(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 464 273**

(51) Int. CI.:

G06F 21/46 (2013.01)
G06Q 20/40 (2012.01)
G06Q 20/38 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.08.2006 E 06793036 (2)**

(97) Fecha y número de publicación de la concesión europea: **05.03.2014 EP 1907970**

(54) Título: **Método para generar una pluralidad de números protegidos únicos y tarjeta que incluye un número tal**

(30) Prioridad:

31.08.2005 EP 05107984

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.06.2014

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
ROUTE DE GENÈVE 22-24
1033 CHESEAUX-SUR-LAUSANNE, CH

(72) Inventor/es:

SASSELLI, MARCO

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método para generar una pluralidad de números protegidos únicos y tarjeta que incluye un número tal

CAMPO TÉCNICO

[0001] La presente invención se refiere a un método para generar una pluralidad de números protegidos únicos, estos números están por ejemplo impresos en un soporte físico y permiten, después de la verificación de su autenticidad, acceder a los derechos u obtener un crédito particularmente. La invención se refiere igualmente a un soporte físico que recibe un número tal.

ANTECEDENTES DE LA INVENCIÓN

[0002] Existen actualmente numerosas maneras de obtener un crédito o un derecho para una aplicación particular. Entre estas, se pueden citar las "tarjetas para rascar" que comportan un número impreso, oculto por una tinta opaca. Cuando el usuario compra la tarjeta, retira la tinta opaca de manera que hace aparecer el número impreso. Envía a continuación este número, por ejemplo en forma de SMS (Servicio de Mensajes Cortos) a través de un teléfono móvil a un centro de gestión. Este verifica la validez del número recibido. En caso de validez, el derecho asociado a este número o el crédito es atribuido.

[0003] Es evidente que la atribución de los derechos o del crédito no debería ser hecha más que si el número enviado es válido, lo que significa que no se necesita que mandando un número al azar, se pueda obtener el crédito o el derecho deseado.

[0004] Por esto, los números protegidos actuales están compuestos por una parte por un número de identificación y por otra parte por un valor de control. El número de identificación puede ser un número aleatorio y representar la primera parte del número protegido.

[0005] El valor de control es un número que depende del número de identificación. Más precisamente, este valor de control se puede calcular a partir del número de identificación, de una información oculta tal como una clave y de una regla de cálculo. Este valor de control representa la segunda parte del número de identificación.

[0006] Cuando un usuario envía un número completo al centro de gestión, el número de identificación se extrae del número completo recibido. El valor de control se calcula a partir de este número de identificación. Este valor de control calculado se compara con el valor de control recibido. El derecho o el crédito se otorga únicamente si estos dos valores de control se corresponden.

[0007] La longitud total del número protegido está habitualmente fijada por el proveedor de servicios. Esta longitud es idéntica para todos los números protegidos de un operador dado. Ella no debe ser demasiado grande para evitar que el usuario deba enviar una sucesión de cifras demasiado importante. Ella no debe tampoco ser demasiado pequeña por una parte para no limitar demasiado fuertemente el número de números posibles y por otra parte para garantizar un nivel de seguridad suficiente.

[0008] En los números protegidos actuales, se separa la longitud del número protegido en dos "campos" de longitud fija. Uno de los campos, por ejemplo el que incluye las cifras de pesos fuertes representa el número de identificación (IN) y el otro campo, que contiene las cifras de peso débiles, representa el valor de control (VC).

[0009] Es evidente que cuanto más pequeño es el número de cifras del número de identificación (IN), más débil es el número de números de identificación que es posible generar. Por el contrario, la seguridad será más grande.

[0010] Inversamente, cuanto más grande es el campo que contiene el número de identificación (IN), más se aumenta el número de números de identificación posibles. Al mismo tiempo, se disminuye la seguridad.

[0011] Uno de los problemas consiste en hallar un buen equilibrio entre estas dos restricciones contradictorias.

[0012] Los soportes físicos tales como las "tarjetas de rascar" que comportan un número tal tienen habitualmente un periodo de validez limitado, pero que puede ser relativamente largo, por ejemplo dos años. Como estos números tienen una longitud limitada, es necesario asegurar que será posible, durante todo el periodo de validez de las tarjetas, generar números protegidos diferentes. Por esto, es por lo tanto necesario prever que la parte que forma el número de identificación sea suficientemente grande. Si esta parte es demasiado corta, ya no será posible después un cierto tiempo de utilización del sistema es decir después la creación de un cierto número de números protegidos, generar nuevos números. Se habrán agotado todas las posibilidades que ofrece el tamaño del número de identificación. Es por lo tanto necesario, desde el inicio,

prever una ubicación suficientemente grande para generar suficientes números de identificación distintos durante el periodo de validez de una tarjeta. Esto se hace en detrimento de la seguridad. De hecho, como la longitud total del número protegido es limitada, cuanto más grande sea la ubicación tomada para los números de identificación, más débil es la que queda para el valor de control.

DESCRIPCIÓN DE LA INVENCIÓN

[0013] La invención se refiere a un método según la reivindicación 1, un soporte físico según la reivindicación 6 y un conjunto de soportes físicos según la reivindicación 8.

[0014] La presente invención se propone proporcionar un procedimiento que permite generar números protegidos válidos durante una duración dada, estos números protegidos tienen un nivel de seguridad óptimo, conservando la posibilidad de crear números suplementarios o de aumentar el nivel de seguridad en función de las necesidades.

[0015] El método de la invención permite por lo tanto generar tantos números protegidos como sea necesario, teniendo un nivel de seguridad máxima, lo que disminuye tanto los riesgos de que el envío de un número al azar permita la atribución de derechos o de un crédito. Los parámetros contradictorios de cantidad de números generados y de seguridad se pueden corregir en cualquier momento.

