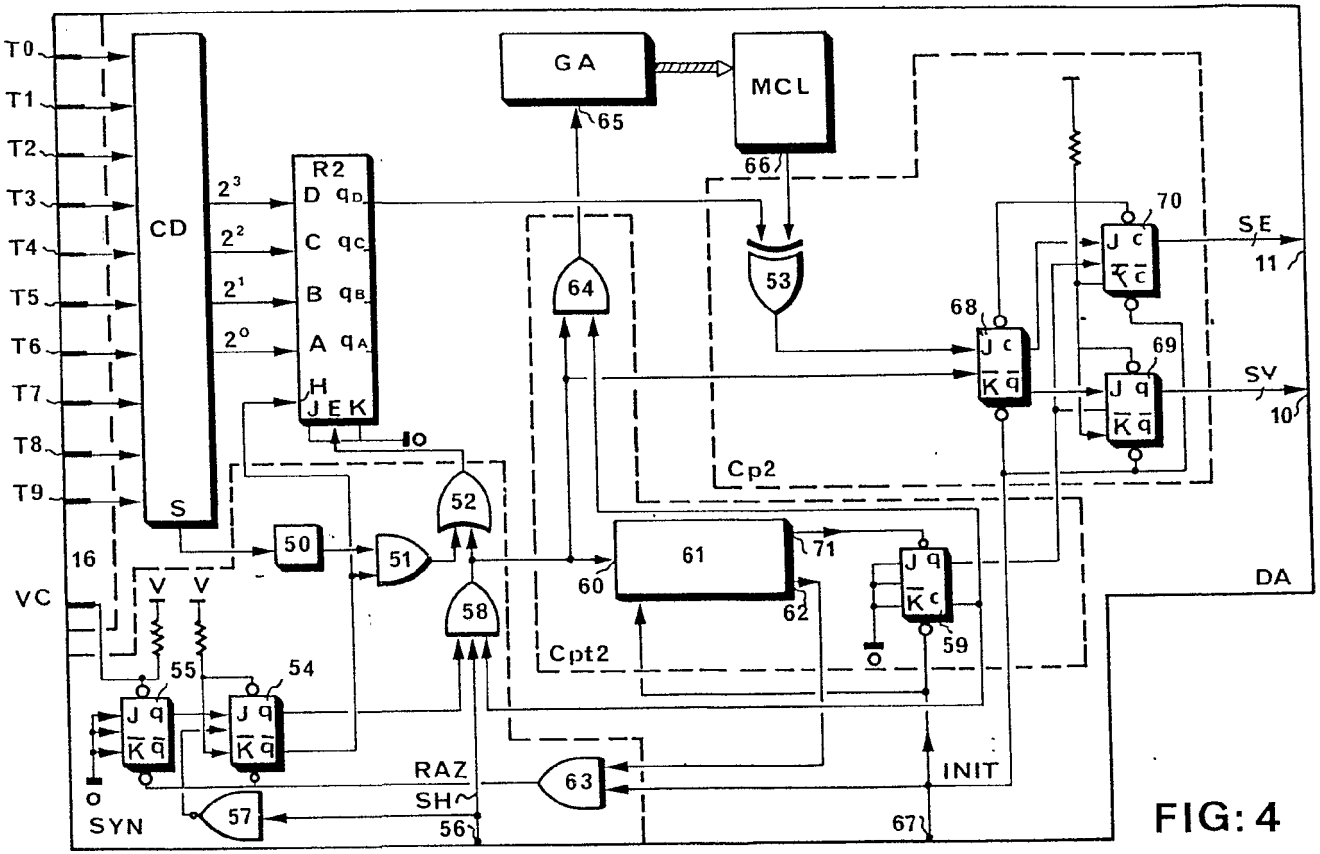
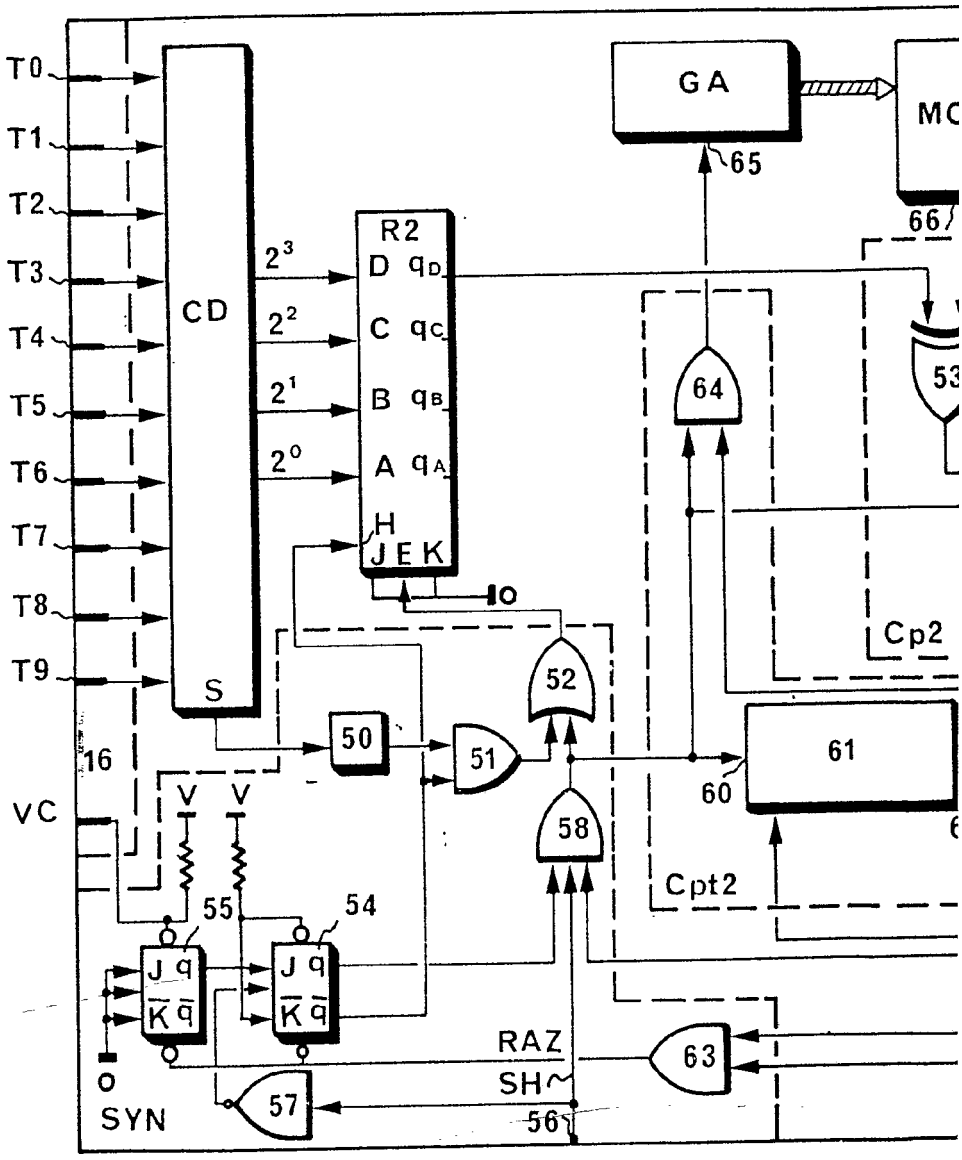


