MINISTERIO DE INDUS...
REGISTRO DE LA PROPIEDAD INDUSTRIAL

ESPAÑA

(19) ES (11) (21) NUMERO 455799 (10) A1

(22) FECHA DE PRESENTACION

CONSULTA

PATENTE DE INVENCION

(30) PRIORIDADES:

(31) NUMERO	(32) FECHA	(33) PAIS

Int. Cl.³ G09B 3/02, 7/02, G06K 7/10

(47) FECHA DE PUBLICIDAD	(51) CLASIFICACION INTERNACIONAL	(62) PATENTE DE LA QUE ES DIVISIONARIA
	G07D	

(54) TITULO DE LA INVENCION

"PERFECCIONAMIENTOS EN LA VERIFICACION DE TARJETAS DE IDENTIFICACION LEGIBLES A MAQUINA EN TRANSACCIONES COMERCIALES"

(71) SOLICITANTE (S)

DIEBOLD, INCORPORATED

DOMICILIO DEL SOLICITANTE

818 Mulberry Road, S.E., Canton, Ohio 44702 U.S.A.

(72) INVENTOR (ES)

Harold Kay McCune y
Michael Ray Kronewitter

(73) TITULAR (ES)

(74) REPRESENTANTE

D. Juan Botella Ãredillo

UNE A-4 MOD. 3106

UTILICESE COMO PRIMERA PAGINA DE LA MEMORIA

RESUMEN DEL DESCUBRIMIENTO

Un método de verificación y un sistema para determinar si el poseedor de una tarjeta está autorizado para completar una transacción a través de un terminal en línea de una institución en una red de instituciones cooperantes, tales como bancos. El método y sistema son también utilizables en aplicaciones tales como el acceso al archivo de los datos de seguridad en una computadora, la entrada en una zona de seguridad, la completación de un punto en una transacción de venta y el funcionamiento de comprobadores automáticos en los bancos que estén en línea. En la materialización física preferente, la tarjeta contiene información que incluye datos que identifican la institución que posée una cuenta de un poseedor autorizado de la tarjeta y unos segundos datos que identifican la cuenta. Los primeros y segundos datos se leen en la máquina que los toma de la tarjeta y un número secreto, derivado de los datos pero conocido únicamente por el poseedor de la tarjeta, se anota en el teclado por el poseedor de la tarjeta. Los primeros datos se utklizan para dirigir una memoria magnética sólo de lectura que tiene almacenados caracteres aleatorios en la misma. Los dígitos de carácter aleatorio transferidos desde la memoria son sucesivamente exclusivos ORéd con cada dígito de los segundos datos y la resultente se aplica a los terminales de dirección de la memoria para originar una representación vectorial pseudo-aleatoria entre los datos aleatorios almacenados en la memoria. Dígitos preseleccionados de los caracteres engendrados por la memoria se ponen en correlación con los dígitos del número secreto para engendrar una indicación de paso no paso acer

ca de si el poseedor de la tarjeta está autorizado para hacer transacciones en el sistema. Por la provisión de un número de neutralización en la tarjeta, todos los dígitos del número secreto pueden seleccionarse por el poseedor de la tarjeta cuando esta se emite. El número de neutralización convierte los dígitos del número secreto seleccionados por el poseedor de la tarjeta en dígitos que corresponden con los dígitos seleccionados de antemano del caracter engendrado por la memoria. La tarjeta puede verificarse en cualquier institución de una red de instituciones.

La tarjeta puede verificarse en cualquier institución de una red de instituciones cooperantes que tengan sistemas de verificación con memorias magnéticas sólo de lectura idénticamente programadas.

Los primeros datos contenidos en la tarjeta originan que la transacción sea cargada contra la institución que posée la cuenta e impide la acumulación de registros de transacción entre las instituciones cooperantes.

CAMPO DE LA INVENCION

La presente invención se refiere de una manera general a los sistemas de verificación de tarjetas, y más particularmente, a un sistema de verificación de la tarjeta que emplea los datos contenidos en la misma representan un número de institución y un número de cuenta o identificación para engendrar un número secreto al dirigirse de manera pseudo-aleatoria a una memoria con los datos.

FUNDAMENTO DE LA INVENCION

Las tarjetas de identificación legibles a máquina en transacciones comerciales y otras aplicaciones se han he-

cho muy generalizadas. Por ejemplo, en los sitemas de seguridad, a menudo se presenta una tarjeta de identificación para lograr el acdeso a una zona protegida. En las transacciones de compra mediante tarjeta de crédito, una tarjeta de identificación legible a máquina, presentada a un vendedor, permite al poseedor de una tarjeta decrédito adeudar una cuenta poseida por la institución emisora de la tarjeta. En las operaciones bancarias comerciales, se han proporcionado terminales de servicios bancarios automáticos, de servicio limitado empleando en equipo que es sensible a una tarjeta de identificación legible a máquina. La tarjeta a menudo está formada de un medio plástico y contiene información legible a máquina en forma de, por ejemplo, indicios grabados en relieve, aberturas, segmentos electricamente conductores o regiones magnéticamente registrables que llevan el número de cuenta del cliente y otra información, tales como la fecha de expiración y el status del cliente.

En un sistema de retirada de fondos en metálico automatizada, el terminal bancario no atendido o pagador automático, que responde favorablemente a la tarjeta legible por la máquina, anticipa el dinero al cliente en cualquier momento del día o la noche . Un aparato de distribución utilizado en tal sistema se descubre en la solicitud copendiente No. de série 502.898, archivada el 3 de Septiembre de 1974, actualmente Patente USA No. 3943335 comumente asignado con la presente invención.

El terminal no atendido ha sido provectado como una unidad de servicio aislada. No obstante, con objeto de ampliar los beneficios de servicio y seguridad de los siste

mas en línea a las unidades aisladas, el terminal bancario no atendido ha sido desde entonces combinado con los sistemas de proceso en línea asociados con cada institución financiera que ofrece el servicio.

Típicamente, los sistemas bancarios automáticos léen los datos contenidos en la tarjeta, tales como el período de tiempo de autorización, cantidad autorizada de la transacción, fecha de la última utilización, balance de la cuenta y número de la cuenta. Si el poseedor de la tarjeta es el poseedor autorizado, la transacción requerida, por ejemplo retirada en metálico, se somete a proceso. Las operaciones de proceso incluyen la interrogación de la cuenta del poseedor para verificar si tiene fondos adecuados, cargar en cuenta la cantidad de la transacción y la entrega de metálico al cliente. Tal sistema ha traído como resultado la provisión de un servicio bancario económico y eficiente en cualquier momento del día o de la noche.

Una dificultad primaria con las anteriores estaciones bancarias automáticas, y con otros sistemas que utilizan los medios de identificación legibles a máquina, ha sido el sistema de seguridad. Un volumen extremadamente grande de tarjetas de identificación del cliente proliferadas por un gran número de instituciones ha creado un problema muy extendido de participación de poseedores de tarjeta no autorizados. En vista del ámplio tráfico de tarjetas de crédito robadas y atrjetas falsificadas, un vendedro o institución financiera ya no está seguro de que el poseedor de la tarjeta está autorizado para realizar transacciones en el sistema.

Para superar esta dificultad, se ha sugerido mezclar

el número de cuenta para desarrollar un número secreto que se revelà únicamente al poseedor autorizado de la tarjeta en el momento de su emisión.

En la práctica, el poseedor de la tarjeta asienta el número secreto dentro del sistema por medio de un teclado o dispositivo similar. Los datos contenidos en la tarjeta son leidos por un analizador en la terminal y son mezclados por un traductor numérico. Si el número mezclado corresponde favorablemente con el número secreto, se supone que el poseedor de la tarjeta está autorizado y la transacción requerida se completa siempre al menos que la tarjeta no haya expirado y en la cuenta haya fondos adecuados para cubrir la retirada de fondos qequerida.

Aunque la utiφización de un número secreto derivado de los datos de la tarjetá para verificación mejora sustancialmente la seguridad del sistema, el número de cuenta en número secreto, aunque extremadamente difícil de averiguar, ha sido ecasionalmente hipotecado por un poseedor no autorizado.

Se han desarrollado sistemas para disminuir la posibilidad de que un poseedor no autorizado de la tarjeta pudiera derivar el número secreto de los datos contenidos en la tarjeta. Por ejemplo, en la patente concedida a Spetz 3.794.813 un sistema de verificación utiliza una tabla de precisión para derivar un número secreto del número de cuenta registrado en la tarjeta. Los datos para dirigir la tabla de presión se derivan lógicamente de bitios seleccionados arbitrariamente de un campo de dígitos codificados digitalmente contenido en la tarjeta. Con objeto de proporcionar la selección arbitraria de los dígitos conte

nidos en la tarjeta, se proporciona una completa disposición de conmutación para muestrear selectivamente determinados bitios de los dígitos binarios codificados registrados en la tarjeta. Un banco u otra institución, una vez que ha elegido arbitrariamente determinados de los bitios para la formación de las palabras de dirección para la tabla de precisión al accionar la disposición de conmutación queda posteriormente limitada a esa elección y el empleo de la tarjeta se limita a ese banco u otra institución.

En tanto que el terminal bancario automático ha proporcionado al cliente acceso a su cuenta en cualquier momento del día o de la noche, el cliente queda todavía restringido a la zona geográfica en la que la institución ha instalado terminales. Es altamente deseable proporcionar también al cliente acceso a su cuenta a través de los dispositivos terminales de otras instituciones con lo cual el cliente ya no queda limitado a un zona geográfica.

Al acceso a una cuenta en una institución desde otra institución cooperadora se hace referencia en el terreno bancario como intercambio y se proporciona sobre una base de reciprocidad en la que las instituciones cooperadoras acuerdan cambiar transacciones mediante conexiones entre sistemas en línea.

Con objeto de efectuar la capacidad de intercambio en un sistema de convalidación de una tarjeta, es necesario proporcionar unsistema que sea compatible entre las instituciones cooperadoras en una red de intercambio, en tanto se evita la acumulación de contabilidad. Consecuentemente, es necesario que se emita una tarjeta standar a todos los clientes de las instituciones cooperadoras, estando codi-

ficadas las tarjetas para identificar a la institución particular que mantiene la cuenta mientras que sea procesable por el equipo terminal de las instituciones cooperadoras. Existe actualmente la necesidad de un sistema de verificación que permita el intercambio entre las diferentes instituciones cooperadoras y que sea altamente inmune a los poseedores de tarjetas no autorizados.

Con objeto de garantizar la máxima seguridad, resulta imperativo que el poseedor autorizado de la tarjeta no registre el número secreto en un lugar que sea accesible a un posible usuario no autorizado de la tarjeta. Por ejemplo, si el poseedor autorizado de la tarjeta, para evitar que se le olvide el número secreto, registra el número secreto en la superficie de la tarjeta, la tarjeta podría ser utilizada por un poseedor no autorizado de la misma para retirar dinero en metálico contra la cuenta del poseedor autorizado debido a que el poseedor no autorizado sería capaz de asentar en el teclado el número secreto.

Se ha propuesto que el poseedor autorizado de la tarjeta se permita seleccionar su propio número secreto cuando se extiende la tarjeta como una ayuda nemotécnica. Por ejemplo, el poseedor autorizado podría escoger el año de su nacimiento como su número secreto para hacer mínima la posibilidad de que posteriormente olvidara el número. En la Patente de Stambler 3.786.420, concedida el 15 de Enero de 1974, como ayuda de seguridad, un sistema de convalidación de la tarjeta incluye medios que permiten al cliente el primer dígito de un número secreto multidígito en el moemnto en que la tarjeta se emite. No bostante, los restantes dígitos del número secreto se generan entonces

por el sistema y el número secreto multidígito, extendido al usuario autorizado, no conserva ninguna relación averiguable con el dígito seleccionado y no sirve como ayuda a la memoria. Es deseable proporcionar un sistema del carácter descrito que permita al poseedor autorizado de la tarjeta seleccionar todos los dígitos de su número secreto - con lo cual el número secreto seleccionado está hecho para corresponder a los datos permanentemente registrados - en la tarjeta con anterioridad a la selecciój por parte del del cliente del número secreto.

OBJETIVOS DE LA INVENCION

Consecuentemente, uno de los objetivos de la presente invención es proporcionar un sistema y método de verificación nuevo y mejorado.

Otro objetivo de la presente invención es proporcionar un sistema y método de verificación nuevo y mejorado en el que el número secreto se deriva de los datos registrados en una tarjeta y en el que los datos contenidos en la tarjeta y el número secreto no guardan relación averiguable lógica o matemática unos con otros.

Todavía otra objetivo de la presente invención es el proporcionar un sistema y método de verificación que proporcione el intercambio entre las instituciones cooperadoras.

Otro objetivo más de la presente invención es proporcionar un sistema y método de verificación nuevo y mejorado en el que todos los dígitos de un número secreto puedan seleccionarse por el cliente cuando se emite la tarjeta.

BREVE DESCRIPCION DE LA INVENCION

De acuerdo con la presente invención, en un método y

sistema para la verificación de que el poseedor de una - tarjeta de identificación es el poseedor autorizado en - cualquier institución dentro de una red de instituciones cooperadoras, una tarjeta conteniendo los datos primeros y segundos, por ejemplo, número de identificación de la - institución y número de cuenta, se lée a máquina y se traduce a un número diferente que está en correlación con un número secreto asentado por el poseedor de la tarjeta por cualquier medio adecuado, tal como un teclado. Si el número traducido corresponde con el número secreto, la transacción requerida se compelta y se carga a la institución identificada por los primeros datos. Al traducir el número, los dígitos de la tarjeta contenían datos consecutivamente de una dirección pseudo-aleatoria una memoria magnética sólo de lectura conteniendo caracteres aleatorios - (conjuntos de bitios conteniendo ocho bitios cada uno de ellos). En una primera forma de operación, los dígitos del número de identificación de la institución se dirigen a - la memoria magñetica sólo de lectura, originando que un - carácter de salida aleatorio se genere a partir de entonces. En un segundo modo de operación, un dígito del carácter de salida aleatorio se combina repetidamente de manera lógica, es decir por una operación EXCLUSIVE OR, con - dada dígito del número de cuenta hasta formar nuevos datos que son utilizados para volver a dirigirse a la misma memoria tal como es dirigido por el número de identificación de la institución, con lo cual se forma un esquema de retroalimentación pseudo-aleatorio. Uno de los dígitos, preferiblemente el menos significativo de los dígitos del número de la cuenta, se aplica nuevamente para dirigirse a

la memoria pseudo-aleatoriamente, y, en un tercer modo de operación, un dígito del carácter final, o número de identificación personal (P/I/N.), engendrado por la memoria se pone en correlación con un dígito del número secreto almacenado en el teclado. Los dígitos adicionales del número de la cuenta se procesan de manera similar para formar los dígitos del P.I.N. para una correlación uno por uno con los restantes dígitos del número secreto y una correlación favorable entre los dígitos del número secreto y los dígitos del P.I.N. indica que el poseedor de la tarjeta es el poseedor autorizado.

Las instituciones cooperadoras que tienen equipo terminal compatible y memorias de lectura únicamente programadas de manera idéntica verifican la autenticidad de los poseedores de tarjetas emitidas por cualquiera de las instituciones cooperadoras. Puesto que las memorias en cada institución están identicamente programadas, una tarjeta que lleve un número de identificación de la institución y un número de cuenta, cuando se aplica al traductor de números, origina que se engendre un P.I.N. en correlación positiva en el sistema de verificación en cualquiera de las instituciones cooperadoras. El sistema en cada institución que responde al número de identificación de la institución registrado en la tarjeta hace que la transacción autorizada se cargue a la institución poseedora de la cuenta con lo cual proporciona la capacidad de intercambio en tanto evita la acumulación de contabilidad entre las instituciones cooperadoras.

Para mejorar adicionalmente la seguridad, como característica opcional el número secreto asentado en el tecla

do se utiliza para dirigir una segunda memoria megnética sólo de lectura, la salida de la cual se compara con el número engendrado por el traductor numérico como respuesta a los primeros y sengundos datos contenidos en la tarjeta. Un número secreto seleccionado por el cliente cuando se extiende la tarjeta puede utilizarse como una dirección para la segunda memoria magnética sólo de lectura al incluir un número de neutralización en la tarjeta. El número de neutralización se combina con el número secreto asentado por el teclado para formar una tanda de bitios de dirección y la segunda memoria magnética sólo de lectura se pone en correlación con el P.I.N.

El método y el aparato descrito son aplicables en otros ambientes distintos del bancario. Por ejemplo, un sistema de verificación del tipo descrito puede utilizarse en aplicaciones tales como el acceso a archivos de seguridad en una computadora, obtención de entrada a una zona protegida tal como un almacén y completar el punto de transacciones de venta, y otros.

Lo anterior, y todavía otros objetivos, características y ventajas adicionales de la presente invención se harán aparentes al considerar la siguiente descripción detallada de varias materializaciones específicas de la misma, especialmente cuando dicha descripción se haga en conjunción con el dibujo acompañante.

BREVE DESCRIPCION DEL DIBUJO

La Figura 1 es un diagrama simplificado en bloque del sistema de verificación de la presente invención;

La figura 2 es un diagrama del circuito del traductor del número y un diagrama en bloques simplificado del orde

nador de secuencia del sistema de verificación;

La figura 3 es un diagrama del circuito de un convertidor exadecimal-alBCD y un comparador digital para comparar los dígitos de del P.I.N. con los correspondientes dígitos del número secreto;

La figura 4 es un diagrama del circuito del contador del sist4ma de verificación para generar una señal de paso no-paso sensible al comparador;

Las figuras 5(a) a 5(c) son diagramas de circuito de prociones del ordenador de secuencia del sistema de verificación;

La figura 6 es un diagrama del circuito de un aparato opcional de la invención para convertir un número secreto seleccionado por el cliente en un P.I.N.; y

La figura 7 es un diagrama en bloque de un aparatos para la generación de un número secreto de los datos contenidos en una tarjeta cuando esta se emite.

DESCRIPCION DETALLADA DE LOS DIBUJOS

Haciendo referencia a la Figura 1, allí se muestra un diagrama simplificado en bloques de un sistema de verificación de acuerdo con la presente invención. Una tarjeta de identificación 10 que va a aplicarse al sistema ha contenido en ellas campos de datos tales como los campos 12, 14 y 16. Preferentemente, los campos 12, 14 y 16 contienen datos que identifican (1) la institución que extendió la tarjeta o que tiene una cuenta del poseedor autorizado de la tarjeta, (2) el número de cuenta de la tarjeta y (3) otros datos, por ejemplo, estado de la cuenta y fecha de expiración. Los datos en los campos 12, 14 y 16 se registran de cualquier forma adecuada, tal como grabados

en relieve, perforador o regiones eléctricamente conductoras, aunque preferiblemente son bitios en una banda magnética de formato apropiado.