[0016] Las metas de la invención se alcanzan por un método para generar una pluralidad de números protegidos (SN) únicos teniendo una longitud fija predeterminada, los números protegidos están formados al menos por un número de identificación (IN) y por un valor de control (VC), este método comporta las etapas de:

Determinación de una primera cantidad de números protegidos que se deben generar;

Determinación del número mínimo de cifras necesarias para generar dicha primera cantidad de números protegidos;

Generación de una primera serie de números de identificación (IN) únicos, estos números de identificación tienen una longitud al menos igual al número mínimo de cifras necesarias para generar los números protegidos (SN), estos números de identificación son seleccionados entre todos los números posibles que tienen la longitud requerida;

Asociación de un valor de control (VC) a cada número de identificación (IN), este valor de control tiene una longitud tal que la longitud total de los números protegidos corresponda a dicha longitud fija predeterminada;

Antes de la utilización de todos los números de identificación disponibles de la primera serie de números de identificación, determinación de una segunda cantidad adicional de números protegidos que se debe generar;

Cálculo del número de números de identificación restante que es posible generar a partir del número de cifras que forma los números de identificación de dicha primera serie;

Si la segunda cantidad de números de identificación que se debe generar es superior a dicho número de números de identificación restante, determinación del nuevo número mínimo de cifras necesarias para generar dicha segunda cantidad de números de identificación;

Determinación de por lo menos un número de identificación no utilizado entre los números de identificación que es posible generar utilizando el número de cifras de la primera cantidad de números de identificación;

Generación de una segunda serie de números de identificación (IN) únicos, estos números de identificación se forman a partir de números de identificación no utilizados entre los números de identificación que es posible generar utilizando el número de cifras de la primera cantidad de números de identificación, estos números de identificación de la segunda serie de números tiene una longitud al menos igual al nuevo número mínimo de cifras necesarias para generar dichos números de identificación (IN) de esta segunda serie de números.

[0017] En el campo de la invención, los números protegidos generados son válidos para un tiempo limitado, por ejemplo dos años. Los números que han sido generados, pero que no han sido utilizados durante este tiempo limitado ya no son válidos. Es evidente que todos los números protegidos no se generan a la vez. Al contrario, ellos se generan por lotes, por ejemplo todos los meses. Es por lo tanto posible que al inicio de la puesta en práctica de un servicio que utiliza tales números protegidos, la cantidad de números que se debe generar en el curso de los primeros meses sea inferior a la cantidad de números que se debe generar después de un largo periodo de utilización. El procedimiento de la invención permite entonces adaptar la cantidad de números de seguridad generados y el nivel de seguridad durante cada intervalo temporal.

[0018] Además, este procedimiento se basa en una estimación de la cantidad de números protegidos que se debe generar en el curso de un intervalo temporal. Si esta estimación es errónea, bien sea en un sentido optimista o pesimista, es posible corregir la cantidad de números protegidos y el nivel de seguridad durante un intervalo temporal.

[0019] Para realizar esto, se determina el periodo de validez de los números protegidos. Esta duración está habitualmente impuesta por el proveedor de "soportes físicos" que comporta estos números protegidos. Se elige a continuación un periodo temporal que es como máximo igual al periodo de validez, pero que es habitualmente una fracción de este periodo de validez. Se estima a continuación la cantidad de números protegidos diferentes que se necesitará generar durante este periodo temporal. Se determina a continuación la magnitud del campo que representa el número de identificación en función de la cantidad de números protegidos estimada. Así, este campo tiene una longitud variable en función de la estimación que ha sido hecha. Las cifras restantes se utilizan para representar el valor de control.

[0020] Si la magnitud del campo reservado para generar los números de identificación no es suficiente en el curso de una unidad temporal, se puede desplazar la frontera durante la unidad temporal hacia la derecha, de manera que se añadan los números posibles. Si al contrario, las previsiones eran demasiado optimistas y la magnitud del campo para los números de identificación era demasiado grande, es posible desplazar la frontera hacia la izquierda, lo que mejora la seguridad.

[0021] Estos desplazamientos de frontera pueden hacerse en el curso de una unidad temporal o al final de una unidad tal, para la unidad temporal siguiente.

[0022] La utilización de tal número de seguridad está por supuesto sometida a una verificación que permita determinar si el valor de control mandado se corresponde bien con el número de identificación recibido. El método según la invención permite una verificación óptima y permite particularmente detectar un intento de ataque sistemático a partir de un número de identificación dado.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0023] La presente invención y sus ventajas serán mejor comprendidas en referencia a las figuras anexadas y a la descripción detallada de una forma de realización particular, en las cuales:

- la figura 1A representa la estructura de un primer número protegido generado según el método de la invención;

- la figura 1B representa la estructura de un segundo número protegido generado según el método de la invención;

- la figura 2A representa un cuadro en forma de valores decimales, de números protegidos generados según la presente invención;

- la figura 2B es una variante del cuadro de la figura 2A;

- la figura 3A representa un cuadro con los números protegidos generados según el método de la invención;

- la figura 3B es una variante del cuadro de la figura 2A

- la figura 3C es una otra variante del cuadro de la figura 2A;

- la figura 4 es un esquema funcional que representa la verificación de un número protegido generado conforme a la presente invención.

MANERA(S) DE REALIZAR LA INVENCIÓN

[0024] En la práctica, es evidente que el número de números protegidos diferentes que debe ser posible generar debe ser relativamente grande para responder a la totalidad de la demanda.

[0025] Sin embargo, en la descripción del principio de la invención, se utilizarán valores suficientemente débiles para poder manipularlos fácilmente.

[0026] Según la presente invención, y como en el estado de la técnica anterior, el número protegido (SN) incluye por una parte un número de identificación (IN) y por otra parte un valor de control (VC) que depende de este número de identificación. Este número protegido está habitualmente inscrito en un soporte físico tal como una tarjeta del tipo "tarjeta para rascar" o un recibo de pago por ejemplo. Podría igualmente aparecer en una pantalla como una pantalla de ordenador o de televisión. En la continuación de la descripción, se supone que el soporte es una tarjeta. En todos los casos, el principio

de funcionamiento es el mismo.

[0027] Según un ejemplo de realización concreto, el número inscrito sobre el soporte, es decir el número protegido SN es un número decimal que puede por ejemplo contener 16 cifras, este número de cifras es definido por el operador. Para el tratamiento de este número en un centro de gestión o de verificación, se convierte en un número binario.

[0028] Como se puede calcular, un número decimal de 16 cifras se puede representar en forma binaria mediante 53 cifras binarias o 53 bits, por el hecho de que 2^{53} es un número de 16 cifras mientras que 2^{54} incluye 17 cifras. Este valor de 53 bits es por lo tanto la longitud total del número de identificación IN y del valor de control VC.