FIG: 4

Madrid, P.P.


T0
T1
T2
T3
T4
T5
T6
T7
T8
T9
CD
S
16
VC
2^3
2^2
2^1
2^0
R2
D q_D
C q_C
B q_B
A q_A
H
J E K
GA
65
MC
66
64
53
Cp2
52
50
51
61
60
58
Cpt2
V
V
55
54
J q
K q̄
RAZ
SH
56
63
57
SYN

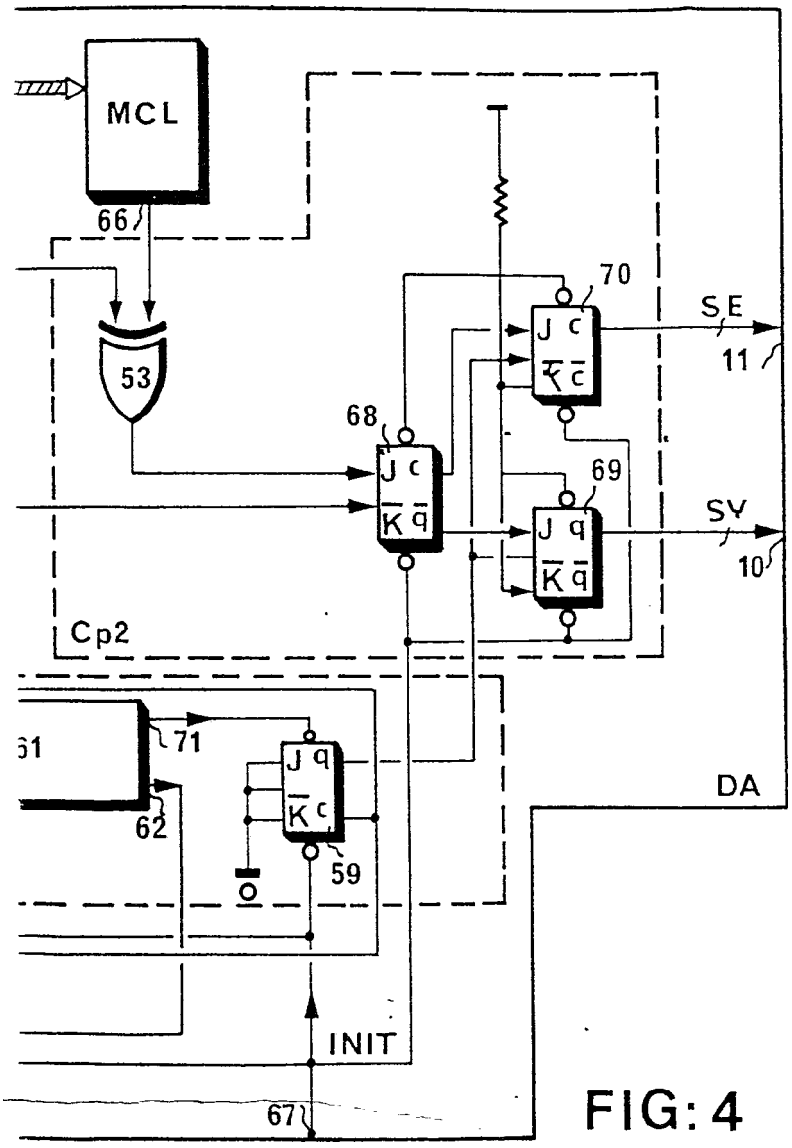


FIG: 4

Madrid, 16 DIC. 1977
P.P.

FRANCISCO GARCIA CABALLERIZO

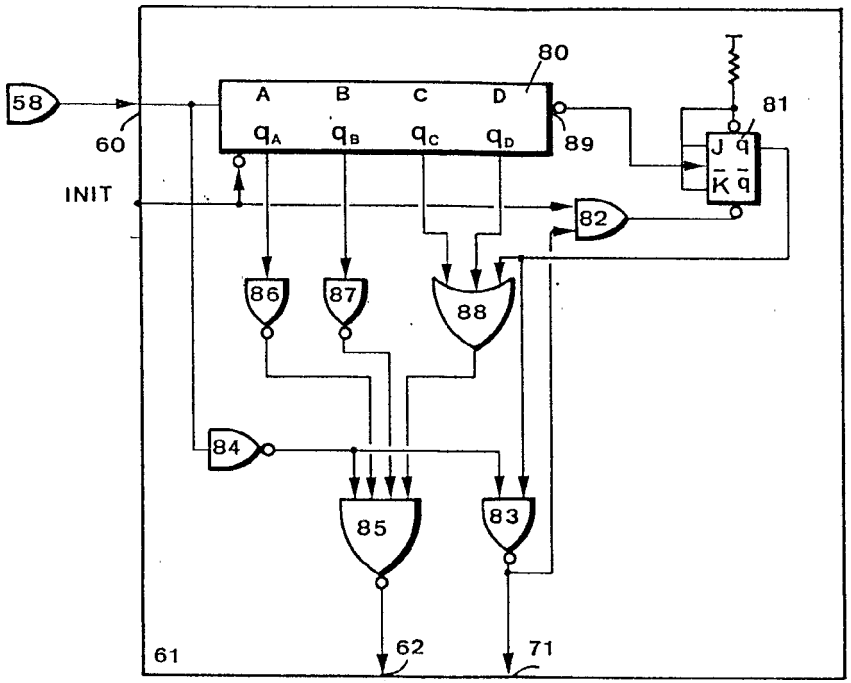
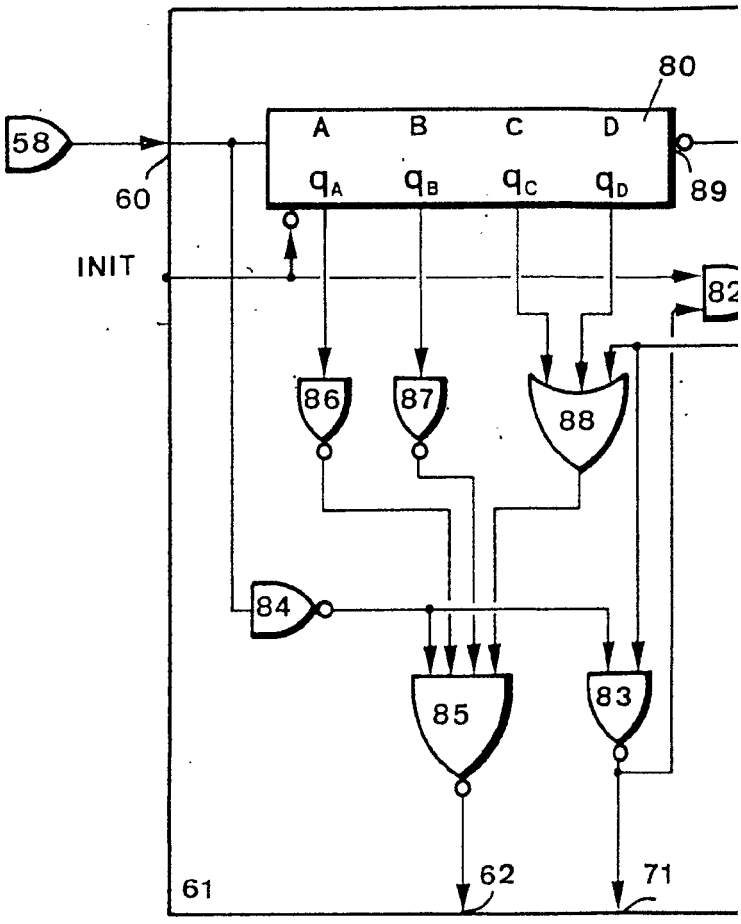