El lector de tarjetas 18 es una unidad analizadora convencional adaptada para recibir la tarjeta 10 y convertir los datos registrados en la tarjeta en señales eléctrica en forma exadecimal, con los datos de los campos 12 14 y 16 siendo respectivamente suministrados a y almacenados en los registros de desplazamiento 42, 44 y 45. Los datos procedentes del lector de tarjeta 18 se aplican al traductor de números 30, unidad de identificación de la institución 26 y sistema central de contabilidad 28. El número de identificación de la institución y los datos del número de cuenta de los camós 12 y 14 se suministran al traductor de números 30 y los datos de los campos 12, 14 y 16 se suministran al sistema de contabilidad central 28.

Acorde con la presente invención, el traductor de números 30 incluye una memoria magnética sólo de lectura que está dirigida inicialmente por los dígitos del campo de Identificación de la institución 12 y entonces, retroalimentando los datos procedentes de la salida de la memoria y combinando lógicamente una porción de los datos de retroalimentación con los dígitos del campo 14 del número de cuenta, se proporciona una dirección pseudo-aleatoria de la memoria y determinados de los datos de salida de la memoria proporcionan la traducción del número de cuenta. Los datos de salida derivados de la memoria, a los que se hace referencia como Número de Identificación Personal (P.I.N.), no guardan relación averiguable con los datos leídos en -

la tarjeta.

Durante la verificación de la tarjera 10, el P.I.N. engendrado por el traductor de números 30 se pone en correlación con un número secreto M que se asienta por el poseedor de la tarjeta a través del teclado 22. Los dígitos - del número secreto se ponen en correlación sobre la base de unoncon los dígitos del P.I.N. en el comparador 24. El comparador 24 engendra una señal de paso no-paso en respuesta a la correlación.

Cada una de las instituciones en una red cooperadora de instituciones está equipada con el sistema de verificación de la presente invención, teniendo cada sistema un - traductor de números 30 idéntico. La unidad de identificación de la institución 26 es un registro binario que almacena los datos de identificación de la institución 12 y - transfiere los datos al sistema de contabilidad central - 28 para cargar la transacción a la institución emeisora. Los datos de identificación de la institución 12 forman - la primera dirección o dirección "clave" de la memoria del traductor 30 y además dan lugar a que la transacción, si está aprobada, se cargue a la institución identificada.

Las tarjetas standard 10, emitidas por las instituciones cooperadoras, son verificables en el sistema de verificación de cualquiera de las instituciónes cooperadoras de la red. Si una tarjeta que ha sido emitida por una institución no-cooperadora se aplica al lector de tarjetas - 18 para verificación, la dirección inicial de la memoria con el número de identificación de la institución y subsiguiente dirección con el número de cuenta harán que la memoria engendre un P.I.N. que no guarda correlación con el

núemro secreto, incluso si el número de cuenta contenido en la tarjeta es idéntdico a un número de cuenta ya en uso entre las instituciones cooperadoras.

Con objeto de que la memoria engendre un P.I.N. que tenga correlación, tanto datos de números de identificación de la institución procedintes del campo 12 y los datos del número de cuenta procedentes del campo 14 contenidos en la tarjeta 10, cuando se aplican al traductor - 30 deberán proporcionar la representación vectorial anticipada pseudo-aleatoria de la memoria para engendrar el correcto P.I.N.

En la operación, el cliente inserta la tarjeta 10 - en el lector de tarjetas 18 y manualmente asienta su número secreto en el teclado 22. Los datos de salida del lector de la tarjeta se aplican al sistema central de contabilidad 28, unida de identificación de la institución 26 y traductor de números 30. El sistema de contabilidad central 28 está situado en una zona accesible a la institución que realiza la transacción e incluye el almacenamiento de la computadora y el equipo de proceso de datos de un tipo que es bien conocido y que actualmente se utiliza en las instalaciones bancarias. El traductor de números 30 está pseudo-aleatoriamente dirigido por los datos de identificación de la institución procedentes del campo 12 y los datos del número de cuenta 14 para engendrar un P.I.N. que está en correlación con los datos del número secreto almacenados en el teclado 22 en el comparador 24. También aplicados al sistema de contabilidad central 28 están los datos derivados del campo 16 en la tarjeta 10 que representan, por ejemplo, el estado legal del posee-

dor de la tarjeta, fecha de expiración de la misma y otra información. Suponiendo que el poseedor de la tarjeta es el poseedor autorizado, según se determina por el comparador, y una transacción de retirada de metálico se autoriza, el dinero se distribuye desde el distribuidor de metálico 31 y la transacción se carga a la institución emisora de acuerdo con los datos de identificación almacenados en la unidad de identificación de la institución 26. Una señal de paso o no-paso se presenta al cliente - al cliente en la unidad de presentación 33 que puede ser un tipo de representación alfabético-numérica ó lámpara de señal o similar.

Los datos de identificación de la institución procedentes del campo 12 se aplican por el lector de tarjeta 18 al registrador de desplazamiento vinario 42 como dos dígitos exadecimales(A_1A_2). Los datos del número de cuenta procedentes del campo 14 se aplican al registro 44 como una pluralidad de dígitos ($Z_1Z_2 \cdots Z_N$), cada uno codificado en sistema exadecimal. El funcionamiento de los registros 42 y 44 se describe en detalle más adelante. Los datos procedentes del campo 16 se aplican al registro 45 para su presentación al sistema de contabilidad central 28.

El registro 26 sirve como un registro de almacenamiento suplementario para el número de identificación de la institución y suministra los datos al sistema central de contabilidad 28 para cargar una transacción a la institución identificada. El registro 26, que se muestra más detalladamente en la Figura 2, puede cargarse al principio de un ciclo de verificación por una señal de control de

carga (LD) que se describe más adelante. Alternativamente, el registro 26 puede cargarse por una señal de interrogación engendrada por el sistema de contabilidad central 28 indicadora que una transacción solicitada ha sido aprobada basándose en el resultado de un ciclo de verificación de la tarjeta y otros datos, por ejemplo, el estadde la cuenta. Los datos de identificación de la institución cargados en el registro 26 se suministran entonces al sistema 28 para cargar la transacción contra la institución identificada.

Haciendo referencia a la Figura 2, el traductor numérico 30 comprende la memoria magnética sólo de lectura (ROM) 40, el ordenador de la secuencia 46, el circuito EXCLUSIVE OR 51, los conmutadores controlados 50, 52, 54 56 y lod registro 42, 44 y 48. Cualquier dispositivo de memoria que pueda funcionar como memória de lectura únicamente tal como una memoria semiconductora o núcleo magnético puede ser utilizado como ROM 40; no obstante, se prefiere una memoria MOSFET programable de lectura únicamente debido al pequeño tamaño y facilidad de programación de la misma. Uno de tales ROM es el Intel 1602A que está programado para contener 256 conjuntos de bitios teniendo valores exadecimales entre 00 y 255 aleatorios y sin repetición (el número 255 se representa como FF en exadecimal; los números exadecimales se representan de acuerdo con la Tabla 1-3, p. 13, Minicomputadoras para Ingenieros y Científicos, Korn, 1973, McGraw-Hill, Inc.).

ROM 40 está dirigido por un conjunto de bitios de dirección que incluyen dos dígitos, teniendo cada uno cuatro bitios, codificados en exadecimal. Los cuatro bi-

tios del primer y sengundo dígito se aplican respectivamente a los terminales I_1-I_4 y I_5-I_8 de ROM 40. Cada conjunto de bitios de ROM 40 es dirigible desde los terminales de dirección I_1-I_8; obstante, no existe relación averiguable entre los conjuntos de bitios almacenados y los conjuntos de bitios de dirección.

Los conmutadores 50, 52, 54 y 56 son pasos con salidas de pilar totémico de tres estados, tal como los SN 74125 manufacturados por Texas Instruments, Inc. que de una manera selectiva pasan los datos entre los terminales de entrada y salida de los mismos dependiendo del estado de control de los terminales CT; una señal lógica cero aplicada al terminal CT acciona un correspondiente conmutador y una señal lógica uno desconecta al conmutador. Los conmutadores 50, 52, 54 y 56 reciben los datos de dirección procedentes de los registros 42 y 48 y circuiti 51 EXCLUSIVE OR y suministran los datos para dirigir los terminales I_1-I_8 de ROM 40 de acuerdo con la señal de modo del número de identificación de la institución (IIN) y el complemento de la misma ($\overline{IIN}$) suministrado por el ordenador de secuencia 46 a los terminales CT. El registro 42 está controlado por la señal de carga del registro (LD), el registro 48 está controlado por la señal de fijación de la retroalimentación (FS), el registro 44 está controlado por la señal de carga (LD) y la señal de desplazamiento de la cuenta (ZSP). Todas las señales de control, que se indican cerradas entre parentesis, se generan por el ordenador de secuencia 46 tal como se describe más adelante.

Los registros 42, 44 y 48 respectivamente almacenan

temporalmente los datos del número de identificación de la institución, los datos del número de cuenta y los datos de salida de ROM 40, bajo control de las señales (LD) y (FS). Los datos del número de identificación de la institución leídos de la tarjeta 10 son bitios paralelos cargados en el registro 42 y los datos del número de cuenta son bitios paralelos cargados en el registro 44. El registro 48 sirve como medio de almacenamiento temporal para los datos salidos de ROM 40 de manera que los datos que han tenido previamente acceso no se pierden cuando ROM 40 es re-dirigida. Cada uno de los registros 42, 44 y 48 incluye un: (a) terminal de fijación S que, cuando emite impulsos, origina que los datos aplicados en bitios paralelos a las entradas del registro queden allí almacenados, y (b) el terminal de desplazamiento SH que, cuando emite impulsor, origina el desplazamiento en serie de los datos almacenados. Un registro tal como el SN 74199 fabricado por Texas Instruments, Inc. resulta adecuado en esta aplicación. El terminal de despalzamiento SH se utiliza únicamente en el registro 44.

El traductor 30 funciona en tres modos de operación es decir (a) un modo IIN del número de identificación de la institución en el que ROM 40 está inicialmente dirigido o "puesto en clave" con el número de identificación de la institución, (b) un modo CAN del número de cuenta de un cliente en el que ROM 40 está dirigido utilizando el número de cuenta, y (3) un modo PING de generación del número de identificación personal en el que los dígitos del P.I.N. se derivan de los conjuntos de bitios engendrados por ROM 40. En el modo de número de identificación

de la institución un conjunto de bitios de dirección que representan los dígitos de identificación de la institución A_1A_2 se aplica a los terminales de dirección I_1-I_8 de ROM 40; en el modo de número de la cuenta, los datos de la salida ROM de los terminales O_1-O_4 son retroalimentados a los terminales de dirección I_1-I_4 y los datos de los terminales de salida O_5-O_8 se retroalimentan y someten a EXCLUSIVE OR con los dígitos individuales Z_N DEL - número de cuenta antes de ser aplicado a los terminales de dirección I_5-I_8. En el modo de generación P.I.N., los dígitos del P.I.N. se generan por ROM 40.

Los dígitos A_1A_2 del número de identificación de la institución, almacenados en el registro 42, se suministran a los terminales de dirección I_1-I_8 de ROM 40 a través de los conmutadores 52 y 54 que están conectados por la aplicación a los terminales CT de los mismos de la señal de control (IIN). La señal (IIN), generada por el ordenador de secuencia 46, está en lógico cero durante el modo de identificación de la institución. Correspondiente al conjunto de bitios de dirección A_1A_2 está un conjunto de bitios de los dígitos en exadecimal almacenado en ROM 40 - el cual, cuando se dirige se genera asincrónicamente en los terminales de salida O_1-O_8 del ROM. El conjunto de bitios de salida no se almacena en el registro 48 hasta - que un primer impulso de fijación (FS) procedente del ordenador de secuencia 46 se aplica al terminal de fijación S del registro 48. El primer carácter de salida procedente de ROM 40, siendo dependiente únicamente de número A_1 A_2 de identificación de la institución sirve como un comienzo del punto de dirección o "clave" para la dirección

pseudo-aleatoria del ROM. El número de identificación de la institución únicamente se suministra una vez a los terminales de dirección I_1-I_8 de ROM 40 y posteriormente a esto se retira al abrir los conmutadores 52 y 54 con la señal de contro (IIN) que está en el lógico uno cuando el sistema está fuera del modo de número de identificación de la institución.

Los primeros cuatro bitios del conjunto de bitios generado por ROM 40 en los terminales de salida O_1-O_4 son retroalimentados a los terminales de entrada del conmutador 50 y los segundos cuatrobitios en los terminales de salida O_5-O_8 son retroalimentados para alternar los terminales de entrada del circuito EXCLUSIVE OR 51. Las entradas a los otros terminales de entrada del circuito EXCLUSIVE OR 51 están provistos del registrador 44 que contiene un primer dígito Z_1 del número de la cuenta.

Preferentemente, el primer dígito del número de la cuenta que se aplica al registro 44 es el dígito menos significativo del número de la cuenta debido a que los dígitos Z_N COdificados del número de cuenta están dispuestos en el campo 14 de la tarjeta 10 y almacenados en el registro 44 de acuerdo con su significación numérica. El carácter aleatorio de los datos generados está parcialmente dirigido por el orden de entrada de los dígitos Z_N; un elevado carácter aleatorio ocurre cuando los dígitos Z_N se asientan sucesivamente comenzando con el dígito menos significativo. No obstante, deberá entenderse que cualquier dígito del número de cuenta podría ser el primer dígito aplicado al traductor 30 durante el mode de número de cuenta; todos los dígitos se aplican por lo me

nos una vez durante un ciclo de verificación.

Los dígitos del número de cuenta, almacenados en el registro 44, se adelantan un dígito (cuatro bitios) a la vez por la aplicación de impulsos de desplazamiento en serie (ZSP) al terminal SH del registro 44. Los impulsos de desplazamiento (ZSP), generador por el ordenados de secuencia 46, están formados por trenes de impulsos conteniendo cuatro impulsos por tren (debido a que dada dígito almacenado en el registro 44 contiene cuatro dígitos). El circuito de retroalimentación 44a proporciona la operación de recirculación del registro de desplazamiento en el registro 44 con lo cual los datos obtenidos del registro se vuelven a aplicar a la entrada del mismo.

Los dígitos del número de la cuanta que han salido en serie del registro 44 son por consiguiente reaplicados en serie al registro y durante el modo de funcionamiento de número de la cuenta, los dígitos recirculados se utilizan para re-dirigir ROM 40. Puesto que los conmutadores 50 y 56 están desconectados por la señal de control ($\overline{TIN}_p$) procedente del ordenador de secuencia 46 durante el modo de número de la institución, por conjuntos de bitios generados por ROM 40 en los terminales de salida O_1-O_8 están aislados de los terminales de dirección I_1-I_8 de ROM 40 hasta la iniciación del modo de número de cuenta.

Bajo control del ordenador de secuencia 46, se inicia el modo de número de cuenta por la generación de la señal de contro (CAN) del modo del número de cuenta lógico uno. En el modo de número de cuenta, los conmutadores 52 y 54 se desconectan por la señal lógico uno (IIN) y los conmutadores 50 y 56 se conectan por la señal ($\overline{TIN}$)

lógico cero. Puesto que el número de identificación de la institución A_1A_2 no se utiliza de nuevo para dirigir ROM 40, los conmutadores 52 y 54 permanecen desconectados durante el resto del ciclo de verificación.

Los conmutadores 50 y 56 estando conectados y desconectados los conmutadores 52 y 54 en el modo de número de cuenta, el conjunto de bitios de salida procedente de ROM 40, almacenado en el registro 48, se suministra a los terminales de dirección I_1-I_8 de ROM 40; el primer dígito de salida en los terminales O_1-O_4 de ROM 40 se suministra directamente a los terminales de dirección I_1-I_4 a través del conmutador 50 y el segundo dígito de salida a los terminales O_5-O_8 se transforma en EXCLUSIVE OR con el dígito Z_1 del número de cuenta almacenado en el registro 44 y el resultado se aplica allos terminales de dirección I_5-I_8. Inmediatamente a la aplicación del nuevo conjunto de bitios de dirección para dirigir los terminales I_1-I_8 de ROM 40, se engendra un nuevo conjunto de bitios en los terminales O_1-O_8 de acuerdo con la programación de ROM 40.

Cuando una segunda señal de fijación de retroalimentación (FS) procedente del ordenador de secuencia 46 se aplica al terminal de fijación S del registro 48, el nuevo conjunto de bitios de salida de ROM 40 se almacena en el registro 48 para sustituir al conjunto de bitios allí almacenado anteriormente. El conjunto de bitios de dos dígitos ahora almacenado en el registro 48 se vuelve a aplicar a los terminales de dirección I_1-I_8 de ROM 40, siendo el segundo dígito generado en los terminales O_5-O_8 de ROM 40 puesto primero en la forma EXCLUSIVE OR con el dígito

Z_1 del número de cuenta en el circuito 51 EXCLUSIVE OR. Bajo el control del ordenador de secuencia 46, el descrito ciclo de dirección se repite sucesivamente al aplicar sucesivamente impulsos de fijación de retroalimentación (FS) al terminal S del registro 48 un número abritrario de veces, preferiblemente siete. Se prefiere el número siete porque está convenientemente generado por un registrador de desplazamiento de ocho etapas 84 comercialmente disponible, descrito más adelante; no obstante puede utilizarse cualquier número entero.

Es aparente que como resultado de la sucesiva dirección de ROM 40 con los datos de salida del mismo, se proporciona la dirección pseudo-aleatoria de ROM 40 con lo que ROM 40 está representado vectorialmente de una manera pseudo-aleatoria para producir una serie de conjuntos de bitios pseudo-aleatorios de salida.

La secuencia de operación anteriormente descrita se ilustra en la Tabla 1 al final de la especificación, teniendo el caracter de ejemplo el número de identificación de la institución A_1A_2 y el el número dígito menos significativo del número de la cuenta Z_1 allí aplicado. Ocho pasos de secuencia, en lugar de siete, aparecen en la Tabla 1 debido a que se incluye la dirección inicial o "clave" utilizando el número de identificación de la institución (10011000 a modo de ejemplo).