[0029] El método de la presente invención funciona de la siguiente manera. Se determina en primer lugar un periodo de validez máxima de una tarjeta. Esta duración, que en la continuación de la descripción se fija a dos años, es habitualmente impuesta por el operador.

[0030] Se divide a continuación esta duración máxima en intervalos temporales más cortos, de tal manera que el número de intervalos sea "razonable" y que la cantidad de números protegidos que se debe generar en el curso de un intervalo temporal sea suficientemente importante. Como ejemplo, para una duración máxima de 2 años, un intervalo temporal de un mes es un valor correcto.

[0031] A partir de la duración máxima y del intervalo elegido, se determina el número de cifras del que hay que disponer para representar todos los intervalos. Más concretamente, para unos intervalos de un mes durante un periodo de 2 años, habrá 24 meses. En modo decimal, se necesitarán dos cifras para representar cada uno de los 24 meses. En modo binario, se necesitarán 5 cifras binarias o 5 bits para representar los 24 meses, puesto que 2^4 es igual a 16 que es inferior a 24 y por lo tanto no suficiente cuando $2^5 = 32$ es suficiente para representar 24 valores diferentes.

[0032] Según la invención, el número de identificación IN se separa en un valor que representa el intervalo temporal VIT y una parte digital de identificación INP. La duración del intervalo temporal VIT es en principio fija. Ella se incrementa habitualmente de 1 en cada cambio de periodo temporal. Así, para un mes y un año dados, por ejemplo agosto, ella valdrá 00000, luego 00001 en septiembre siguiente y así sucesivamente hasta 11111. A continuación, el ciclo recomienza. Dado que el periodo de validez máximo ha transcurrido antes de que el ciclo recomience, no puede haber dos tarjetas válidas idénticas.

[0033] La longitud total del número protegido menos la longitud reservada para el intervalo temporal está por lo tanto disponible para la parte digital y el valor de control.

[0034] La etapa siguiente del procedimiento consiste en evaluar la cantidad de números protegidos diferentes que será necesario generar en el curso del próximo intervalo temporal. Esta valoración puede hacerse habitualmente según las indicaciones dadas por el operador. Como se explica en detalle más abajo, una de las ventajas del método de la invención es permitir una corrección sencilla de la cantidad de números protegidos generada en el curso de un intervalo temporal. Así, en particular al inicio de la puesta en funcionamiento del sistema, si las evaluaciones son demasiado optimistas o al contrario demasiado pesimistas, es posible efectuar las modificaciones en el curso de un intervalo temporal.

[0035] Cuando se ha evaluado la cantidad de números protegidos que se debe generar durante el intervalo temporal concernido, se determina a continuación la longitud mínima necesaria para generar esta cantidad de números. Como ejemplo, si se evalúa el número de números protegidos que se debe generar durante un mes determinado a 100 000, serán necesarios 17 bits. De hecho, 16 bits son insuficientes puesto que $2^{16} = 65\,536$ es inferior a la cantidad evaluada cuando $2^{17} = 131\,072$ es superior a la cantidad evaluada.

[0036] Se elegirá a continuación, entre los números protegidos posibles, es decir en el ejemplo considerado, entre 131 072 números, un cierto número de números diferentes, hasta alcanzar la cantidad deseada, a saber 100 000 en nuestro ejemplo.

[0037] La longitud total del número protegido SN menos la longitud utilizada por el intervalo temporal VIT menos aquella utilizada para la parte digital INP nos da la longitud total utilizable para el valor de control. Retomando el ejemplo concreto descrito arriba, para 53 bits de número protegido, hay 5 bits para el intervalo temporal, 17 bits para la parte digital, lo que corresponde a un total de 22 bits para el número de identificación. El valor de control VC tiene por lo tanto una longitud de 53-22=31 bits.

[0038] Este valor de control depende del número de identificación. Según una manera de generar este valor de control, se toma el número de identificación, al cual se agrega eventualmente informaciones, luego se aplica una operación al conjunto. Tal operación podría por ejemplo ser una función de comprobación aleatoria con clave o cualquier otra función en la cual sea necesario conocer una información oculta para calcular el valor de control a partir del número de identificación.

MODIFICACIÓN DE LA CANTIDAD DE NÚMEROS PROTEGIDOS DISPONIBLES

[0039] La continuación de la descripción se basa en las figuras 2 y 3 y se refiere al funcionamiento del método cuando se debe generar una cantidad de números protegidos diferentes de el que ha sido inicialmente evaluado.

[0040] Las figuras 2A y 2B describen un ejemplo en el cual el identificador del intervalo temporal se omite por razones de claridad y el número protegido incluye 4 cifras decimales.

[0041] En primer lugar, se ha estimado que será necesario generar como máximo 100 números protegidos. Para esto, dos cifras decimales bastan. Los dos primeras columnas IN1 e IN2 de la figura 2A contienen los valores posibles para generar 100 números diferentes, es decir los valores de 00 a 99. El valor de control incluye igualmente 2 cifras de manera que se respete una longitud total de 4 cifras. Este valor de control se indica en las columnas anotadas como VC1 y VC2 de la figura 2A. En el ejemplo elegido, la columna VC1 contiene el valor absoluto de la diferencia entre las dos cifras que componen el número de identificación y la columna VC2 contiene su suma módulo 10.

[0042] El número protegido SN está formado por la concatenación de las 4 cifras indicadas en las columnas IN1, IN2, VC1 y VC2.

[0043] Como se indica anteriormente, tomando dos cifras decimales, es posible generar 100 números protegidos diferentes. Si durante el intervalo temporal, resulta que la cantidad estimada de números protegidos es insuficiente, es posible añadir, lo que se ilustra por la figura 2B.

[0044] En esta figura, el número de identificación ya no está formado por 2 cifras, sino por tres, anotadas como IN1, IN2 y IN3 en la figura. Por eso resulta que a partir de una línea del cuadro de la figura 2A, que representa un número protegido, es posible generar 10 líneas en el cuadro de la figura 2B, que representa diez números protegidos.

[0045] En tal caso, el valor de control no incluye más que una cifra, aquí la suma módulo 10 de las cifras que forma el número de identificación, de manera que conserve la longitud total de 4 cifras.

[0046] Las figuras 3A, 3B y 3C ilustran un ejemplo similar, en el cual el número inscrito sobre la tarjeta es decimal, pero los valores utilizados para el tratamiento y la generación de estos números es binaria, lo que es habitualmente el caso en la práctica.