FIG.5

Madrid,
P.P.

FRANCISCO GARCIA CABRERIZO

Compagnie Internationale pour l'Informatique Cii-Honeywell Bull



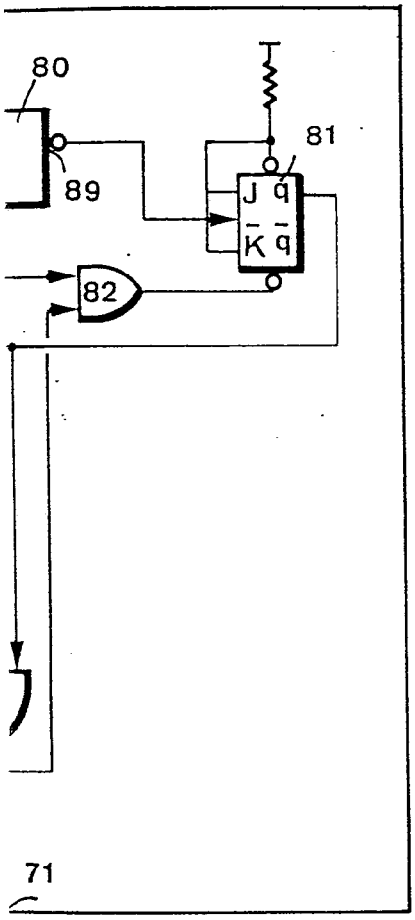


FIG.5

Madrid,
P.P.

FRANCISCO GARCIA CABREIZO
P. P.