En el ejemplo de la Tabla 1, después de siete ciclos consecutivos de dirección a ROM 40 con lo cual siete conjutnos de bitios almacenados al azár tienen acceso de manera pseudo-aleatoria para generar el conjunto de bitios 10111000, bajo control del ordenador de secuencia 46 el

siguiente dígito menos significativo Z_2 del número de cuenta almacenado en el registro 44 se desplaza a las últimas cuatro etapas del registrador 44 con impulsos de desplazamiento 44 (ZSP). El dígito Z_2 del número de cuenta se aplica para dirigir de manera pseudo-aleatoria ROM 40 de la misma manera que se describió anteriormente con respecto al dígito Z_1.

Siete ciclos de dirección de retroalimentación se repiten bajo control de la señal de fijación de retroalimentación (FS) para cada uno de los restantes dígitos $Z_3 \cdots Z_{10}$ del número de la cuenta. Se hace aparente que con un número de cuenta del cliente de diez dígitos, por ejemplo, ROM 40 se accede 71 veces (recordando que ROM 40 fué dirigida una vez utilizando el número de identificación de la institución en el modo IIN). Se observa que en este momento, el conjunto de bitios generador por ROM 40 han sido utilizados únicamente para proporcionar una representación vectorial pseudo-aleatoria de datos aleatorios almacenados en ROM 40. Ninguno de los datos de salida ha sido todavía utilizado para establecer la correlación con el número secreto.

Después de que todos los dígitos Z_1-Z_{10} del número de la cuenta han sido utilizados para engendrar direcciones pseudo-aleatorias para ROM 40, habiendo sido recirculados en la registro 44 por medio de la línea 44a los cuatro dígitos menos significativos z_1-z_4 se aplican nuevamente uno por uno para dirigirse pseudo-aleatoriamente a ROM 40 bajo el controal de la señal de fijación de retroalimentación (FS). El dígito menos significativo Z_1 se utiliza para dirigir ROM 40 siete veces y el primer dígito

del conjunto de bitios generado desde ROM 40 en los terminales de salida O_1-O_4 representa el primer dígito del P.I.N. El ordenador de secuencia 46 ahora genera una señal de control de modo de generación (PING) que inhibe la aplicación de la señal de fijación de retroalimentación (FS) al registro 48 haciendo que los datos P.I.N. permanezcan almacenados allí durante la correlación con los correspondientes dígitos M_1 del número secreto en el comparador 24. A continuación de un ciclo de comparación el ordenador de secuencia 46 engendra una señal lógico uno (CAN), haciendo que el traductor 30 actúe de nuevo en el modo de cuenta, dirigiendo ROM 40 con el dígito Z_2 para engendrar el segundo dígito del P.I.N. La generación de las señales del control de modo se describe en detalle con respecto al ordenador de secuencia más adelante.

Los dígitos Z_2, Z_3 y Z_4 del número de cuenta se utilizan individualmente para dirigir de una manera pseudoaleatoria ROM 40, dirigiendo cada dígito ROM 40 siete veces en el modo de cuenta y comparando el segundo, tercero y cuarto dígitos del P.I.N. generado en los terminales de salida ROM O_1-O_4, respectivamente, con el segundo, tercero y cuarto dígitos del número secreto en el modo de generación del P.I.N. Los cuatro bitios de cada dígito P.I.N. generados por ROM 40 en los terminales de salida O_5-O_8 no se utilizan para correlación con el número secreto y se ignoran. La anterior secuencia de funcionamiento con la cual el más significativo dígito de el P.I.N. que tiene como ejemplo un valor numérico 0101 se genera, se ilustra en la Tabla 2 al final de la especificación. Los siete pasos de la secuencia se extienden entre los números

de secuencia 113 y 119 como se ve también en la Tabla 4 al final de la especificación, y de lo que se tratará más adelante. Esta secuencia está precedida por una secuencia de carga (un paso), una secuencia de modo (un paso), diez secuencias CAN (setenta pasos) y diez secuencias de desplazamiento (cuarenta pasos). Estos pasos están indicados en la Tabla 4.

Los dígitos generados por ROM 40 son exadecimales - mientras que los dígito del número secreto generador por el teclado 18 son decimales binarios codificados (BCD). Consecuentemente, antes de la correlación en el comparador 24, deberá proporcionarse una conversión exadecimal--a-BCD para los dígitos generados por ROM 40. Haciendo referencia a la Figura 3, el circuito convertidor exadecimal-a-BCD 53 recibe dígitos de los terminales de salida O_1-O_4 de ROM 40 en exadecimal y convierte dos dígitos a BCD.

En el convertidor 53 la conversión exadecimal-a-BCD se proporciona al determinar digitalmente si el valor del dígito exadecimal procedente de los terminales O_1-O_4 de ROM es menos de seis (0110) y si es así añade ocho (1000) a aquel. Si el dígito es de un valor mayor o igual a seis el dígito se utiliza directamente.

La tabla 3 muestra el resultado de la conversión exadecimal-a-BCD utilizando el anterior algoritmo de conversión si los dígitos resultantes están completamentados como se indica en la columna encabezada por "BCD". Se observa que los números decimales 2-7 aparecen dos veces en la representación de dígitos exadecimales 0-15 a dígitos decimales 0-9. Consecuentemente, el acaecimiento de

los numerales 0,1,8 y 9 ocurre menos frecuentemente que los restantes numerales 2-7. Esta falta de uniformidad de densidad espectral originada por la representación no uniforme no hace que la transformación entre la información registrada en la tarjeta y el número secreto sustancialmente más pronosticable. En la Figura 3, los cables a, b, c y d del circuito representado cada uno recibe, en bitios paralelos, un bitio de los cuatro bitios del dígito exadecimal generado por ROM 40 en los terminales de salida O_1-O_4. La conversión a BCD se proporciona por el paso 60 y el inversor 62 que intervienen entre la salida del registrador 48 (Figura 2) y la entrada del comparador 24. El comparador 24 comprende cuatro pasos EXCLUSIVE OR 24a, 24b, 24c y 24d que comparan cda dígito de cuatro bitios del P.I.N. generado en los terminales de salida O_1-O_4 de ROM 40 con dada dígito de cuatro bitios del número secreto M asentado en el teclado, y los pasos 66 y 66a.

Cualquier dígito exadecimal aplicado a los cables a, b, c, d, que tenga un valor menor de seis (0110) tiene añadido por el paso 60 el numeral ocho dígito binario (1000) en tanto que los dígitos que tengan un valor mayor o igual a seis (0110) se aplican al comparador 24 sin añadir el dígito 1000 al mismo. En el ejemplo de la Tabla 2, el dígito 0101 generado en los terminales O_1-O_4 de ROM 40 se aplica a los terminales de entrada a, b, c, d del convertidor 53. El invertidor 62 y el paso 60 convierten el dígito 0101 al dígito 1101 antes de su aplicación al comparador 24. El dígito 1101 es el complemento binario del dígito BCD 0010 que corresponde al dígito exadecimal 0101 como se indica en la Tabla 3. El dígito com

plementado BCD mencionado anteriormente se aplica al comparador 24 para establecer la correlación con un dígito no complementado del número secreto. Dado que cada etapa del comparador 24 es realmente un paso exclusive-OR, cada etapa genera una señal lógica uno siempre que las señales de entrada allí aplicadas sean opuestas, es decir, un lógico uno y un lógico cero. Por esta razón, los dígitos del número secreto procedentes del teclado 22 se suministran directamente al comparador 24; no están complementados. En el presente ejemplo, el comparador 24 genera una señal lógico uno para el dígito generado en el teclado 0010. El circuito contador 70, que se muestra en la Figura 4, es sensible a las señales lógico uno generadas por el inversor binario 66a.

El circuito contador 70 comprende un par de cuatro bitios, registradores de derivación serial in/out 71 y 72 tal como el SN 7493 fabricado por Texas Instruments, Inc. El terminal de salida del paso 69, después de la inversión en el inversor binario 69a, se conecta al terminal In del registro de desplazamiento 72. El terminal de entrada 2 del paso 69 recibe la señal del reloj comparador (COMPCLK) generada por el ordenador de secuencia 46. La señal (COMPCLK) se genera durante el modo de generación del P.I.N. y se deriva de la señal de fijación de retroalimentación (FS). Un impulso de la señal (COMPCLK) se genera por cada siete impulsos de fijación de retroalimentación de la señal (FS) como se describe en detalle en la descripción del ordenador de secuencia 46 más adelante. Durante el modo de generación P.I.N., La señal (FS) está inhibida de ser aplicada al registrador 48 y un

impulso de la señal (COMPCLK) se carga serialmente en el registrador 71 durante la generación de cada dígito del P.I.N. Cada vez que una señal lógico uno (COMPCLK) se aplica al terminal del entrada 2 del paso 69, la señal - lógico uno es tambien cargada serialmente en la primera etapa del registrador de despalzamiento 71. Si, coincidente con la generación de una señal lógico uno (COMPCLK) procedente del ordenador de secuencias 46, existe una - comparación positiva en el comparador 24 entre un dígito del número secreto y ROM 40 ha generado un dígito P.I.M. una señal lógico uno tambien se aplica al terminal de entrada 1 del paso 69. Sensible a la misma, el terminal de salida del paso 60 NAND cambia a lógico cero y, por inversión de la señal en el inversor binario 69a, una señal - lógico uno se carga serialmente dentro del registro 72. Cada señal lógico uno cargada dentro del registrador de desplazamiento 71 es indicadora del acaecimiento de un - ciclo de generación P.I.N.; cada señal lógico uno cargada dentro del registrador de desplazamiento 72 es indicadora de una comparación faborable entre un dígito del P.I.N. y un dígito correspondiente del número secreto M almacenado en el teclado 22. A continuación de la generación de cuatro dígitos al P.I.N. con lo cual cuatro impulsos de la señal (COMPCLK) se cargan serialmente en el registrador de desplazamiento de cuatro etapas 71, una señal lógico uno se genera a la salida del mismo. Si y únicamente si todas las cuatro comparaciones son positivas, - indicando que los cuatro dígitos del P.I.N. generado en ROM 40 son idénticos a los cuatro dígitos del número secreto, una señal de "paso" lógico cero se genera en el -

terminal de salida del paso NAND 74. Si se desea la señal puede invetirse mediante el inversor binario 74a.

Se entiende que los registros 71 y 72 contiene cada uno exactamente una etapa para cada dígito del número secreto y que mientras se muestra un número secreto de cuatro dígitos en la materialización física preferente, puede ser utilizado cualquier número de dígitos.

El ordenador de secuencia 46 proporciona la cronometración y control de las señales para el sistema de verificación 30. Las señales encerradas entre paréntesis identifican señales generadas en el ordenador de secuencia 46. Las señales de control de secuencia comprenden las señales de control de modo (IIN), (CAN) Y (PING) que indiqan respectivamente, el número de identificación de la institución, el número de cuenta del cliente y los modos de operación que generan el P.I.N.; la señal de carga del registro lógico uno (LD) para controlar el almacenamiento de datos leidos por el lector de tarjetas 18 dentro de los registros 42 y 44, fijación de la retroalimentación lógico uno (FS) para controlar el almacenamiento de los datos de salida de ROM 40 en el registro 48 durante la dirección pseudo-aleatoria del TOM, una señal de reloj comparador lógico uno (COMPCLK) para contar el número de dígitos P.I.N. generados por ROM 40, y impulsos de desviación uno (ZSP) para serialmente desviar el conjunto de dígitos Z_N del número de cuenta en el registrador 44.

El ordenador de secuencia 48 tambien genera una señal de reloj (CL) que es la señal de sincronización básica del sistema. La señal del reloj (CL) se genera en el ordenador de secuencia 46 por un multivibrador standard

que funciona libremente; todas las secuencias de operaciones en el sistema 3o están sincronizadas con la señal -del reloj (CL). Las señales (RESET) y (DISPLAY) controlan todas las funciones citadas en el sistema.

Los controladores de secuencia son bien conocidos - en la profesión y pueden adquirir muchas formas incluyendo los controles de almacenamiento de lectura únicamente controles del descodificador contador, etc. Por ejemplo, el almacenamiento de lectura únicamente podría utilizarse para general las señales necesarias del control para la carga de los registradores 42 y 44, conmutadores de control 50, 52, 54 y 56, registro de fijación 48, comparador interrogante 24 y dígitos de desplazamiento en el registro 44 de acuerdo con una secuencia programada. La secuencia completa de funcionamiento del ordenador de secuencia 46 se inidica para un número de cuenta de diez - dígitos en la Tabla 4 al final de la especificación.

Las Figuras 5A-5C son un diagrama lógico de una materialización física del ordenador de secuencia 46. El - registro de derivación 82 que se muestra en la Figura 5A genera una señal de carga del registro (LD), señales del control de modo (IIN), (CAN) y (PING), señales de presentación (DISPLAY) para presentar la señal de paso o no-paso a continuación del ciclo de verificación, y la señal de redisposición (RESET). Las Figuras 5B y 5C descubren la ciruciterfa lógica para derivar las señales de control (FS), (COMPLK) y (ZSP) generadas por el registro de desplazamiento 82.

En la Figura 5A, el reloj 80, la fuente básica de - cronometración del sistema, genera impulsos de reloj (CL)

al terminal de desplazamiento CL del registro 82. El circuito basculador disposición-re-disposición 81 está inicialmente dispuesto para proporcionar una salida de señal lógico uno en repuesta de una señal (RESET).

(RESET) se suministro al final de un anterior ciclo de verificación. El basuclador 81 suministra la señal lógico uno al terminal de entrada IN de la primera etapa - del registrador 82. La salida del basculador 81 se redispone entonces a una señal lógico cero durante el segundo impulso del reloj (CL), generado por el generador de impulsos del reloj 80, por medio del cirucito de retroalimentación 81a conectado entre la salida de la primera etapa del registrador 82 y el terminal R de redisposición - del basculador 81. Como el reloj 80 genera impulsos adicionales para desplazar el terminal SH del registrador - 82, un solo bitio lógico uno se adelanta serialmente etapa por etapa de izquierda a derecha en el registrador 82 como se indica en la Figura 5A. La primera etapa del registrador 82 proporciona la señal de carga (LD) que se - suministra a los registradores 42 y 44. Las restantes etapas proporcionan señales de control de modo (IIN), (CAN) (PING) que se suministran al traductor 30. Los terminales de salida corrientemente etiquetados, por ejemplo CAN, están conectados juntos a través de una circuitería lógica OR (no indicada). La circuitería OR Lógica es preferentemente del tipo de calbe robusto para reducir la cantidad de material requerida para el circuito.

Generalizando, se ve que la segunda etapa del registrador 82 genera un impulso de la señal de control de modo (IIN) y los impulsos de la señal de control de modo -

(CAN) están generados desde el registrador 82 en las etapas 3, 4, 5, ... (11N + 9), en la que N es el número de dígitos en el número de la cuenta. En la Tabla 4, donde se utiliza un número de cuenta de diez dígitos, a modo de ejemplo, la señal de control (CAN) se genera desde las etapas 3-119 del registrador 82. La señal de control de modo (PING) se genera por el registrador 82 despues de que todos los dígitos del número de la cuenta Z_1-Z_N hayan sido aplicados a la dirección pseudo-aleatoria ROM 40 y el dígito menos significativo Z_1 haya sido, por segunda vez aplicado a la dirección pseudo-aleatoria ROM 40 (en la etapa 120 del registrador 82 en ela Tabla 4). La señal de control del modo de generación P.I.N. (PING) inhibe la aplicación de las señales de fijación de retroalimentación al registrador 48 en cuyo momento cada dígito generado ROM 40 del P.I.N. se compara con los correspondientes dígitos del número secreto en el comparador 24. La señal de control de modo (PING) se genera por el registro 82 a continuación de la segunda aplicación de los dígitos del número de la cuenta que son recirculados en el registro 44 para dirrigirse de manera pseudo-aleatoria a ROM 40.

En la secuencia,(PING) se genera por el registro de memoria 82 desde las etapas (11N + 10) ... (11N + 16). Cuando el bitio en el registro 82 se desplaza a la etapa (11N + 9) (etapa 119 cuando N = 10), el primer dígito del P.I.N. generado se almacena en el registro 48. El control de la señal (PING) se aplica para impedir que el registro 48 quede fijado por la señal de fijación de retroalimentación (FS) hasta despues de que el dígito almacenado ha sido comparado con el correspondiente número secreto asentado

en el teclado. La señal de control de modo (CAN) se genera de nuevo por el registro 82 en la etapa (11N + 17) y ROM 40 es dirigida pseudo-aleatoriamente utilizando el próximo dígito menos significativo Z_2 del número de la cuenta.

El dígito Z_2 del número de la cuenta se desplaza en posición en el registro 44 para dirigir ROM 40 por la generación de impulsos de desplazamiento (ZSP) procedentes del circuito de la Figura 5(c).

Cuando el bitio almacenado en el registro 82 se desplaza a la etapa (11N + 27) (etapa 137 cuando N = 10 como en la Tabla 4), el segundo de ROM 40 que ha generado P.I.N. se almacena en el registro 48 y la señal (PING) se aplica para inhibir la aplicación de los impulsos de fijación de retroalimentación al registro 48 durante la comparación del dígito almacenado con el correspondiente dígito de un dígito m del número secreto M. La generación de señales de control de modo alternativamente (PING) y (CAN), que corresponden respectivamente a la generación y comparación del tercero y cuarto dígitos P.I.N. con el tercero y cuarto dígitos del número secreto M, se ilustra en la Tabla 4 para un número de cuenta de diez dígitos y un número secreto de cuatro dígitos (N=10, m=4). A continuación del ciclo de verificación en la etapa (11N + 18m-1) del registro 82 (etapa 181 en la Tabla 4), la señal de presentación (DISPLAY) se genera por el registro de memoria 82 para presentar el paso o no-paso del resultado de la verificación. La señal de control (DISPLAY) se suministra para presentar la unidad 33 en la Figura 1.

En la materialización física preferente, las señales

(LD), (IIN), (CAN), (DISPLAY) y (RESET) se suministran por el registro de desplazamiento 82; las restantes señales se derivan del registro 82 suministrando señales por medio de la circuitería lógica.

La Figura 5b es un diagrama lógico de un circuito para la generación, sensible a las señales generadas por el registro de derivación 82, las señales (FS) y (COMPCLK). La señal de fijación de retroalimentación (FS) se aplica al registro de control 48; la señal del reloj comparador (COMPCLK) se aplica a los circuitos contadores 71 y 72 cada vez que ha sido hecha una comparación positiva entre un dígito del P.I.N. y un dígito correspondiente del número secreto M en el modo de generación P.I.N.