[0047] En el ejemplo de la figura 3A, se supone que la longitud total del número protegido es de 9 bits y que la longitud del número de identificación es de 4 bits. Eso permite generar 16 números protegidos diferentes, anotados de 1 a 16 en la columna izquierda de la figura.

[0048] Imaginemos que a partir de que el 11.º número protegido es generado, se constata que 16 posibilidades no son suficientes, se podrá, tal y como se ilustra por el cuadro de la figura 3B, utilizar un bit suplementario para generar el número de identificación. Así, el 12.º número de identificación, que es 1011 sobre la figura 3A, se puede escindir en 10110 y 10111. Pasará lo mismo para los números siguentes. Así, cada número protegido de la figura 3A puede dar lugar a 2 números protegidos como se indica en la figura 3b.

[0049] Por el contrario, en lugar de 5 bits disponibles para el valor de control en la figura 3A, ya no quedan más que 4 en la figura 3B. La seguridad se encuentra por lo tanto debilitada.

[0050] Si al contrario, se constata que la cantidad de números disponibles es demasiado grande, es posible, tal y como se ilustra por la figura 3C, disminuir esta cantidad sin utilizar más que tres bits para generar el número de identificación. Así, los números 13 y 14 de la figura 3A, es decir 1100 y 1101 no forman más que una sola posibilidad en la figura 3C, a saber 110. Por el contrario, el valor de control se codifica sobre 6 bits, lo que mejora la seguridad.

[0051] Esta flexibilidad en la modificación de los números de cifras binarias o decimales utilizados para formar el número de identificación y el valor de control ofrece dos ventajas. Por una parte, eso permite modificar la cantidad de números protegidos que es posible generar y la seguridad asociada, durante un intervalo temporal, para corregir por ejemplo una estimación errónea. Por otra parte, eso permite adaptar esta cantidad al inicio de cada intervalo temporal, en función particularmente de la evolución de la utilización de los números protegidos.

Verificación de un número protegido enviado

[0052] La descripción que precede se refiere a la manera de generar los números protegidos así como su estructura.

[0053] La continuación de la descripción se refiere preferentemente a la utilización de un número tal protegido, y particularmente la determinación, por un órgano de control, de la autenticidad de un número recibido por parte de un usuario.

[0054] Cuando un usuario envía un número protegido, una verificación en dos etapas está prevista para determinar si este número es auténtico y da derecho a un crédito por ejemplo, o si es falso.

Etapa 1

[0055] En la primera etapa, el número se envía a un centro de gestión. Se debe señalar que este centro no conoce necesariamente la longitud del número de identificación puesto que esta puede variar en el curso de un intervalo temporal. En cambio, a partir del número de identificación IN, puede conocer una zona de valores en la cual se encuentra este número. Como ejemplo, retomando el caso de la figura 3A, imaginemos que entre las 16 posibilidades mencionadas, se han elegido las posibilidades N° 2 a 8 y 11 a 15 para producir los números protegidos instalado en circulación. Las otras posibilidades no han dado lugar a los números protegidos puestos en circulación.

[0056] Para cada número protegido puesto en circulación, se determinará un valor mínimo y un valor máximo asociado a este número. Tomando por ejemplo el número protegido que lleva la referencia 2 en la figura 3A, el número de identificación que corresponde es 0001. El número protegido está formado por 8 bits. El valor mínimo que puede tomar el número protegido que tiene 0001 como cuatro primeros bits de peso fuerte es 00010000, lo que corresponde al número de identificación concatenado con 0, hasta alcanzar la longitud deseada. De manera similar, el valor máximo corresponde al número de identificación concatenada con 1, sea 00011111. Convirtiendo estos números en valores decimales, se tiene un terminal inferior igual a 32 y un terminal superior igual a 63.

[0057] En las figuras 3A, 3B y 3C, los límites inferiores de los intervalos aparecen en la columna anotada como "Min" y los límites superiores en la columna anotada como "Max".

[0058] El centro de gestión no conoce los números protegidos exactos, pero conoce las zonas asociadas a los números protegidos que han sido atribuidos.

[0059] Si un usuario envía el número protegido 284, corresponde al caso 9 de la figura 3A, partiendo de la hipótesis de que este número protegido no haya sido atribuido, el centro de gestión va a verificar si este valor de 284 pertenece a una zona auténtica. Retomando la hipótesis precedente, las zonas de valores atribuidos son 32-255,320-479. El valor 284 no forma parte de ninguna zona atribuida. Él será por lo tanto considerado por el centro de gestión como un valor falso y el derecho o el crédito asociado no será atribuido. El número enviado al no haber pasado esta primera etapa de verificación, no se transmite para experimentar la segunda etapa.

[0060] Si el usuario envía el número protegido correspondiente al caso 12, a saber 370, el centro de gestión podrá determinar que este valor forma parte de las zonas válidas y podrá pasar a la segunda etapa de verificación.

Etapa 2

[0061] En esta segunda etapa, el número protegido se transmite a un centro de verificación. Este contiene por una parte la lista de los números de identificación IN válidos y por otra parte, el valor de control VC asociado. Como se indica anteriormente, este valor de control está formado por el número de identificación al cual se agrega eventualmente informaciones y al cual se aplica una operación. Esta operación puede por ejemplo ser un cifrado, una función de comprobación aleatoria con clave o toda otra operación que no permita fácilmente hallar las informaciones de salida conociendo el valor de control.

[0062] Se debe señalar que el número protegido es habitualmente dado en forma decimal mientras que se trata en forma binaria en el centro de gestión y en el centro de verificación. Antes de las operaciones de control, el valor decimal recibido es por lo tanto habitualmente transformado en valor binario.

[0063] Se debe igualmente notar que el número protegido podría ser inscrito en forma alfanumérica, siempre y cuando los medios de transmisión sean apropiados. En tal caso, este código alfanumérico debería ser convertido a un formato utilizable por el centro de gestión, normalmente en forma binaria.

[0064] A la recepción del número de identificación IN, el centro de verificación agrega las informaciones mencionadas previamente y aplica la función de comprobación aleatoria con clave, con por ejemplo la clave del mes. Compara a continuación el resultado calculado con el resultado esperado, éste siendo memorizado en el centro de verificación.