Firmado: M.ª Dolores Jorquera

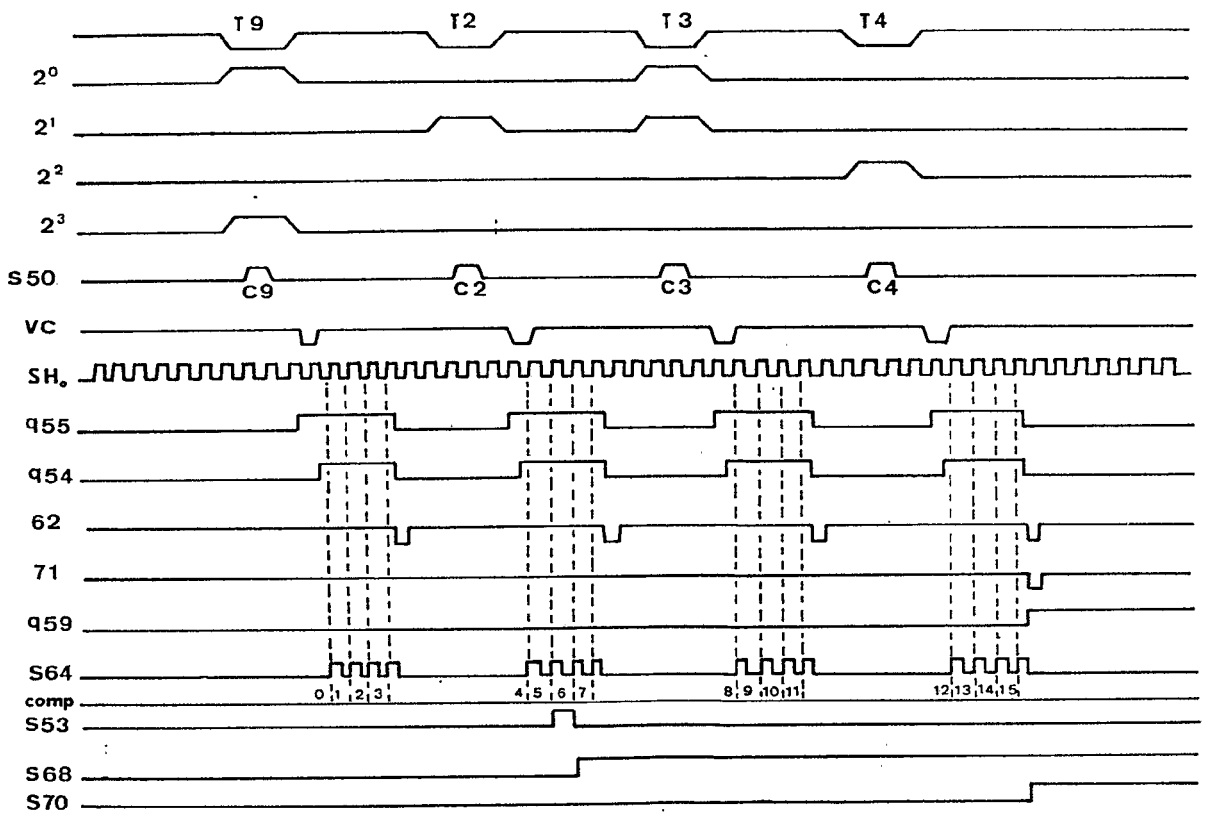


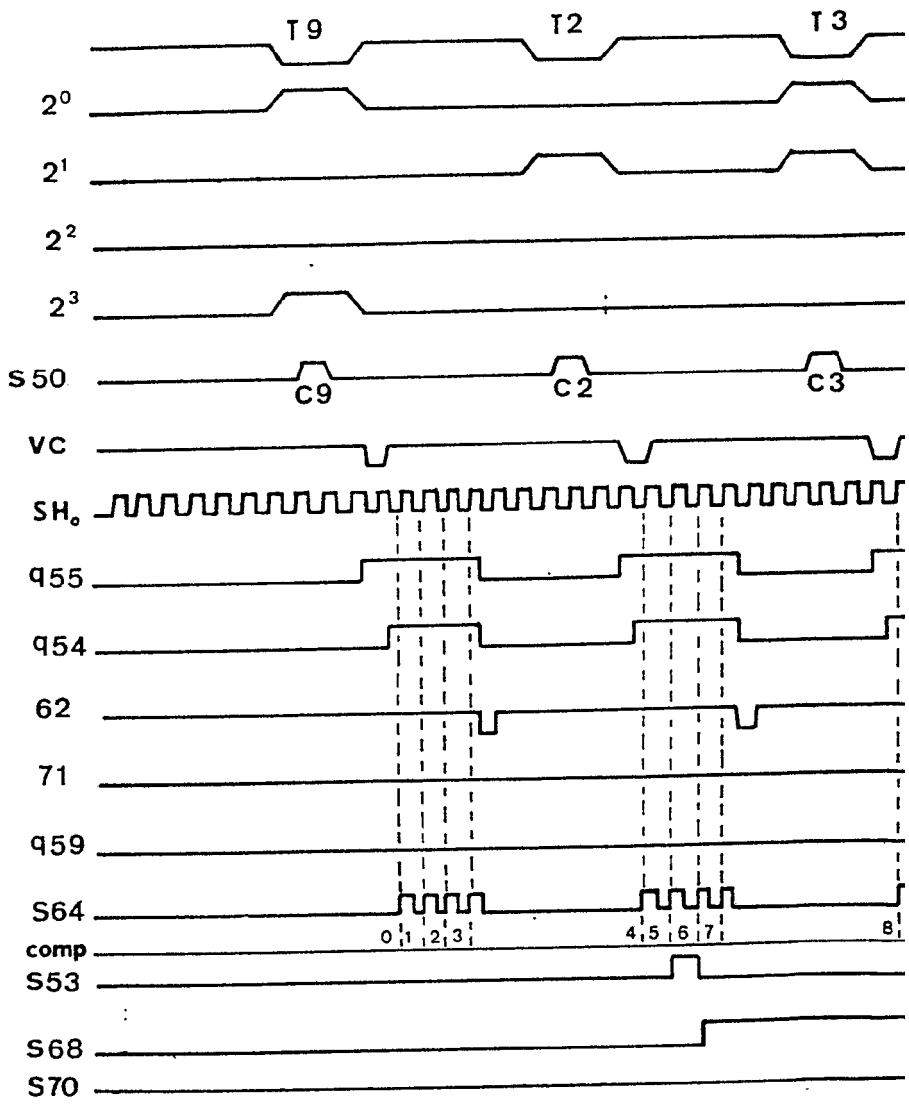
FIG.6

Madrid.

P.P.

FRANCISCO GARCIA CABREIZO
P. P.

Firmado: M.ª Dolores Jorquera


T9
T2
T3
2⁰