La señal de fijación de la retroalimentación (FS) comprende un grupo de tremes de impulsos, preferentemente siete impulsos por tren, que se genera durante el modo de operación número de cuenta sensible a la señal del control de modo (CAN). Además, un solo impulso de fijación se aplica durante el modo de operación del número de identificación de la institución en donde ROM 40 está inicialmente dirigida con los datos del número de identificación de la institución.

La etapa ocho del registro de desviación en serie 84 está controla-da por impulsos de despalzamiento generados por el paso NAND 85 y el paso OR 87. Las salidas paralelas de las etapas del registro está normalmente en un lógico uno. Los impulsos de desplazamiento se aplican al terminal de desplazamiento SH del registro 84 durante la generación de los modos de operación del número de cuenta y P.I.N.

La salida $\overline{Q}$ del basculador de dirsposición-redisposi

ción 89, conectada al terminal de entrada IN del registro 84, carga una sola señal lógica cero dentro de la primera etapa del registro de desplazamiento.

Posteriormente a esto el basculador 89 se redispone automáticamente por medio del circuito de retroalimentación 89a conectado al terminal de redisposición R. El paso 86, conectado a la primera y octava etapas del registro 84, proporciona una señal lógico uno al basculador 88a cuando la señal lógico cero, almacenada en el registro 84, está localizada en la primera u octava etapas del mismo. El basculador J-K 86a está accionado como un basculador articulado y suministra una señal lógico uno a una entrada del paso 88 mientras el lógico cero en el registro 84 está en las etapas dos a ocho. La señal del reloj (CL) procedente del generador de la señal del reloj 80 se suministra a la otra entrada del paso 88. Durante los modos CAN y PING, sensibles a la señal del reloj (CL) y basculador 86a, el paso 88 genera trenes de impulsos sincronizados con el generador del reloj 80, conteniendo cada tren siete impulsos. El paso 90 hace que se añada un impulso al tren de impulsos únicamente durante el modo IIn de operación. El paso OR 92 genera un tren de impulsos que incluye tanto el tren de impulsos generado por el paso 88 como el impulso aislado durante el modo IIN suministrado por el paso 90.(PING), aplicado a través del inversos binario 95a al paso NAND 95, inhibe la señal de fijación de retroalimentación (FS) durante el modo PING de operación. Durante el modo PING, los dígitos P.O.N., almacenados en el registro 48, se comparan con los dígitos del teclado que han asentado el número secreto M.

La señal (COMPCKK), que se aplica al contador de fijación 70 durante cada siete ciclos de dirección de ROM 40 en el modo de operación que genera el P.I.N., se deriva - al hacer lógicamente NAND la señal de salida de una etapa del registro 84 con señal de control de modo (PING) en el paso 94. El paso NAND 94 se muestra conectado al terminal de salida de la cuarta etapa del registro 84 pero se entiende que el paso 94 puede concetarse a cualquiera de - las etapas 2-8 de aquel. Una señal de salida se deriva de la última etapa del registro 84.

Esta señal de salida se utiliza para sincronizar la generación de los impulsos de desviación del número de - cuenta (ZSP) como se indica en la Figura 5(c).

Haciendo referencia a la Figura 5(c), los impulsos - (ZSP) se generán por el ordenador de secuencia 46 y se aplican al registro de desplazamiento 44 en la Figura 2 durante el modo CAN de operación.

Los impulsos (ZSP) comprenden trenes de cuatro impulsos cuando se inician a continuación de cada conjunto de siete direcciones pseudo-aleatorias generadas por ROM 40. Cada tren de impulsos (ZSP) se suministra al terminal de desplazamiento SH del registro de desplazamiento 44 para originar un avance de cuatro etapas de los bitios almacenados en el registrador, es decir, un dígito.

El paso NAND es sensible a (CL) (generado por el generador reloj 80), el basculador 96 y (CAN). Durante el - modo CAN de operación, se sumimistra una señal lógico uno a uno de los terminales de entrada del paso NAND 99. Cuando se genera una señal lógico cero por la última etapa del registro 84, el basculador 96 suministra una señal lógico

uno al paso 99. Bajo el estado descrito, el paso NAND - 99 suministra impulsos de reloj (CL) al terminal de desplazamiento SH del registro de desplazamiento de cuatro etapas en serie 98.

Los terminales de salida de las etapas del registro 98 están normalmente en lógico uno. La salida $\overline{Q}$ del basculador 100 carga únicamente la primera etapa del registro de desplazamiento 98 con una señal lógico cero; la salida $\overline{Q}$ del basculador 100 se redispone posteriormente a esto a una señal lógico uno por medio del circuito de retroalimentación 100a/. Las señales suministradas al terminal de desplazamiento SH por el paso NAND 99 avanzan en serie la señal lógico cero en el registro de desplazamiento 98.

Las señales de salida de cada etapa del registro 98 despues de su inversión en binarias por los invertidores 98a, se aplican al paso OR 102. La salida del paso OR 102 se convierte lógicamente en NAND con (CL) en el paso 103. El invertidor binario 103a, sensible al paso 103, genera trenes de impulsos que contienen cuatro impulsos por tren comprendiendo /ZSP).

La salida de la última etapa del registro 98 se hace volver a los terminales de disposición S del basculador 89 y al terminal R del basculador 98 para preparar el circuito generador (ZSP) para otro ciclo de operación.

Todos los componentes del presente sistema son convencionales y están preferentemente formados de TTL lógico. Debe entenderse que el sistema podría construirse con otros tipos de familias lógicas tales como DTL, RTL ó MOS lógicos, aunque TTL se prefiere en vista de la relativa-

mente alta velocidad y elevada inmunidad al ruido características de la familia TTL. La circuitería del tipo - CMOS podría tambien utilizarse si se desea, especialmente donde se requiera una elevada inmunidad al ruido.

Un aspecto importante de la presente invención es - que el número de identificación de la institución, aparte de ser una "clave" o punto de arranque para la dirección pseudo-aleatoria de ROM 40, tambien proporciona un medio para cargar una transacción a la institución emisora de la tarjeta o que retiene la cuenta identificada. - En los casos en que las instituciones son parte de una - red de intercambio en la que a un cliente que tenga una cuenta en una institución se le permite hacer transacciones en una institución cooperadora, la presente invención proporciona tal transacción en tanto que es preventiva - de la acumuladión de contabilidad. En cada institución - cooperadora, el sistema de verificación responde al número de identificación de la institución localizado en el campo 12 de la tarjeta 10 y transfiere una señal representativa del número de identificación de la institución a una red de contabilidad central para informar a la red - que la presente transacción debe cargarse a la institución que tiene el número de identificación. Debido a que las instituciones cooperadoras tienen idénticas memorias magnéticas sólo de lectura (ROM 40), una tarjeta standard es verificable en todas las instituciones cooperadoras, siendo cargada la transacción únicamente a la institución identificada. De esta manera, un cliente bancario puede retirar fondos de su cuenta de ahorro en el banco B desde un terminal no atendido en el banco A, o un comprador

puede realizar una compra a crédito contra una cuenta de crédito con la institución de crédito C en un punto de terminal de ventas que acepte el crédito de la institución de crédito C y otras.

Como ejemplo, supongamos que un cliente es portador de una tarjeta que tiene un número de cuenta 0123456789 y un número de identificación de la institución 12 el cual cuando se aplica al terminal de verificación de la institución emisora genera un P.I.N. de 1234 (en exadecimal). La tarjeta, cuando se presenta en otra institución que tenga el número de identificación 15 tambien genera el P.I.N. 1234 (en exadecimal) puesto que las memorias están identicamente programadas en las dos instituciones y el sistema responde únicamente a los datos contenidos en la tarjeta. No obstante, el sistema en la institución 15, que reponde al número de identificación de la institución en el campo 12 de la tarjeta, aparte de verificar que el poseedor de la tarjeta es el poseedor autorizado, carga la transacción a la cuenta 0123456789 en la institución que tenga el número de identificación 12. La transacción no se carga a una cuenta que tenga un número idéntico mantenido por la institución 15. Por el contrario, una tarjeta que lleve un número de identificación de una institución de una institución no cooperadora cuando se aplica al sistema de verificación de la presente invención genera un P.I.N. que no guarda correlación con el número secreto predeterminado, incluso si el número de cuenta es idéntico al del anterior ejemplo debido a que el número de la institución no cooperadora genera un diferente punto de arranque de la dirección o "clave" a ROM 40 del de

el ejemplo anterior. Por lo tanto, números de cuenta idén ticos pueden ser simultáneamente activos en diferentes - instituciones pero debido al número de identificación de cada institución que es único, P.I.N. se generan únicamen te de los datos contenidos en la tarjeta y la transacción se carga únicamente a la institución identificada.

Si la tarjeta standard se aplica al sistema de veri ficación de una institución no-cooperadora, se genera un P.I.N. que no tiene correlación debido a que los sistemas de verificación de las instituciones no-cooperadoras con tienen memorias magnéticas sólo de lectura (ROM 40) que están programadas diferentemente de las instituciones coo peradoras. Desde luego, las instituciones no-cooperadoras pueden cooperar en otro sistema de instituciones coopera doras que estén provistas con los sistemas de verifica- ción de la presente invención que tengan ROM 40s idénti- camente programados.

Cuando el número secreto proporcionado al cliente - es el P.I.N. generado pseudo-aleatoriamente derivado de los números de la cuenta y de identificación de la insti tución en el traductor de números 30, el número secreto, asentado en el teclado por el cliente, se compara direc- tamente con el P.I.N. generado por ROM 40 durante un ci- clo de verificación. Resulta ventajoso, como una ayuda a la memoria del cliente, permitir que éste seleccione un número secfeto que pueda recordar fácilmente y entonces convertir el número secreto en un número que tenga corre lación durante la verificación. Si el número secreto se selecciona por el cliente en el momento de la emisión - de una tarjeta, se añade un número de neutralización al

P.I.N. seleccionado por el cliente para formar el resultante P.I.N. que se compara positivamente con el P.I.N. generado por ROM 40. La relación para la verificación de la tarjeta se describe mediante la siguiente ecuación:

$$(CSPIN)_{10} + (OFFSET)_{10} = (GPIN) \text{ (sin exceso)}$$

cuando CSPIN es el número de identificación personal seleccionado por el cliente, OFFSET es una conversión del número de neutralización y GPIN es el P.I.N. generado por ROM 40.

El número de neutralización OFFSET está contenido en la tarjeta 10 preferiblemente en el campo 14 y se desarrolla en el momento de emisión de la tarjeta partiendo de la siguiente ecuación:

$$(OFFSET)_{10} = (GPIN)_{10} - (CSPIN)_{10} \text{ (sin préstamo)}$$

Con objeto de evitar la presencia de dígitos negativos $(OFFSET)_{10}$ con anterioridad a la sustracción, el número diez se añade individualmente a cada dígito de $(GPIN)_{10}$ que es menos que el correspondiente dígito de $(CSPIN)_{10}$.

Durante la verificación, el P.I.N. derivado del número secreto seleccionado por el cliente y el número OFFSET pueden generarse por un circuito sumador decimal sin exceso. Otro medio para sumar el número secreto y el número OFFSET en decimal sin exceso es proporcionar una memoria magnética sólo de lectura que esté programada para generar caracteres que representen la suma decimal sin exceso de cada dígito del número secreto y el número de neutralización.

En la Figura 6, ROM 110 está programada para generar, en los terminales $O_1 - O_4$, la suma decimal sin exceso, de dos dígitos de cuatro bitios, es decir, el dígito del nú

mero secreto y el dígito OFFSET, aplicados para dirigir los terminales I_1-I_4 y I_5-I_8 deaquel. El registro 112 almacena los dígitos del número secreto M asentado en el teclado por el cliente y el registro 114 almacena los dígitos del número de neutralización OFFSET leído de la tarjeta 10 por el lector de tarjeta 18. Estos registros están paralelamente cargados con señal (LD). Cuando el número secreto es un número de cuatro dígitos $M_1M_2M_3M_4$, los registros 112 y 114 contienen 16 etapas cada uno. Despues que se ha producido la primera señal (PING), el circuito de desplazamiento 116 permite que los datos en los registros 112 y 114 sean desplazados serialmente simultáneamente con el registro 44. Esto asegura que el número de neutralización y el número secreto estarán sincronizados con el adecuado GPIN para su comparación.

El circuito de desplazamiento 116 comprende el basculador tió D 124, el paso NAND 126 y el inversor 128. El basculador 124, sensible al primer (PING) despues de la redisposición, registra el hecho de que la secuencia PING-CAN ha sido asentada, y de este modo suministra un lógico uno a una entrada de NAND 126. ZSP se suministra al otro terminal de entrada de NAND 126. NAND 126, a través del inversor 128, suministra los requeridos impulsos de desplazamiento a los terminales SH de los registros 112 y 114, para el resto de la secuencia PING-CAN, La redisposición interrumpirá estos impulsos para la secuencia inicial CAN.

La Figura 7 es un diagrama en bloque simplificado de aparato para generar un número secreto a un cliente en el momento de emisión de la tarjeta. El generador del número

secreto 130 comprende el registro 132 para almacenar temporalmente los datos del número de identificación de la institución y los datos del número de cuenta del cliente, circuitería de control 134, primera memoria sólo de lectura 138. El registro 132 es idéntico a los registros 42 y 44 en la Figura 2, el control 134 es idéntico a los conmutadores 50, 52, 54, 56 y el circuito EXCLUSIVE OR - 51, y ROM 136 es idéntica a ROM 40.

ROM 138 es la inversa de ROM 110 en la Figura 6, es decir, está programada para general la diferencia entre los dígitos individuales de CSPIN y GPIN en base 10 a fin de proporcionar el OFFSET.

Con objeto de evitar el acaecimiento de dígitos negativos $(OFFSET)_{10}$, con anterioridad a la sustracción el número "diez" se añade individualmente a cada dígito de - $(CSPIN)_{10}$. De nuevo, si se desea, ROM 138 puede ser un - sustractor en circuito decimal. No obstante, se prefiere una ROM porque es fácilmente disponible y es idéntica a ROM 138 y ROM 40. Un ordenador de secuencia (no indicado) tal como el ordenador de secuencia 46 de la Figura 2 proporciona la sincronización y señales de control al generador 130. Sensible a un número de identificación de una institución y número de la cuenta del cliente, aplicado al registro 132, el generador 130 del número secreto produce un número secreto en una presentación alfabético-numérica o impresión para informar al cliente de su número secreto. Esta operación fué descrita en detalle con respecto a la Figura 1.

En el sistema de verificación 30 de la Figura 2, el P.I.N. fué aplicado al comparador 24 para su comparación

con el número secreto. Si no se utiliza un P.I.N. seleccionado por el cliente (CSPIN), el cliente entrega el GPIN a la memoria; cuando se utiliza un CSPIN, OFFSET se deriva del circuito de sustracción decimal 138 que decimalmente sustrae el P.I.N. seleccionado por el cliente del ROM 136 que ha engendrado otro P.I.N., siendo el resultante OFFSET registrado en el campo 14 de la tarjeta 10. La tarjeta 10 puede contener registrados en la misma datos tales como los datos del número de identificación de la institución y datos del número de la cuenta con anterioridad a la emisión de la misma, con lo que los datos son leídos por el aparato de la Figura 7 con medios convencionales lectores de tarjeta, tal como un sensor magnético, el aparato que genera OFFSET y P.I.N., y entonces registrar los datos del númeroOFFSET sobre la tarjeta. Alternativamente, todos los datos que incluyen los datos del número OFFSET puede registrarse sobre la tarjeta en el momento de emisión con lo que los datos de identificación de la institución y número de cuenta se suministran al aparato de la Figura 7 y los datos de identificación junto con los datos del número OFFSET generado se registran sobre la tarjeta.

Aunque el debate sobre la presente invención se ha dirigido primordialmente al ambiente bancario, debe entenderse que la invención no queda limitada exclusivamente a eso. Se apreciará que los métodos y aparatos aquí descubiertos son totalmente aplicables para la convalidación de cualquier tarjeta y otro distintivo que lleve un número de cuenta u otros indicios utilizados con fines crediticios, acceso a un sistema de seguridad o cualesquiera o-

tras finalidades de identificación.

De particular importancia, los datos del número de identificación de la institución que están almacenados en el registro 26 para interrogación por el sistema central de contabilidad se aplican tanto para dirigir inicialmente o "poner en clave" ROM 40 a la salida de un ciclo de dirección pseudo-aleatorio durante la verificación de una tarjeta como para cargar una transacción autorizada a la institución identificada. Deberá entenderse que mientras un número de identificación de la institución formado por dos dígitos ha sido descrito a modo de ejemplo; pueden utilizarse tres o más dígitos con lo cual dos de los dígitos se seleccionan como el conjunto de bitios de dirección clave para ROM 40 y el sistema de contabilidad central 28 es sensible a todos los dígitos para su identificación.

En tanto ha sido descrita e ilustrada una materialización física específica de la invención, deberá estar claro que pueden realizarse variaciones de los detalles de construcción que está específicamente ilustrados y descritos sin apartarse del verdadero espíritu y alcance de la invención. Por ejemplo, se entiende que el número de cuenta y el número secreto pueden contener cualquier número de dígitos; no obstante, cuatro dígitos del número secreto es un límite superior práctico dado que el número secreto se entrega a la memoria por el cliente. Tambien se entiende que mientras cada dígito del número de cuenta se dirige pseudo-aleatoriamente a ROM 40 siete veces en la materialización física preferente, puede utilizarse cualquier otro número. Además, en tanto que los datos

de salida generados por ROM 40 están dispuestos EXCLUSIVE OR con dígitos del número de cuenta para generar direcciones pseudo-aleatorias, se entiende que otras operaciones adecuadas lógicas o aritméticas pueden realizarse en la salida de datos para proporcionar la genración de direcciones pseudo-aleatorias, siempre que la particular operación utilizada no degrade sustancialmente el carácter aleatorio de los datos de salida.

TABLA 1

No. de secuencia	A_1 A_2	Z_1	I_1-I_8	O_1-O_8
2	10011000	Ø	10011000	11100011
3	Ø	0100	11100111	01001101
4	Ø	0100	01001001	11011100
5	Ø	0100	11011000	01110011
6	Ø	0100	01110111	11011110
7	Ø	0100	11011010	11000111
8	Ø	0100	11000011	10010101
9	Ø	0100	10010001	10111000

Ø = Sin importancia

TABLA 2

No. de secuendia	A_1 A_2	Z_1	I_1-I_8	O_1-O_8
112	Ø			10011001
113	Ø	0100	10011101	01001011
114	Ø	0100	01001111	01011101
115	Ø	0100	01011001	10111110
116	Ø	0100	10111010	11101001
117	Ø	0100	11101101	01101011
118	Ø	0100	01101111	10001001
119	Ø	0100	10001101	0101 0011

Ø = Sin importancia

[ ] = dígito más significativo de P.I.N.