[0065] Si el resultado calculado corresponde al resultado esperado, el número protegido se considera como válido y el crédito o el derecho es acordado. Sino, el crédito o el derecho es negado.

[0066] En caso de que el número protegido sea enviado después del final del periodo de validez, incluso si el número de identificación es correcto, la clave o la información oculta utilizada para calcular el valor de control a partir del número de identificación habrá cambiado. En tal caso, el valor de control calculado será diferente del valor de control esperado y el número protegido será considerado como inválido.

REIVINDICACIONES

1. Método para atribuir un número protegido único a un soporte físico, este número protegido único es generado por un método para generar una pluralidad de números protegidos (SN) únicos que tienen una longitud fija predeterminada, los números protegidos están formados al menos por un número de identificación (IN) y de un valor de control (VC), dicho método de atribución de un número protegido comporta las etapas de:

- determinación de una primera cantidad de números protegidos que se debe generar;
- determinación del número mínimo de cifras necesarias para generar dicha primera cantidad de números protegidos;
- generación de una primera serie de números de identificación (IN) únicos, estos números de identificación tienen una longitud al menos igual al número mínimo de cifras necesarias para generar los números protegidos (SN), estos números de identificación son seleccionados entre todos los números posibles que tienen la longitud requerida;
- asociación de un valor de control (VC) a cada número de identificación (IN), este valor de control tiene una longitud tal que la longitud total de los números protegidos corresponda a dicha longitud fija predeterminada, este valor de control (VC) se calcula a partir de dicho número de identificación, de una información oculta y de una regla de cálculo;
- antes de la utilización de todos los números de identificación disponibles de la primera serie de números de identificación, determinación de una segunda cantidad adicional de números protegidos que se deben generar;
- cálculo del número de números de identificación restante que es posible generar a partir del número de cifras que forma los números de identificación de dicha primera serie;
- si la segunda cantidad de números de identificación que se debe generar es superior a dicho número de números de identificación restante, determinación del nuevo número mínimo de cifras necesarias para generar dicha segunda cantidad de números de identificación;
- determinación de por lo menos un número de identificación no utilizado entre los números de identificación que es posible generar utilizando el número de cifras de la primera cantidad de números de identificación;
- generación de una segunda serie de números de identificación (IN) únicos, estos números de identificación se forman a partir de números de identificación no utilizados entre los números de identificación que es posible generar utilizando el número de cifras de la primera cantidad de números de identificación, estos números de identificación de la segunda serie de números tiene una longitud al menos igual al nuevo número mínimo de cifras necesarias para generar dichos números de identificación (IN) de esta segunda serie de números;
- elección de un número protegido único entre dicha pluralidad de números protegidos únicos generados; y
- impresión de dicho número único elegido en un soporte físico.

2. Método según la reivindicación 1, **caracterizado por el hecho de que**

- si la segunda cantidad de números protegidos que se debe generar es inferior a dicho número de números protegidos restantes, determinación del nuevo número mínimo de cifras necesarias para generar dicha segunda cantidad de números protegidos;
- determinación del número de números de identificación que es posible generar utilizando dicho número mínimo de cifras necesarias para generar dicha segunda cantidad de números de identificación, estos nuevos números de identificación son diferentes de los números de identificación de la primera serie truncados a la longitud de los números de identificación de la segunda serie;
- si el número de números de identificación que es posible generar utilizando dicho número mínimo de cifras es superior a la segunda cantidad, generación de una serie de números de identificación únicos, que tienen una longitud igual a dicho número mínimo de cifras necesarias para generar dicha nueva cantidad de números de identificación y tales que estos nuevos números protegidos sean diferentes de los números protegidos de la primera serie truncados a la longitud de los números de identificación de la segunda serie.

3. Método según la reivindicación 1 o 2, **caracterizado por el hecho de que** se determina el número de números protegidos que se debe generar en el curso de un intervalo temporal.

4. Método según la reivindicación 3, caracterizado por el hecho de que dicho intervalo temporal corresponde a toda o parte de una duración de validez máxima del número protegido.

5. Método según la reivindicación 1, caracterizado por el hecho de que dicho soporte físico se utiliza para acceder a los derechos y/o obtener un crédito.

6. Soporte físico para el acceso a un derecho y/o un crédito, que comporta un número protegido (SN) único que tiene una longitud fija predeterminada, este número protegido está formado al menos por un número de identificación (IN) y por un valor de control (VC), **caracterizado por el hecho de que** dicho número protegido único se genera por las etapas siguientes:

- determinación de una primera cantidad de números protegidos que se debe generar;
- determinación del número mínimo de cifras necesarias para generar dicha primera cantidad de números protegidos;
- generación de una primera serie de números de identificación (IN) únicos, estos números de identificación tienen una longitud al menos igual al número mínimo de cifras necesarias para generar los números protegidos (SN), estos números de identificación son seleccionados entre todos los números posibles que tienen la longitud requerida;
- asociación de un valor de control (VC) en cada número de identificación (IN), este valor de control tiene una longitud tal que la longitud total de los números protegidos corresponda a dicha longitud fija predeterminada, este valor de control (VC) se calcula a partir de dicho número de identificación, de una información oculta y de una regla de cálculo;
- antes de la utilización de todos los números de identificación disponibles de la primera serie de números de identificación, determinación de una segunda cantidad adicional de números protegidos que se debe generar;
- cálculo del número de números de identificación restante que es posible generar a partir del número de cifras que forma los números de identificación de dicha primera serie;
- si la segunda cantidad de números de identificación que se debe generar es superior a dicho número de números de identificación restante, determinación del nuevo número mínimo de cifras necesarias para generar dicha segunda cantidad de números de identificación;
- determinación de por lo menos un número de identificación no utilizado entre los números de identificación que es posible generar utilizando el número de cifras de la primera cantidad de números de identificación;
- generación de una segunda serie de números de identificación (IN) únicos, estos números de identificación se forman a partir de números de identificación no utilizados entre los números de identificación que es posible generar utilizando el número de cifras de la primera cantidad de números de identificación, estos números de identificación de la segunda serie de números tienen una longitud al menos igual al nuevo número mínimo de cifras necesarias para generar dichos números de identificación (IN) de esta segunda serie de números;
- elección de un número protegido (SN) único entre los números protegidos únicos generados;
- impresión de dicho número protegido (SN) único elegido sobre dicho soporte físico.