2¹
2²
2³
S50
C9
C2
C3
VC
SH₀
q55
q54
62
71
q59
S64
0 1 2 3
4 5 6 7
8
comp
S53
S68
S70

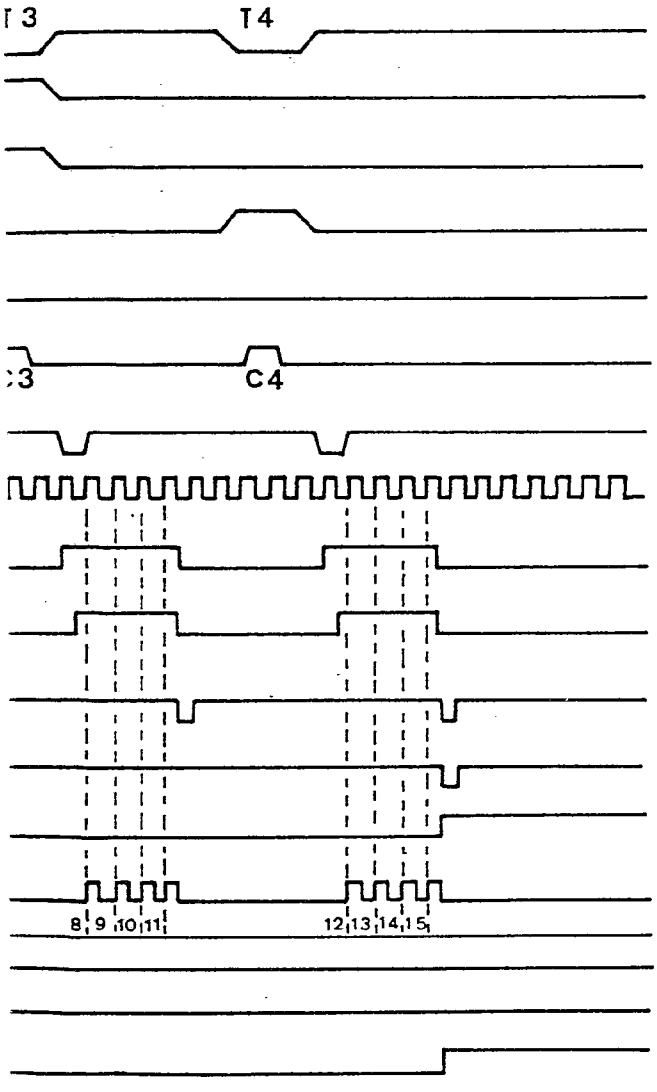


FIG.6

Madrid.

P.P.

FRANCISCO GARCIA CABREIZO
P. P.

Firmado: M.ª Dolores Jorquera