TABLA 3

Decimal	Exadecimal	BCD†	Complemento BCD††	Decimal
0	0000	1000	0111	7
1	0001	1001	0110	6
2	0010	1010	0101	5
3	0011	1011	0100	4
4	0100	1100	0011	3
5	0101	1101	0010	2
6	0110	0110	1001	9
7	0111	0111	1000	8
8	1000	1000	0111	7
9	1001	1001	0110	6
10	1010	1010	0101	5
11	1011	1011	0100	4
12	1100	1100	0011	3
13	1101	1101	0010	2
14	1110	1110	0001	1
15	1111	1111	0000	0

† Suministrado al comparador 24 por el convertidor 53

†† Suministrado al comparador 24 por el teclado 22

TABLA 4

No. del impulso del reloj	LD	IIN	CAN	PING	FS	ZSP	COMPCLK	PRESENTACION	REDISPOSICION
1	1	0	0	0	0	0	0	0	0
2	0	1	0	0	1	0	0	0	0
3	0	0	1	0	1	0	0	0	0
4	0	0	1	0	1	0	0	0	0
5	0	0	1	0	1	0	0	0	0
6	0	0	1	0	1	0	0	0	0
7	0	0	1	0	1	0	0	0	0
8	0	0	1	0	1	0	0	0	0
9	0	0	1	0	1	0	0	0	0
10	0	0	1	0	0	1	0	0	0
11	0	0	1	0	0	1	0	0	0
12	0	0	1	0	0	1	0	0	0
13	0	0	1	0	0	1	0	0	0
14	0	0	1	0	1	0	0	0	0
15	0	0	1	0	1	0	0	0	0
16	0	0	1	0	1	0	0	0	0
17	0	0	1	0	1	0	0	0	0
18	0	0	1	0	1	0	0	0	0
19	0	0	1	0	1	0	0	0	0
20	0	0	1	0	1	0	0	0	0
21	0	0	1	0	0	1	0	0	0
22	0	0	1	0	0	1	0	0	0
23	0	0	1	0	0	1	0	0	0
24	0	0	1	0	0	1	0	0	0
25	0	0	1	0	1	0	0	0	0
26	0	0	1	0	1	0	0	0	0
27	0	0	1	0	1	0	0	0	0
28	0	0	1	0	1	0	0	0	0
29	0	0	1	0	1	0	0	0	0
30	0	0	1	0	1	0	0	0	0
31	0	0	1	0	1	0	0	0	0
32	0	0	1	0	0	1	0	0	0
33	0	0	1	0	0	1	0	0	0
34	0	0	1	0	0	1	0	0	0
35	0	0	1	0	0	1	0	0	0
36	0	0	1	0	1	0	0	0	0
37	0	0	1	0	1	0	0	0	0
38	0	0	1	0	1	0	0	0	0
39	0	0	1	0	1	0	0	0	0
40	0	0	1	0	1	0	0	0	0
41	0	0	1	0	1	0	0	0	0
42	0	0	1	0	1	0	0	0	0
43	0	0	1	0	0	1	0	0	0
44	0	0	1	0	0	1	0	0	0
45	0	0	1	0	0	1	0	0	0
46	0	0	1	0	0	1	0	0	0

47	0	0	1	0	1	0	0	0 0
48	0	0	1	0	1	0	0	0 0
49	0	0	1	0	1	0	0	0 0
50	0	0	1	0	1	0	0	0 0
51	0	0	1	0	1	0	0	0 0
52	0	0	1	0	1	0	0	0 0
53	0	0	1	0	1	0	0	0 0
54	0	0	1	0	0	1	0	0 0
55	0	0	1	0	0	1	0	0 0
56	0	0	1	0	0	1	0	0 0
57	0	0	1	0	0	1	0	0 0
58	0	0	1	0	1	0	0	0 0
59	0	0	1	0	1	0	0	0 0
60	0	0	1	0	1	0	0	0 0
61	0	0	1	0	1	0	0	0 0
62	0	0	1	0	1	0	0	0 0
63	0	0	1	0	1	0	0	0 0
64	0	0	1	0	1	0	0	0 0
65	0	0	1	0	0	1	0	0 0
66	0	0	1	0	0	1	0	0 0
67	0	0	1	0	0	1	0	0 0
68	0	0	1	0	0	1	0	0 0
69	0	0	1	0	1	0	0	0 0
70	0	0	1	0	1	0	0	0 0
71	0	0	1	0	1	0	0	0 0
72	0	0	1	0	1	0	0	0 0
73	0	0	1	0	1	0	0	0 0
74	0	0	1	0	1	0	0	0 0
75	0	0	1	0	1	0	0	0 0
76	0	0	1	0	0	1	0	0 0
77	0	0	1	0	0	1	0	0 0
78	0	0	1	0	0	1	0	0 0
79	0	0	1	0	0	1	0	0 0
80	0	0	1	0	1	0	0	0 0
81	0	0	1	0	1	0	0	0 0
82	0	0	1	0	1	0	0	0 0
83	0	0	1	0	1	0	0	0 0
84	0	0	1	0	1	0	0	0 0
85	0	0	1	0	1	0	0	0 0
86	0	0	1	0	1	0	0	0 0
87	0	0	1	0	0	1	0	0 0
88	0	0	1	0	0	1	0	0 0
89	0	0	1	0	0	1	0	0 0
90	0	0	1	0	0	1	0	0 0
91	0	0	1	0	1	0	0	0 0
92	0	0	1	0	1	0	0	0 0
93	0	0	1	0	1	0	0	0 0
94	0	0	1	0	1	0	0	0 0
95	0	0	1	0	1	0	0	0 0
96	0	0	1	0	1	0	0	0 0
97	0	0	1	0	1	0	0	0 0
98	0	0	1	0	0	1	0	0 0
99	0	0	1	0	0	1	0	0 0
100	0	0	1	0	0	1	0	0 0
101	0	0	1	0	0	1	0	0 0
102	0	0	1	0	1	0	0	0 0
103	0	0	1	0	1	0	0	0 0
104	0	0	1	0	1	0	0	0 0
105	0	0	1	0	1	0	0	0 0

106	0	0	1	0	1	0	0	0	0
107	0	0	1	0	1	0	0	0	0
108	0	0	1	0	1	0	0	0	0
109	0	0	1	0	0	1	0	0	0
110	0	0	1	0	0	1	0	0	0
111	0	0	1	0	0	1	0	0	0
112	0	0	1	0	0	1	0	0	0
113	0	0	1	0	1	0	0	0	0
114	0	0	1	0	1	0	0	0	0
115	0	0	1	0	1	0	0	0	0
116	0	0	1	0	1	0	0	0	0
117	0	0	1	0	1	0	0	0	0
118	0	0	1	0	1	0	0	0	0
119	0	0	1	0	1	0	0	0	0
120	0	0	0	1	0	0	0	0	0
121	0	0	0	1	0	0	0	0	0
122	0	0	0	1	0	0	0	0	0
123	0	0	0	1	0	0	1	0	0
124	0	0	0	1	0	0	0	0	0
125	0	0	0	1	0	0	0	0	0
126	0	0	0	1	0	0	0	0	0
127	0	0	1	0	0	1	0	0	0
128	0	0	1	0	0	1	0	0	0
129	0	0	1	0	0	1	0	0	0
130	0	0	1	0	0	1	0	0	0
131	0	0	1	0	1	0	0	0	0
132	0	0	1	0	1	0	0	0	0
133	0	0	1	0	1	0	0	0	0
134	0	0	1	0	1	0	0	0	0
135	0	0	1	0	1	0	0	0	0
136	0	0	1	0	1	0	0	0	0
137	0	0	1	0	1	0	0	0	0
138	0	0	0	1	0	0	0	0	0
139	0	0	0	1	0	0	0	0	0
140	0	0	0	1	0	0	0	0	0
141	0	0	0	1	0	0	1	0	0
142	0	0	0	1	0	0	0	0	0
143	0	0	0	1	0	0	0	0	0
144	0	0	0	1	0	0	0	0	0
145	0	0	1	0	0	1	0	0	0
146	0	0	1	0	0	1	0	0	0
147	0	0	1	0	0	1	0	0	0
148	0	0	1	0	0	1	0	0	0
149	0	0	1	0	1	0	0	0	0
150	0	0	1	0	1	0	0	0	0
151	0	0	1	0	1	0	0	0	0
152	0	0	1	0	1	0	0	0	0
153	0	0	1	0	1	0	0	0	0
154	0	0	1	0	1	0	0	0	0
155	0	0	1	0	1	0	0	0	0
156	0	0	0	1	0	0	0	0	0
157	0	0	0	1	0	0	0	0	0
158	0	0	0	1	0	0	0	0	0
159	0	0	0	1	0	0	1	0	0
160	0	0	0	1	0	0	0	0	0
161	0	0	0	1	0	0	0	0	0
162	0	0	0	1	0	0	0	0	0
163	0	0	1	0	0	1	0	0	0

164	0	0	1	0	0	1	0	0	0
165	0	0	1	0	0	1	0	0	0
166	0	0	1	0	0	1	0	0	0
167	0	0	1	0	1	0	0	0	0
168	0	0	1	0	1	0	0	0	0
169	0	0	1	0	1	0	0	0	0
170	0	0	1	0	1	0	0	0	0
171	0	0	1	0	1	0	0	0	0
172	0	0	1	0	1	0	0	0	0
173	0	0	1	0	1	0	0	0	0
174	0	0	0	1	0	0	0	0	0
175	0	0	0	1	0	0	0	0	0
176	0	0	0	1	0	0	0	0	0
177	0	0	0	1	0	0	1	0	0
178	0	0	0	1	0	0	0	0	0
179	0	0	0	1	0	0	0	0	0
180	0	0	0	1	0	0	0	0	0
181	0	0	0	0	0	0	0	1	0
182	0	0	0	0	0	0	0	0	1

1.- Perfeccionamientos en la verificación de trajetas de identificación legibles a máquina en transacciones comerciales, caracterizada porque traduce un número de cuenta contenido en una tarjeta y establece la correlación del número traduccido con un número secreto conocido unicamente por el poseedor autorizado de la tarjeta para proporcionar una señal indicativa de la validez de la tarjeta, comprendiendo la mejora medios sensibles a los datos de identificación de la institución contenidos en dicha tarjeta para determinar la traducción de dicho número de cuenta; y medios sensibles a dichos datos de identificación de la institución para cargar una transacción a una institución identificada.

2.- Perfeccionamientos en la verificación de tarjetas de identificación legibles a máquina en transacciones comerciales, según la reivindicación 1, caracterizada porque los medios determinantes de la traducción incluyen medios de memoria dirigibles que contienen conjuntos de bitios allí almacenados al azar, formando dichos datos de identificación de la institución un conjunto de bitios de dirección inicial para dirigirse de una manera pseudoaleatoria a dichos medios de memoria.

3.- Perfeccionamientos en la verificación de tarjetas de identificación legibles a máquina de transacciones comerciales según la reivindicación 1 caracterizada porque los medios para cargar una transaccuín incluyen elementos de registro y almacenamiento para almacenar los datos del número de identificación de la institución, y elemento para transferir los datos del número de identificación de dicha institución a un sistema central de contabili-

dad.

4.- Perfeccionamientos en la verificación de tarjetas de identificación legibles a máquina en transacciones comerciales, según la reivindicación nº 1 caracterizada porestar dotada de medios para determinar si el poseedor de una tarjeta está autorizado para completar una transacción, conteniendo la tarjeta unos primeros datos que identifican una institución y unos segundos datos que identifican un número de cuenta, suministrando dicho poseedor al sistema los datos del número secreto derivados de dichos primeros y segundo datos, comprendiendo: un medio dirigible de memoria; medios sensibles a dichos primeros datos para dirigir una posición de los medios de memoria y originando que dichos medios de memoria generan una primera señalde salida; medios sensibles a dicho primera señal de salida y dichos segundos datos para dirigir dichos medios de memoria y originar que dichos medios de memoria generen una segunda señal de salida; medios para comparar dicha segunda señal de salida con los datos de dicho número secreto y para generar una señal de paso o no-paso; medios para generar una señal de convalidación de acuerdo con dicha señal, de paso o no-paso; y medios para cargar una transacción autorizada a una institución identificada por dichos primeros datos.

5.- Perfeccionamientos en la verificación de tarjetas de identificación legibles a máquina en transacciones comerciales, según la reifindicación 4 caracterizado porque los medios de dirección sensibles a la primera señal de salida y los segundos datos incluyen medios para combinar lógicamente la primera señal de salida y los segun

dos datos para formar un conjunto de bitios de dirección para dichos medios de memoria.

6.- Perfeccionamientos en la verificación de tarjetas de identificación legibles a máquina en transacciones comerciales, según la reivindicación 4 caracterizada porque los del tipo denominado medios de comparación incluyen en circuito EXCLUSIVE OR (sin traducir al español) - para comparar los bitios de dicha segunda señal de salida con los bitios de los datos de dicho número secreto.

7.- Perfeccionamientos en la verificación de tarjetas de identificación legibles a máquina de transacciones comerciales, según la reivindicación 4 caracterizada porque los medios de cargo incluyen elementos de registro para almacenar los primeros datos, y medios para suministrar dichos datos almacenados a un sistema central de contabilidad.

8.- Perfeccionamientos en la verificación de tarjetas de identificación legibles a máquina en transacciones comerciales, según la reivindicación 1 caracterizada porque el intercambio de transacción entre las instituciones financieras cooperadoras, existiendo dichas instituciones a los clientes autorizados una tarjeta standard - que contiene datos que incluyen los datos del número de identificación de la institución y datos del número de - la cuenta, en la que dicho cliente autorizado asienta - los datos del número secreto derivados de dichos datos - del número de cuenta e identificación, comprendiendo: medios para traducir dichos datos del número de identificación de la institución y los dichos datos del número de cuenta en tados de identificación representativos de un

número de identificación personal no averiguable; medios para establecer la correlación entre dichos datos de identificación con los datos de dicho número secreto para proporcionar una señal de paso o no-paso; y medios sensibles a dicha señal de paso y los datos del número de identificación de dicha institución para cargar una transacción requerido a una institución identificada por dichos datos del número de identificación.

9.- Perfeccionamientos en la verificación de tarjetas de identificación legibles a máquina en transacciones comerciales, según la reivindicación 8, caracterizado porque los medios de traducción incluyen una memoria dirigible que tiene almacenados allí conjuntos de bitios al azar incluyendo dicho sistema además medios para dirigirse de manera pseudo-aleatoria a las posiciones de almacenamiento de dicha memoria dirigible medios para generar conjuntos de bitios de salida, incluyendo determinado de esos conjuntos de bitios dígitos de dicho número de identificación personal no averiguable.

10.- Perfeccionamientos en la verificación de tarjetas de identificación legibles a máquina en transacciones comerciales, según la reivindicación 8, caracterizado porque los medios de traducción además incluyen medios para combinar lógicamente de manera sucesiva los datos generados por dichos medios de memoria dirigibles con dígitos de los datos del número de cuenta para formar conjuntos de bitios de dirección pseudo-aleatorios para dirigir las posiciones de almacenamiento de dichos medios de memoria dirigible.

11.- Perfeccionamientos en la verificación de tarjetas

de identificación legibles a máquina en transacciones comerciales, según la reivindicación 8, caracterizado porque los medios de correlación comprenden un comparador - digital.

12.- PERFECCIONAMIENTOS EN LA VERIFICACION DE TARJETAS DE IDENTIFICACION LEGIBLES A MAQUINA EN TRANSACCIONES COMERCIALES.

Todo conforme se describe en la Memoria que antecede, se ilustra como ejemplo de ejecución en los planos unidos a ella y se reivindica.

Esta Memoria consta de sesenta hojas foliadas, escritas a máquina por una sóla cara y planos que la acompañan.

Madrid, 10 de Febrero de 1977

DIEBOLD INCORPORATED

P.A.