7. Soporte físico según la reivindicación 6**, caracterizado por el hecho de que** dicho número protegido único está impreso sobre dicho soporte físico.

8. Conjunto de soportes físicos para el acceso a un derecho y/o un crédito, cada soporte físico comporta un número protegido (SN) único que tiene una longitud fija predeterminada, este número protegido está formado al menos por un número de identificación (IN) y de un valor de control (VC), **caracterizado por el hecho de que** dicho número protegido único se genera por las etapas siguientes:

- determinación de una primera cantidad de números protegidos que se debe generar;
- determinación del número mínimo de cifras necesarias para generar dicha primera cantidad de números protegido;
- generación de una primera serie de números de identificación (IN) únicos, estos números de identificación tienen una longitud al menos igual al número mínimo de cifras necesarias para generar los números protegidos (SN), estos números de identificación son seleccionados entre todos los números posibles que tienen la longitud requerida;
- asociación de un valor de control (VC) en cada número de identificación (IN), este valor de control tiene una longitud tal que la longitud total de los números protegidos corresponda a dicha longitud fija predeterminada, este valor de control (VC) se calcula a partir de dicho número de identificación, de una información oculta y de una regla de cálculo;
- antes de la utilización de todos los números de identificación disponibles de la primera serie de números de identificación, determinación de una segunda cantidad adicional de números protegidos que se debe generar;
- cálculo del número de números de identificación restantes que es posible generar a partir del número de cifras que forma los números de identificación de dicha primera serie;
- si la segunda cantidad de números de identificación que se debe generar es superior a dicho número de números de identificación restante, determinación del nuevo número mínimo de cifras necesarias para generar dicha segunda cantidad de números de identificación;
- determinación de por lo menos un número de identificación no utilizado entre los números de identificación que es posible generar utilizando el número de cifras de la primera cantidad de números de identificación;
- generación de un segunda serie de números de identificación (IN) únicos, estos números de identificación se forman a partir de números de identificación no utilizados entre los números de identificación que es posible generar utilizando el número de cifras de la primera cantidad de números de identificación, estos números de identificación del segunda serie de números tienen una longitud al menos igual al nuevo número mínimo de cifras necesarias para generar dichos números de identificación (IN) de esta segunda serie de números;
- elección de una cantidad de números protegidos (SN) únicos diferentes entre los números protegidos únicos generados, esta cantidad es al menos igual al número de soportes físicos que forma el conjunto de soportes físicos;
- impresión sobre cada uno de dichos soportes físicos que forma dicho conjunto de soportes físicos, de un número protegido (SN) único diferente elegido entre dichos números protegidos (SN) únicos generados.