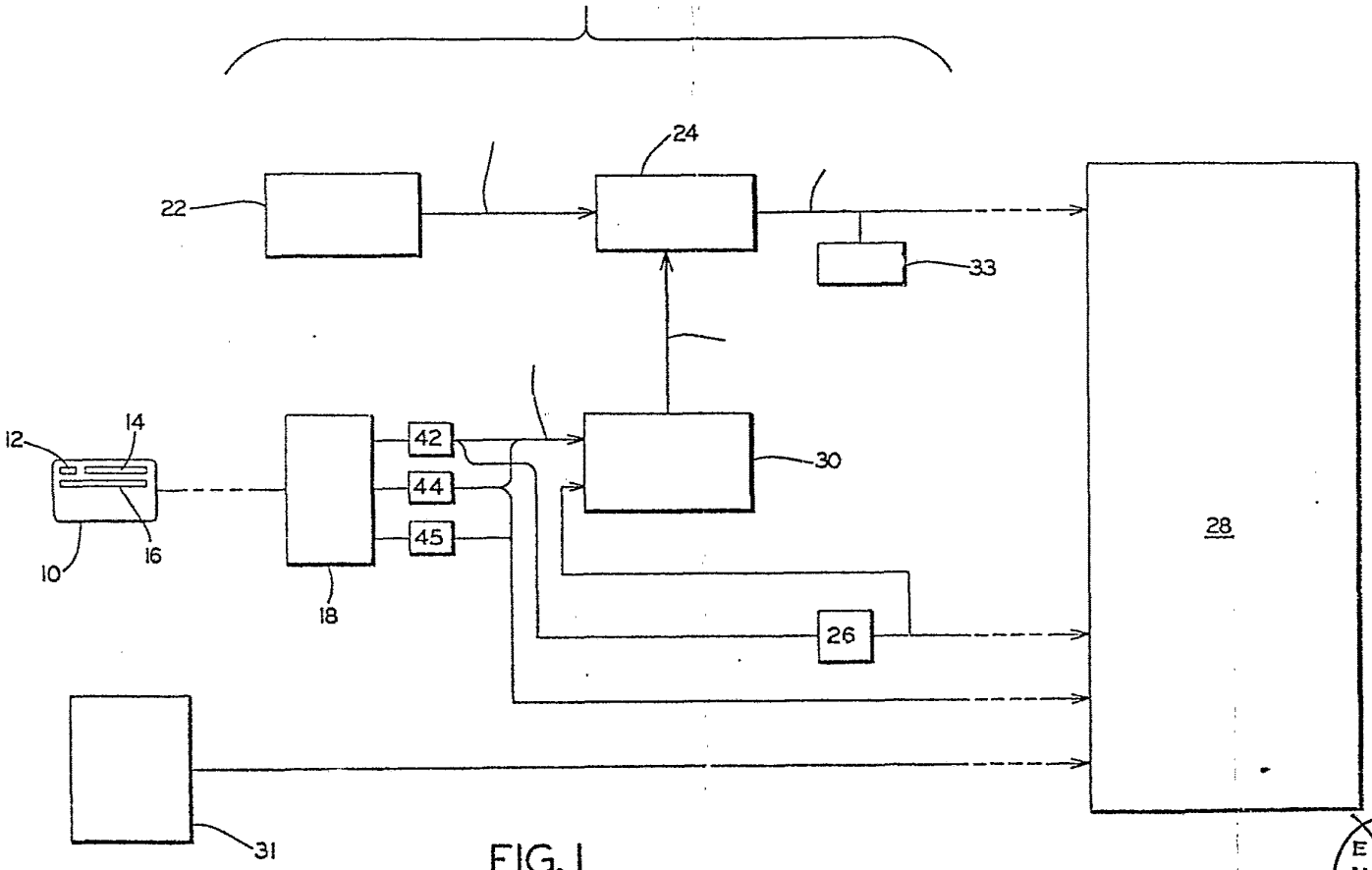


FIG. 1

DIEBOLD, INCORPORATED

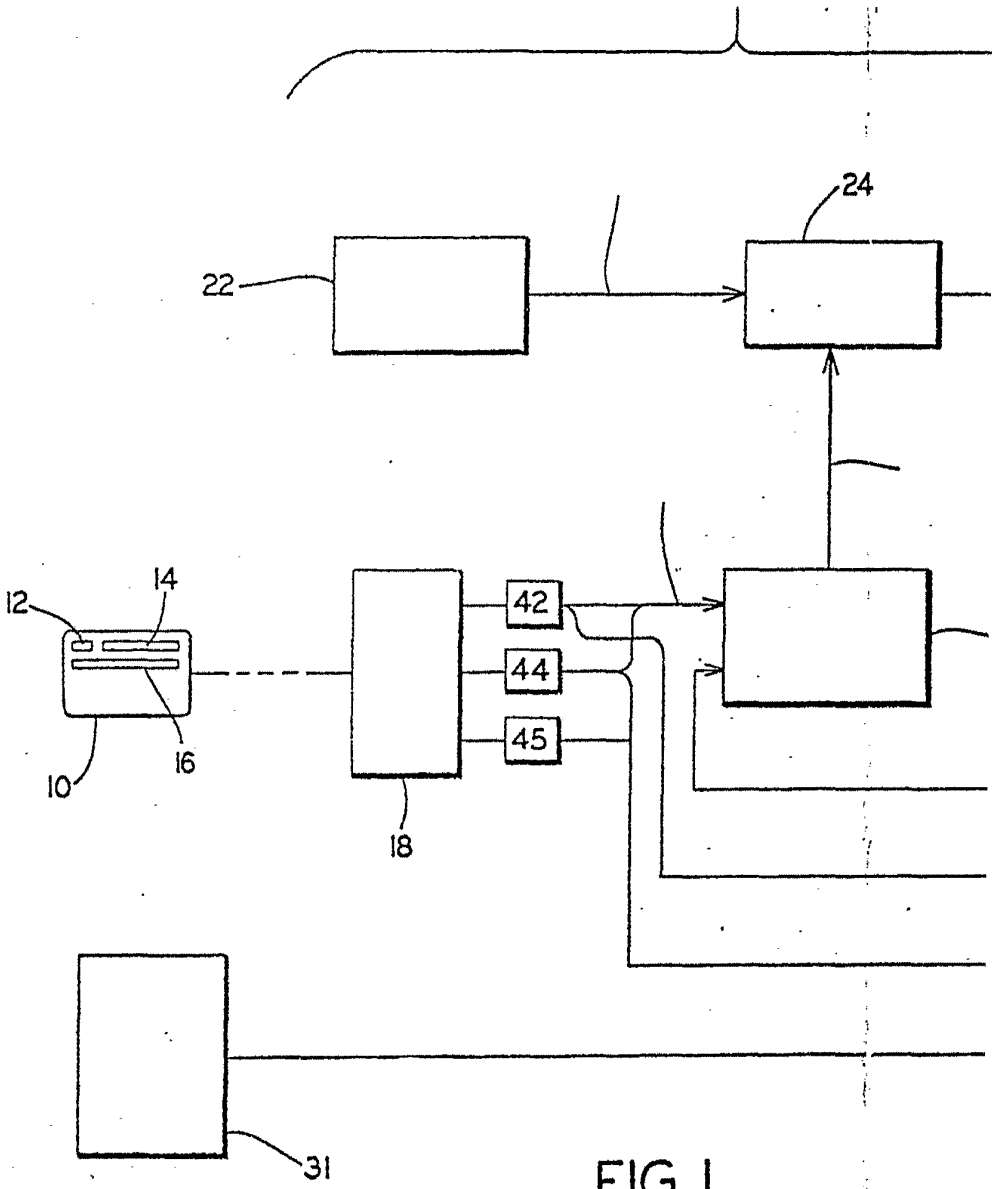
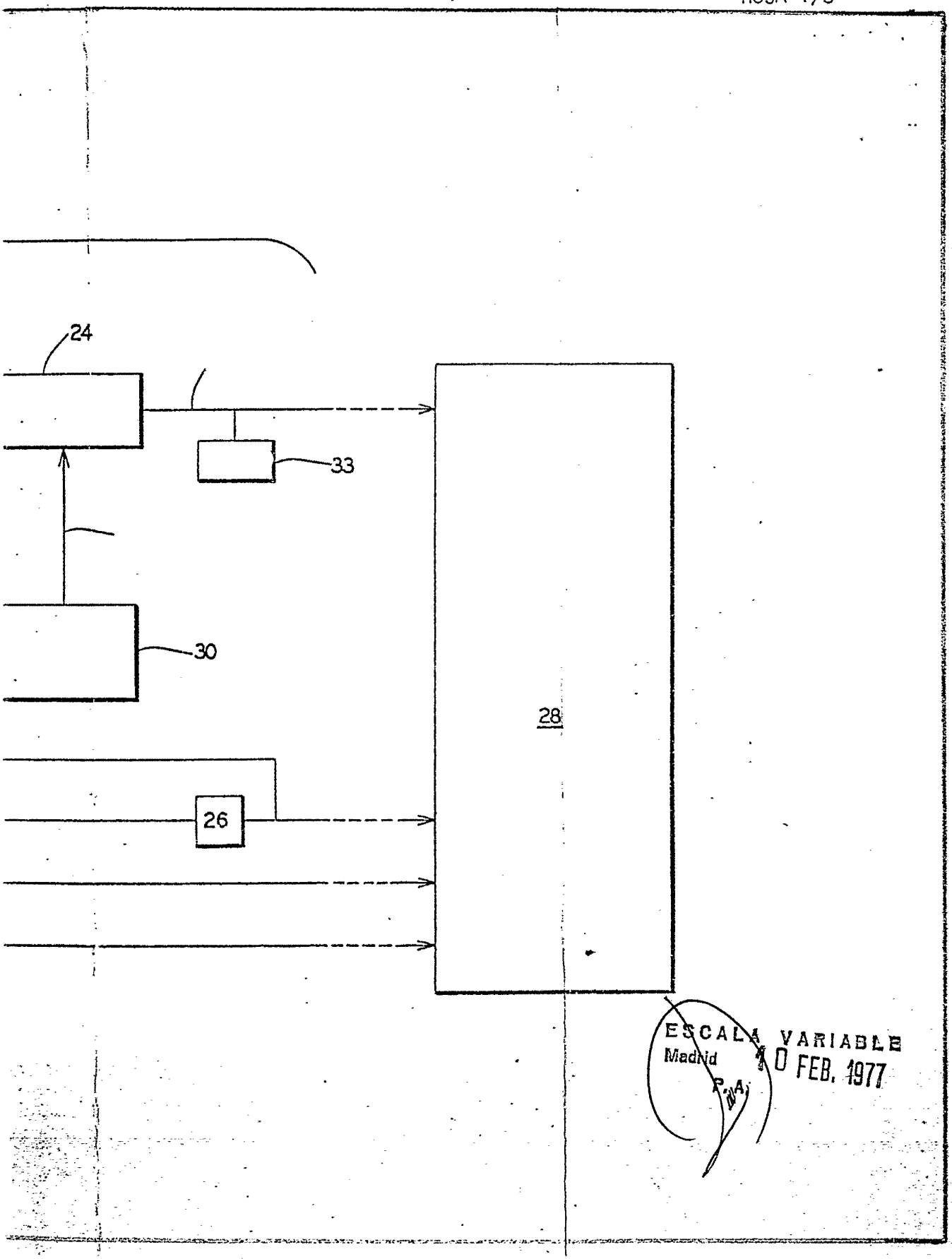


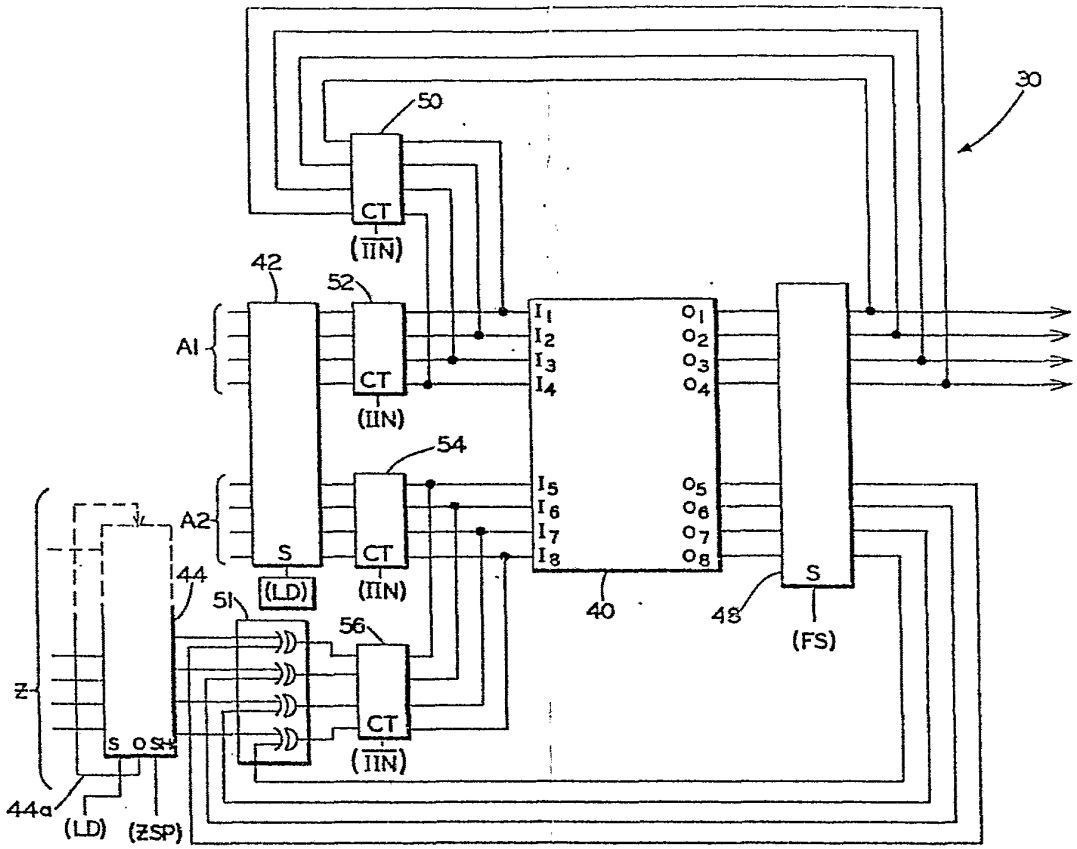
FIG. 1



ESCALA VARIABLE

Madrid 10 FEB. 1977

P.N.A.



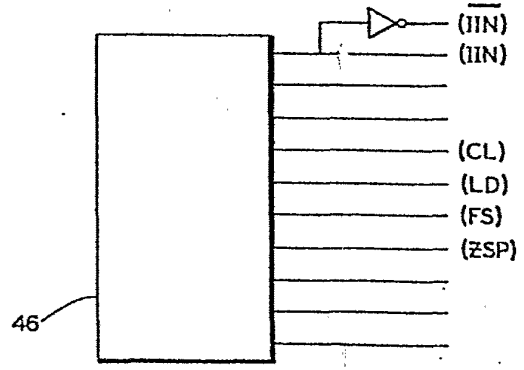
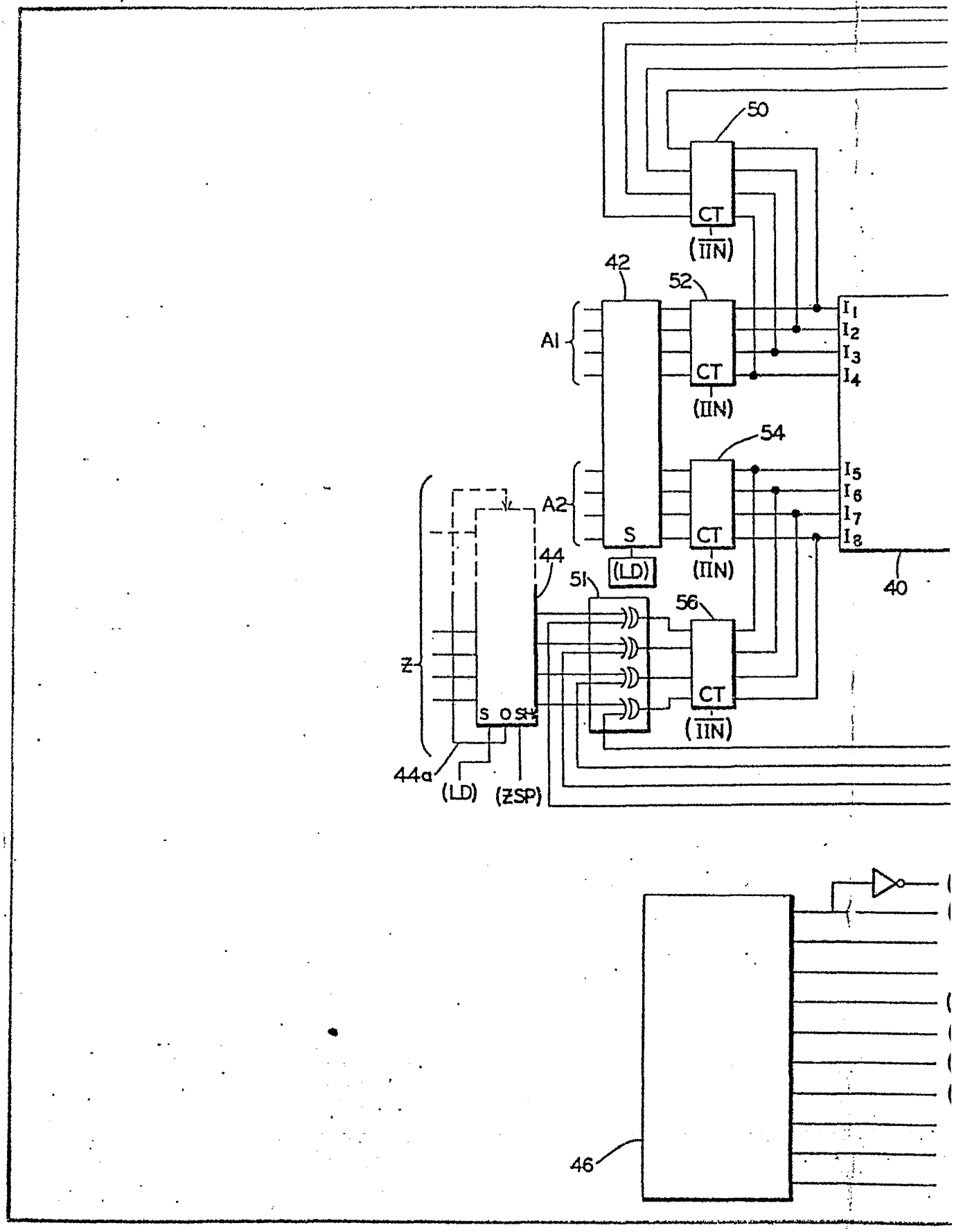
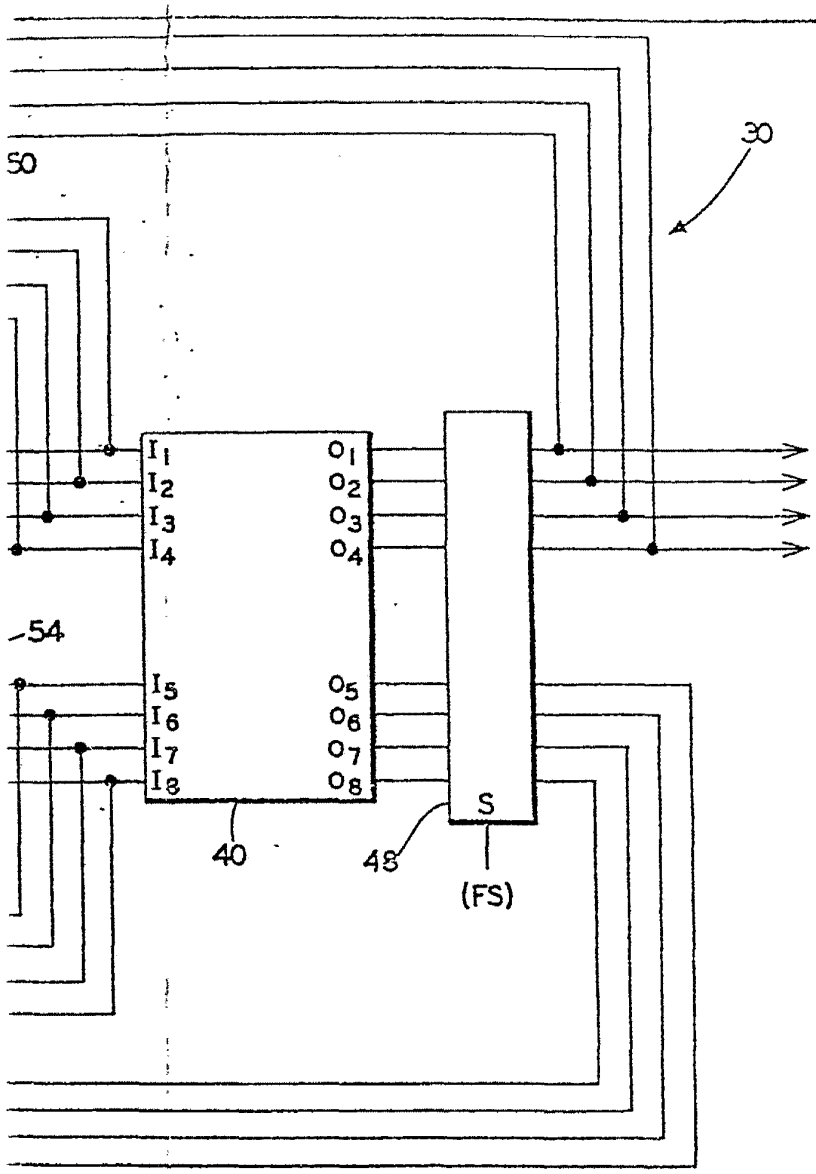