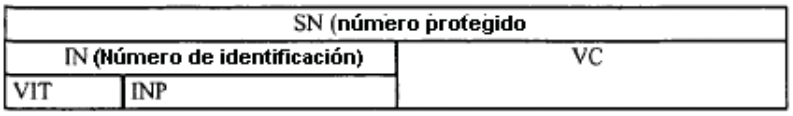


FIG 1A

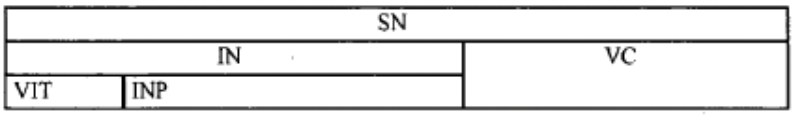


FIG 1B

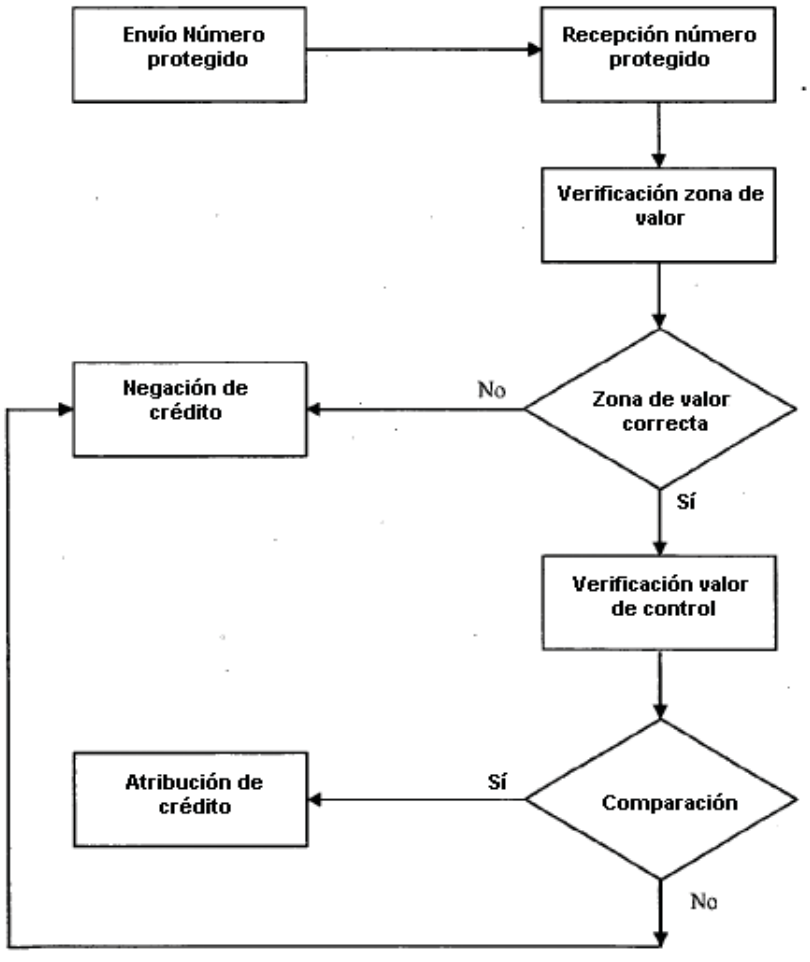
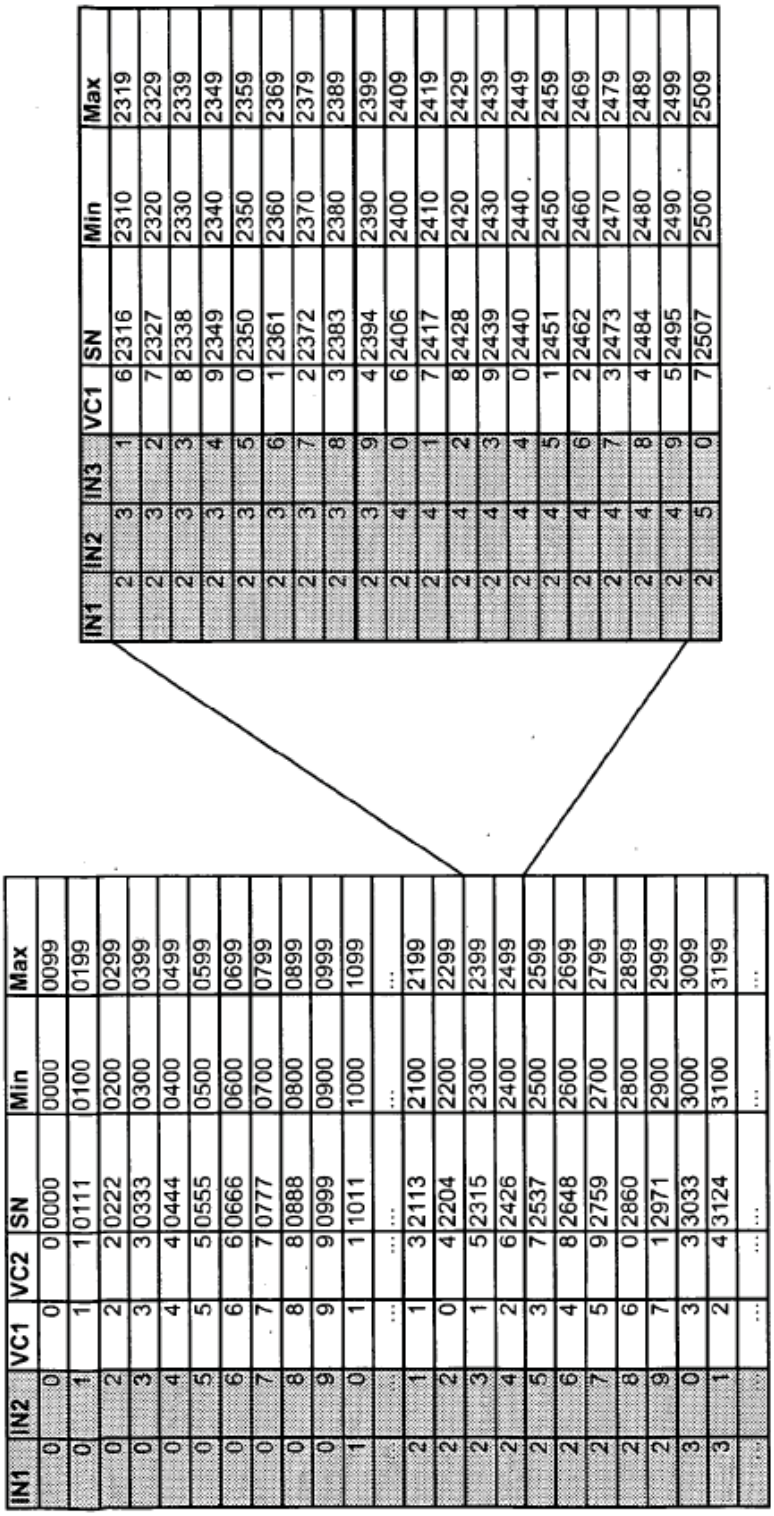


FIG 4

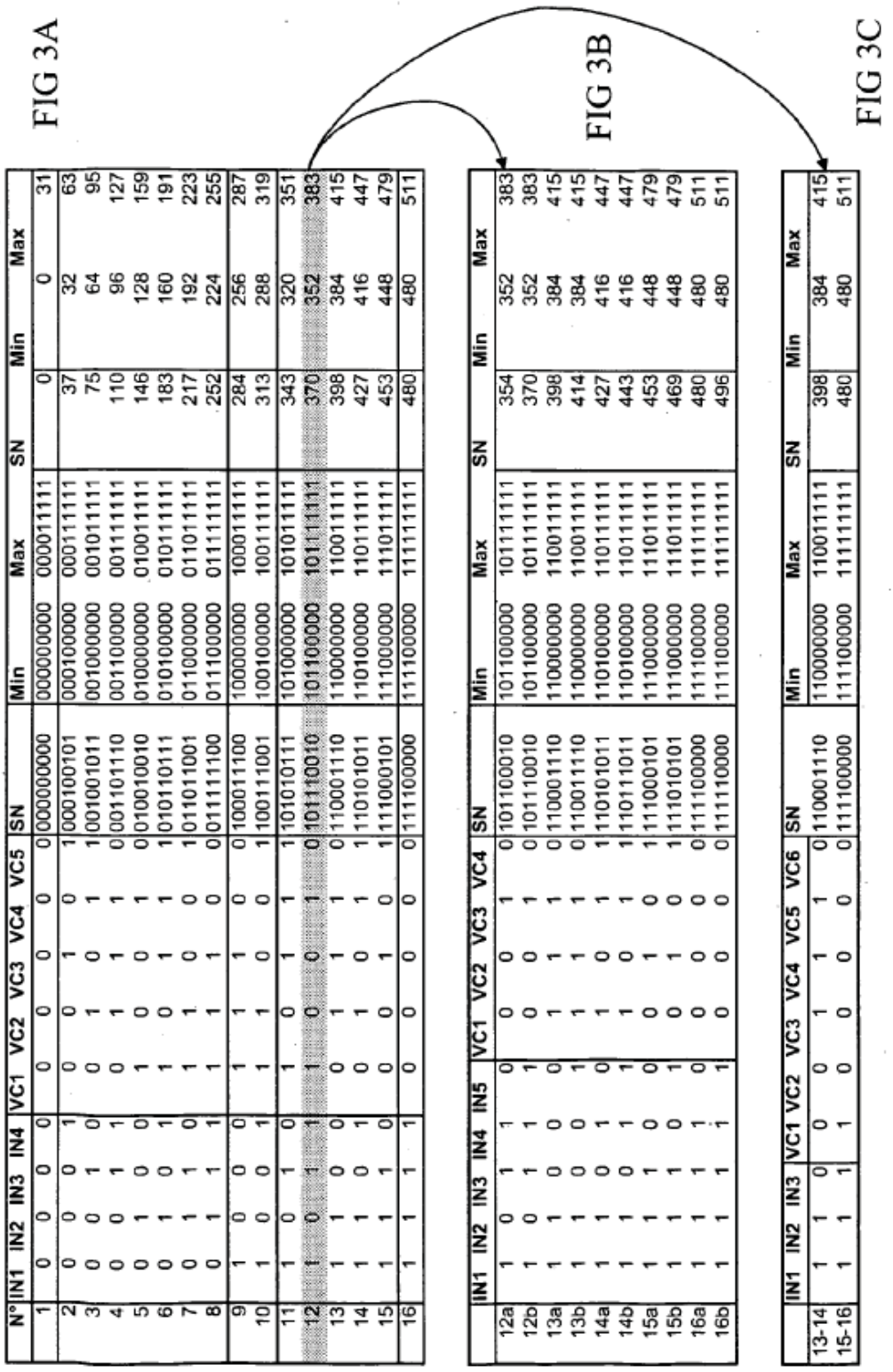


IN1	IN2	VC1	VC2	SN	Min	Max
0	0	0	0	0000	0000	0099
0	1	1	1	0111	0100	0199
0	2	2	2	0222	0200	0299
0	3	3	3	0333	0300	0399
0	4	4	4	0444	0400	0499
0	5	5	5	0555	0500	0599
0	6	6	6	0666	0600	0699
0	7	7	7	0777	0700	0799
0	8	8	8	0888	0800	0899
0	9	9	9	0999	0900	0999
1	0	1	1	1011	1000	1099
...	...	...	...	...	...	...
2	1	1	3	2113	2100	2199
2	2	0	4	2204	2200	2299
2	3	1	5	2315	2300	2399
2	4	2	6	2426	2400	2499
2	5	3	7	2537	2500	2599
2	6	4	8	2648	2600	2699
2	7	5	9	2759	2700	2799
2	8	6	0	2860	2800	2899
2	9	7	1	2971	2900	2999
3	0	3	3	3033	3000	3099
3	1	2	4	3124	3100	3199
...	...	...	...	...	...	...

FIG 2A

IN1	IN2	IN3	VC1	SN	Min	Max
2	3	1	6	2316	2310	2319
2	3	2	7	2327	2320	2329
2	3	3	8	2338	2330	2339
2	3	4	9	2349	2340	2349
2	3	5	0	2350	2350	2359
2	3	6	1	2361	2360	2369
2	3	7	2	2372	2370	2379
2	3	8	3	2383	2380	2389
2	3	9	4	2394	2390	2399
2	4	0	6	2406	2400	2409
2	4	1	7	2417	2410	2419
2	4	2	8	2428	2420	2429
2	4	3	9	2439	2430	2439
2	4	4	0	2440	2440	2449
2	4	5	1	2451	2450	2459
2	4	6	2	2462	2460	2469
2	4	7	3	2473	2470	2479
2	4	8	4	2484	2480	2489
2	4	9	5	2495	2490	2499
2	5	0	7	2507	2500	2509

FIG 2B



N°	IN1	IN2	IN3	IN4	VC1	VC2	VC3	VC4	VC5	SN	Min	Max	SN	Min	Max
1	0	0	0	0	0	0	0	0	0	0000000000	0000000000	0000011111		0	31
2	0	0	0	1	0	0	1	0	1	0000100101	0000100000	0000111111		37	63
3	0	0	1	0	0	1	0	1	1	0010011011	0010000000	0010111111		75	95
4	0	0	1	1	0	1	1	1	0	0011101110	0011000000	0011111111		110	127
5	0	1	0	0	1	0	0	1	0	0100010010	0100000000	0100111111		146	159
6	0	1	0	1	1	0	1	1	1	0101110111	0101000000	0101111111		183	191
7	0	1	1	0	1	1	0	0	1	0110011001	0110000000	0110111111		217	223
8	0	1	1	1	1	1	1	0	0	0111111100	0111000000	0111111111		252	255
9	1	0	0	0	1	1	1	0	0	1000111100	1000000000	1000111111		284	287
10	1	0	0	1	1	1	0	0	1	1001111001	1001000000	1001111111		313	319
11	1	0	1	0	1	0	1	1	1	1010101111	1010000000	1010111111		343	351
12	1	0	1	1	1	0	0	1	0	1011100010	1011000000	1011111111		370	383
13	1	1	0	0	0	1	1	1	0	1100001110	1100000000	1100111111		398	415
14	1	1	0	1	0	1	0	1	1	1101010111	1101000000	1101111111		427	447
15	1	1	1	0	0	0	1	0	1	1110001011	1110000000	1110111111		453	479
16	1	1	1	1	0	0	0	0	0	1111000000	1111000000	1111111111		480	511

	IN1	IN2	IN3	IN4	IN5	VC1	VC2	VC3	VC4	SN	Min	Max	SN	Min	Max
12a	1	0	1	1	0	0	0	1	0	1011000010	1011000000	1011111111		354	383
12b	1	0	1	1	1	0	0	1	0	1011100010	1011000000	1011111111		370	383
13a	1	1	0	0	0	1	1	1	0	1100001110	1100000000	1100111111		398	415
13b	1	1	0	0	1	1	1	1	0	1100011110	1100000000	1100111111		414	415
14a	1	1	0	1	0	1	0	1	1	1101010111	1101000000	1101111111		427	447
14b	1	1	0	1	1	1	0	1	1	1101110111	1101000000	1101111111		443	447
15a	1	1	1	0	0	0	1	0	1	1110001011	1110000000	1110111111		453	479
15b	1	1	1	0	1	0	1	0	1	1110101101	1110000000	1110111111		469	479
16a	1	1	1	1	0	0	0	0	0	1111000000	1111000000	1111111111		480	511
16b	1	1	1	1	1	0	0	0	0	1111100000	1111000000	1111111111		496	511

	IN1	IN2	IN3	VC1	VC2	VC3	VC4	VC5	VC6	SN	Min	Max	SN	Min	Max
13-14	1	1	0	0	0	1	1	1	0	1100011110	1100000000	1100111111		398	384	415
15-16	1	1	1	1	0	0	0	0	0	1111100000	1111000000	1111111111		480	480	511

FIG 3A

FIG 3B

FIG 3C