FIG.2

DIEBOLD, INCORPORATED





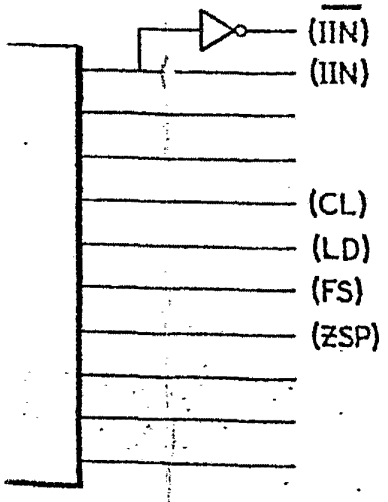


FIG.2

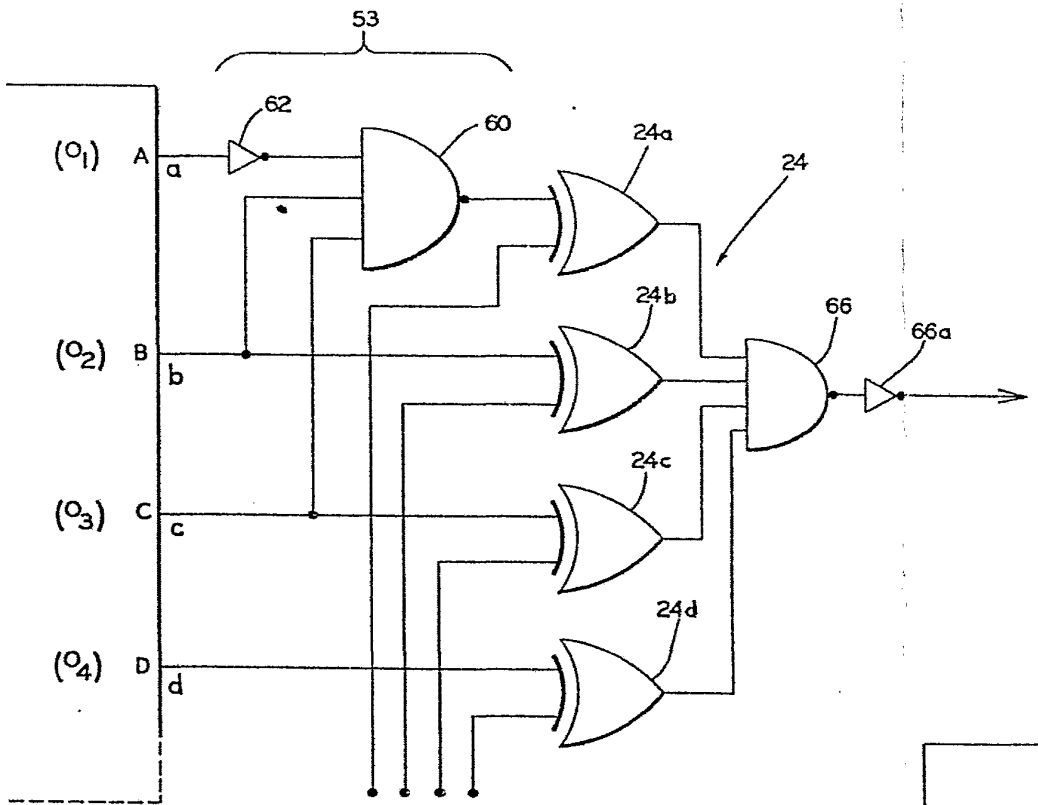


FIG.3

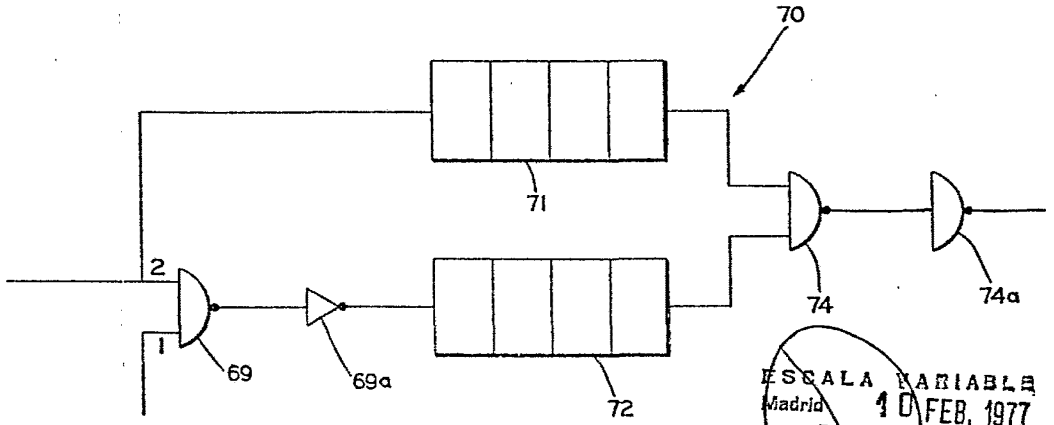


FIG. 4

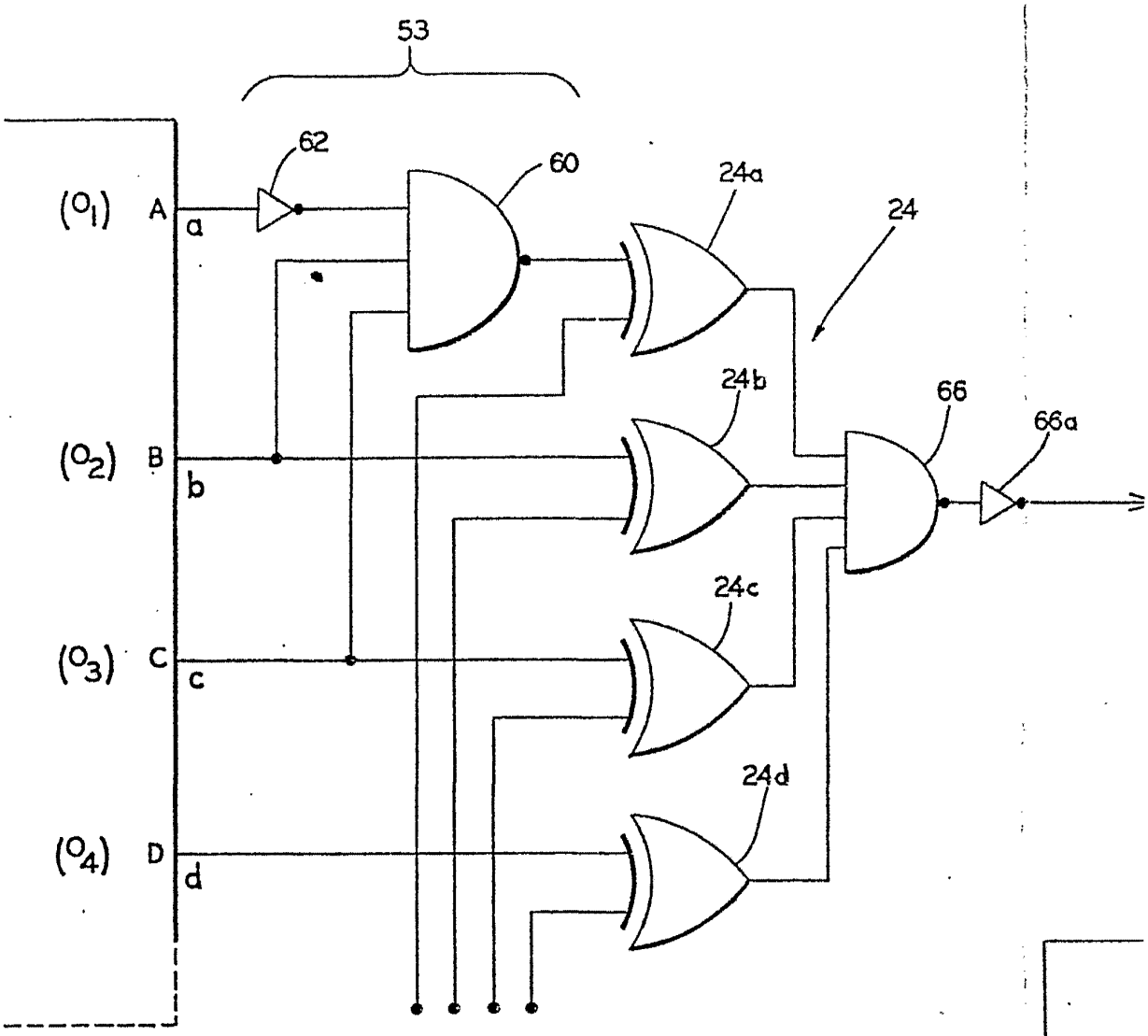
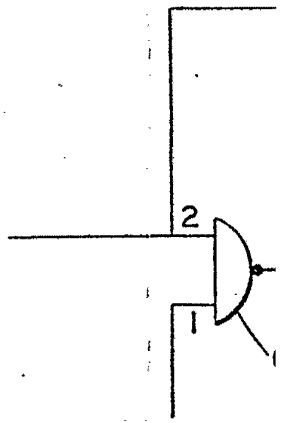
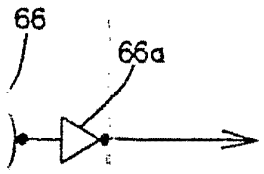


FIG.3





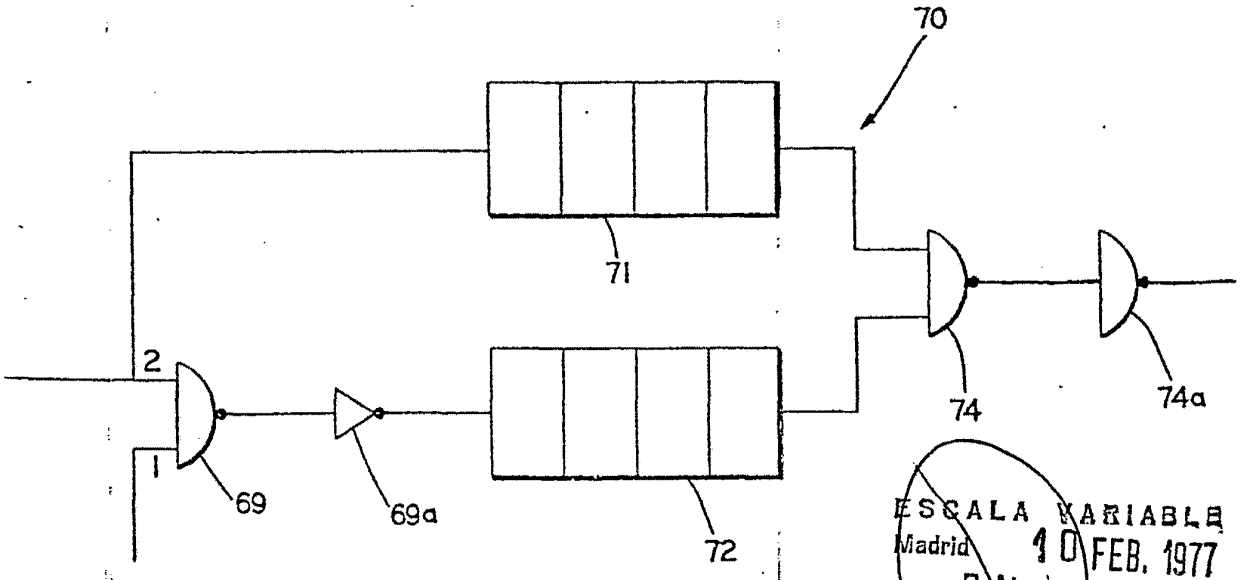


FIG. 4

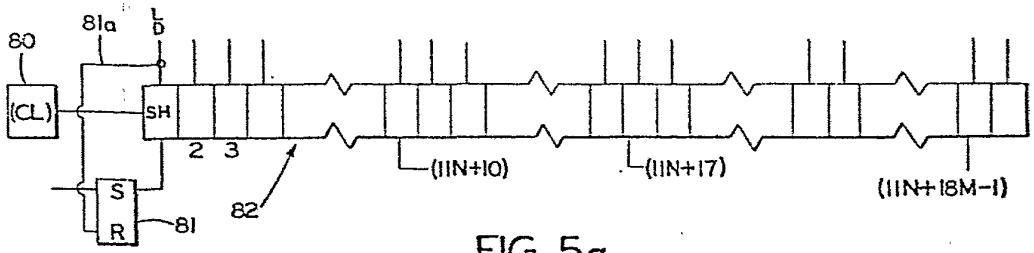


FIG. 5a

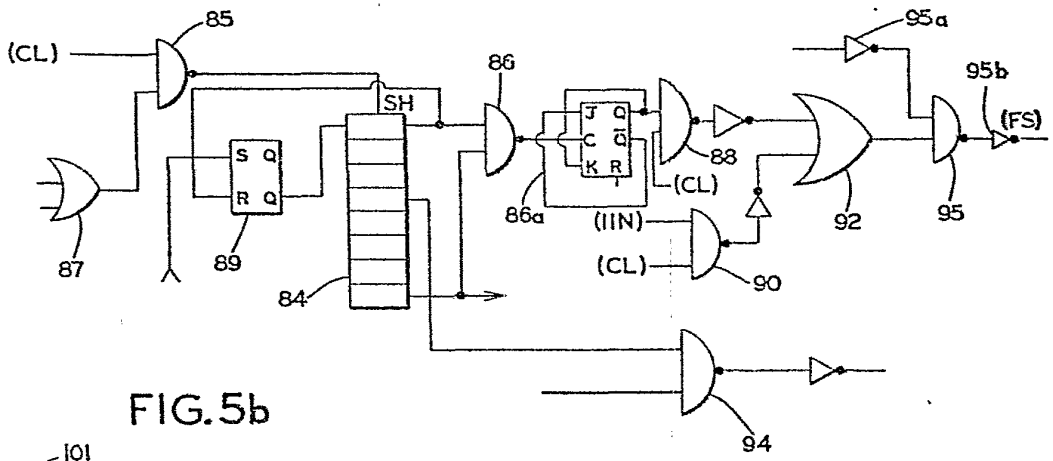


FIG. 5b

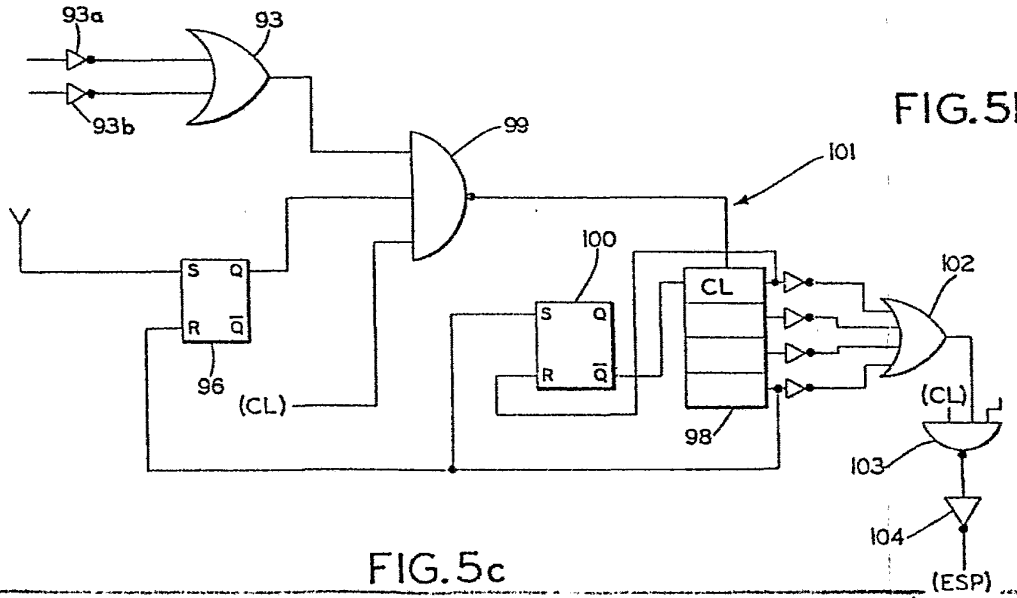
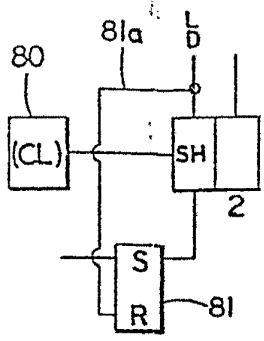


FIG. 5c


81a
L
D
80
(CL)
SH
2
S
R
81

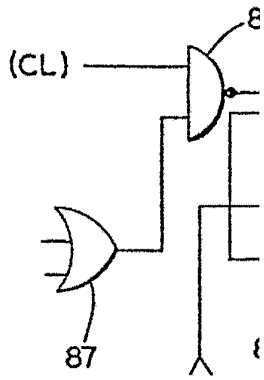

(CL)
87

FIG.

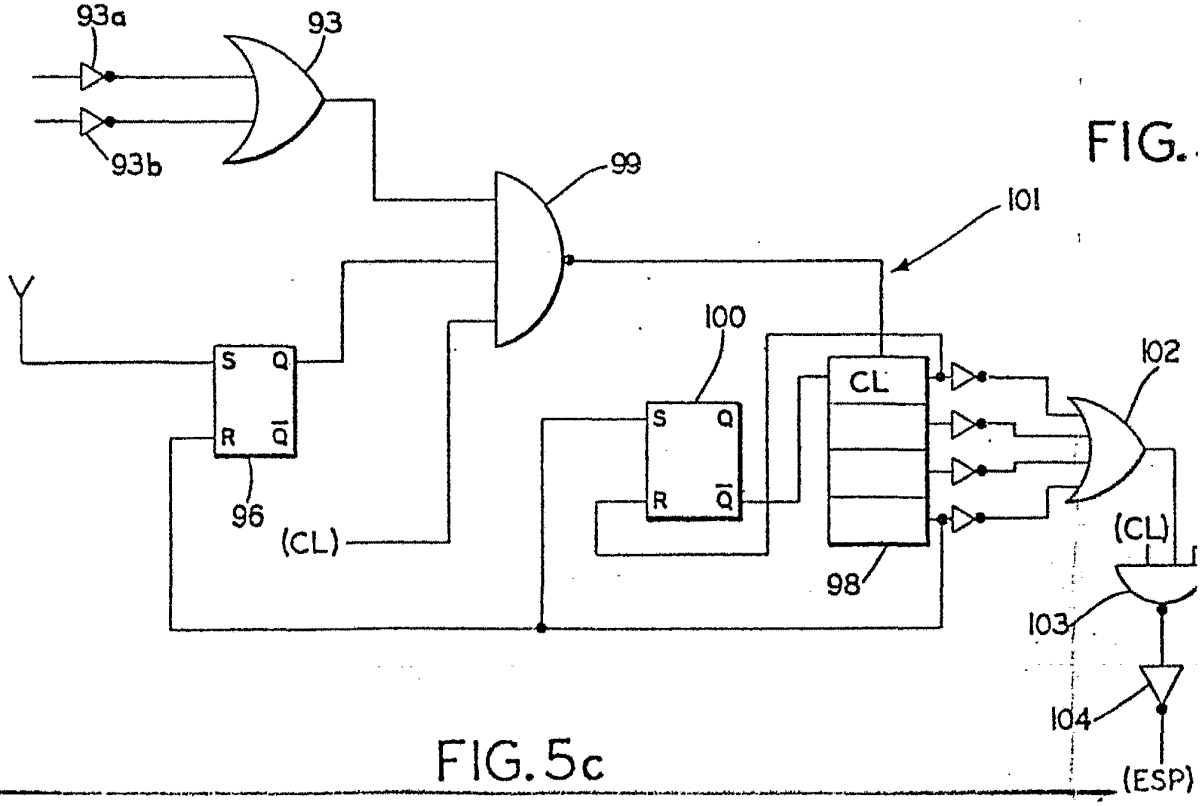

93a
93
93b
99
101
100
102
S
Q
R
Q̄
96
(CL)
CL
98
(CL)
103
104
(ESP)

FIG. 5c

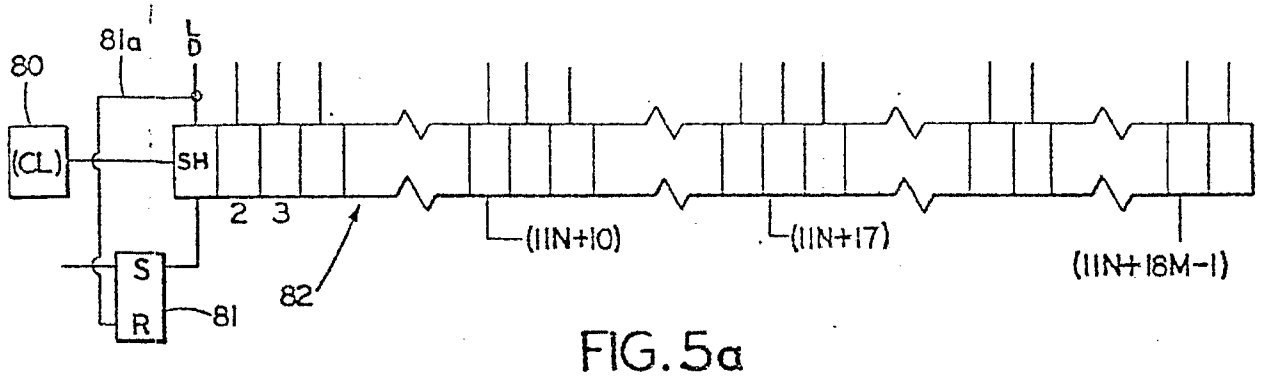


FIG. 5a

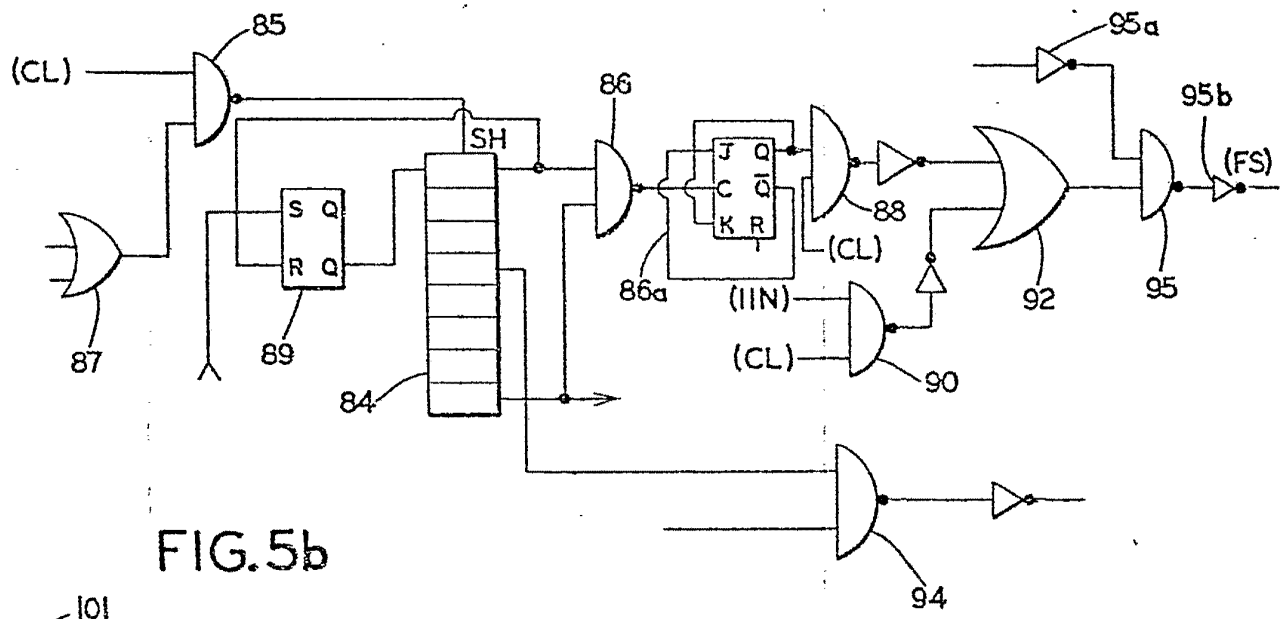
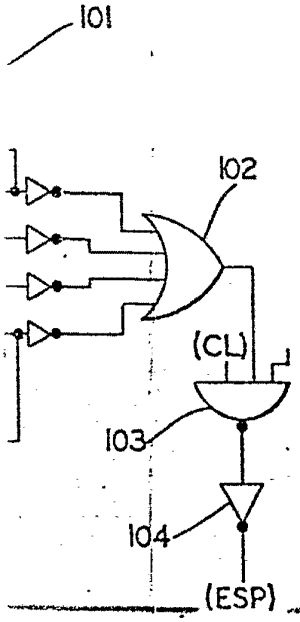


FIG. 5b



ESCALA VARIABLE
Madrid 10 FEB. 1977
F. A.

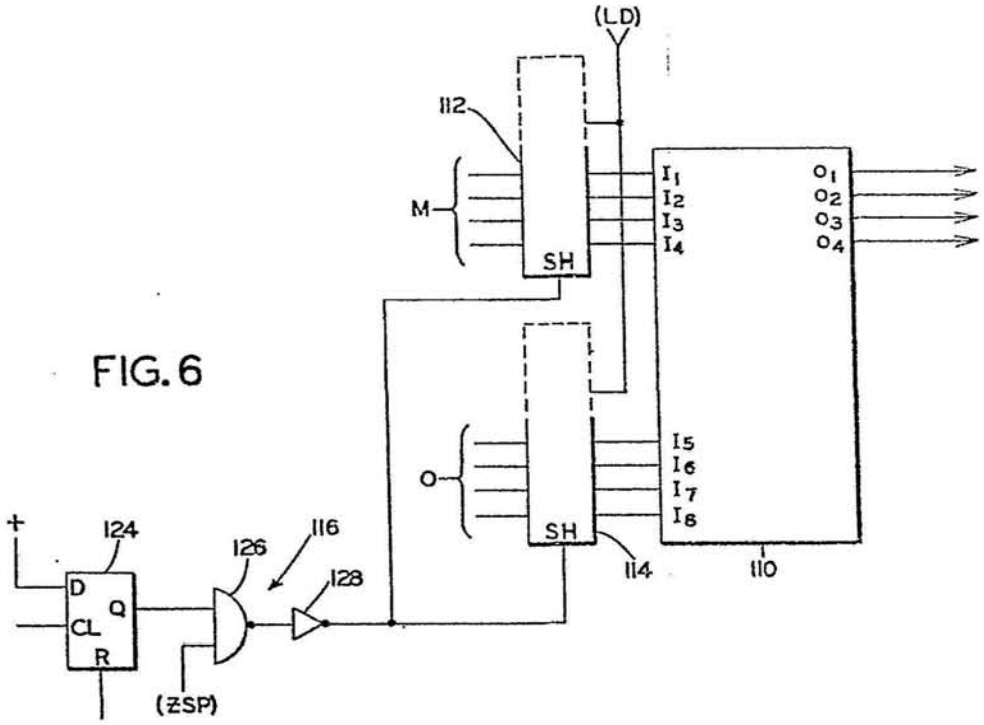


FIG. 6

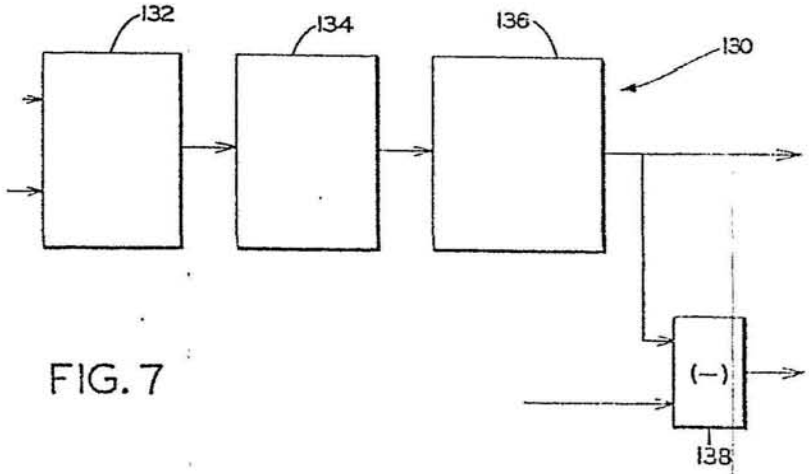


FIG. 7

ESCALA VARIABLE

10 FEB. 1977

Madrid
P. A.

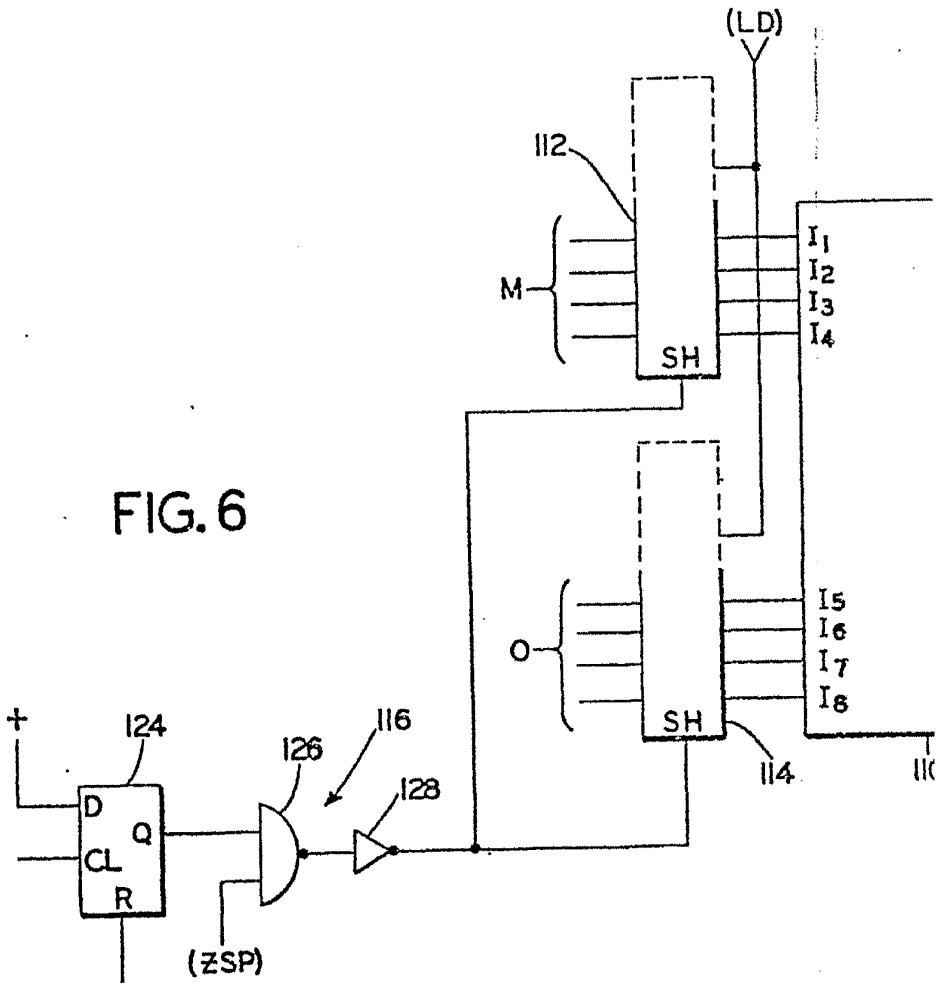

(LD)
112
M
SH
I1
I2
I3
I4
O
SH
I5
I6
I7
I8
114
+
124
D
Q
CL
R
126
116
128
(ZSP)

FIG. 6

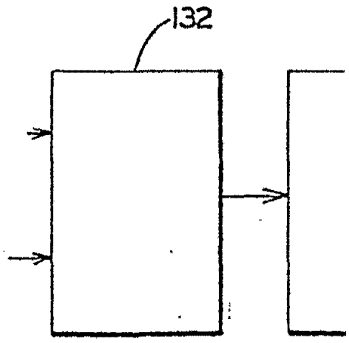
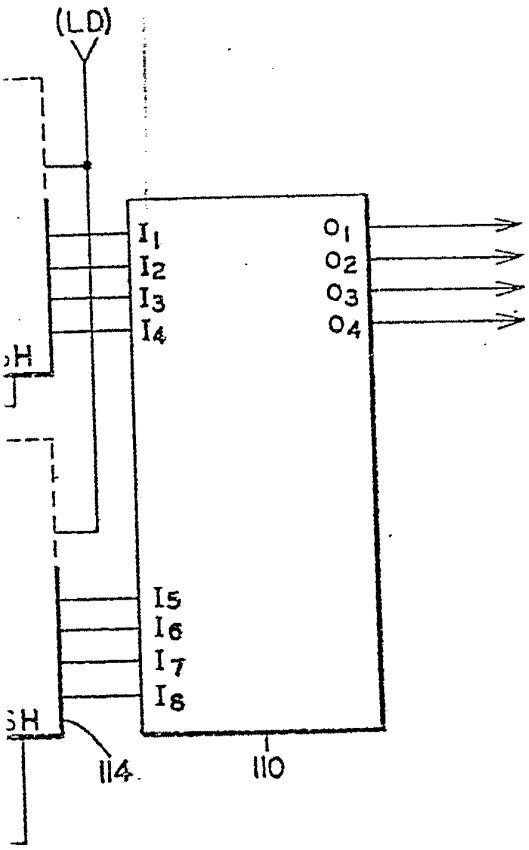

132

FIG. 7



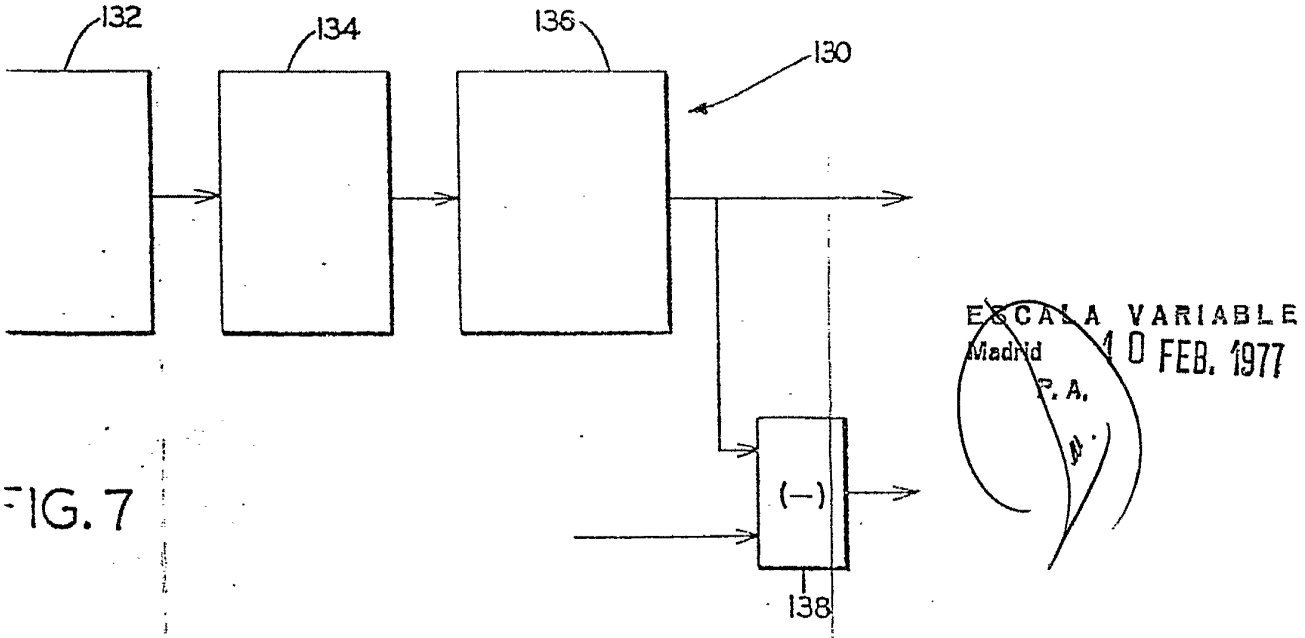


FIG. 7