(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 382 301**

(51) Int. CI.:
H04L 9/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08865750 .7**
(96) Fecha de presentación: **05.12.2008**
(97) Número de publicación de la solicitud: **2232762**
(97) Fecha de publicación de la solicitud: **29.09.2010**

(54) Título: **Procedimiento de codificación de un secreto formado por un valor numérico**

(30) Prioridad:
07.12.2007 FR 0708541

(45) Fecha de publicación de la mención BOPI:
07.06.2012

(45) Fecha de la publicación del folleto de la patente:
07.06.2012

(73) Titular/es:
MORPHO
27, Rue Leblanc
75015 Paris, FR

(72) Inventor/es:
PELLETIER, Hervé y
SENGMANIVANH, Isabelle

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Procedimiento de codificación de un secreto formado por un valor numérico.

La invención concierne a un procedimiento de codificación de un secreto, formado por un valor numérico.

El considerable desarrollo de las comunicaciones por transmisión de mensajes electrónicos no ha tardado en plantear el problema de la confidencialidad de los datos transmitidos.

Se han propuesto soluciones muy sofisticadas de cifrado/descifrado de estos datos por medio de algoritmos de cifrado de clave secreta única, sirviendo para el cifrado/descifrado, y luego de clave pública, que lleva asociada una clave privada, utilizada para el descifrado de los datos, cifrados por medio de la clave pública.

Por ejemplo, el documento D_1=WO2006/046187 describe un procedimiento de ocultación aplicado con ayuda de un operador de grupo abeliano sobre una estructura de Feistel.

Las antedichas soluciones son satisfactorias, por cuanto que los algoritmos de clave secreta difícilmente se pueden romper, por lo menos en ausencia de compromiso de la clave secreta, y por cuanto que los algoritmos de clave pública/clave privada no conllevan limitaciones en lo que respecta a la difusión de la clave pública y precisan de la puesta en práctica de medios de soporte físico y lógico de complejidad y de coste computacional prohibitivos, ya sea a efectos de romper el algoritmo de cifrado/descifrado, o bien de dar con el valor de la clave privada, asociada a la clave pública.

En cualquier caso, en la utilización de un esquema criptográfico de clave secreta única o de clave pública, que lleva asociada una clave privada, es imprescindible impedir cualquier compromiso de la clave secreta o de la clave privada, con el fin de garantizar la confidencialidad de los datos transmitidos.

Aun cuando se han propuesto satisfactorios componentes criptográficos con acceso protegido, en particular integrados en forma de procesadores de seguridad de los componentes criptográficos de tarjetas electrónicas, llamadas tarjetas inteligentes, pudiendo hacerse extremadamente difícil, si no prácticamente imposible, el acceso exterior por mediación del puerto de entrada/salida a los componentes de seguridad de estas tarjetas electrónicas, la manipulación de las claves secretas o privadas en lectura/escritura mediante esos componentes es susceptible de permitir el compromiso de las antedichas claves, en particular de los valores secretos o los secretos que entran en la definición de estas últimas.

Este compromiso es susceptible de concurrir mediante ataque por «canales colaterales» (Side Chanel attack en inglés), pudiendo consistir por ejemplo este tipo de ataque en detectar las variaciones de intensidad de la corriente eléctrica consumida por el componente de seguridad o la tarjeta en el transcurso de esas manipulaciones, necesarias.

La presente invención tiene por objeto subsanar los inconvenientes de los riesgos de ataque por canales colaterales, mediante la puesta en práctica de un procedimiento de codificación de un secreto, subdividido en varios elementos de secreto no correlacionados entre sí, sin que la manipulación de los elementos de secreto pueda permitir, aunque cada elemento de secreto pueda, llegado el caso, verse comprometido, dar con el secreto original.

El procedimiento de codificación de un secreto formado por un valor numérico, en un esquema de criptografía de clave secreta o de clave pública en el que ese secreto se divide entre una pluralidad de un número determinado de elementos, del cual una ley de composición representa el valor de ese secreto, objeto de la presente invención, es notable por el hecho de que consiste, además, en recalcular una nueva pluralidad de elementos del secreto sin manipular nunca ese secreto. Para ello, hay que calcular una primera imagen de ese secreto mediante aplicación iterativa de la ley de composición término a término entre la primera imagen de orden anterior y el producto de composición según esta ley de composición del elemento de orden siguiente y un valor aleatorio de igual orden escogido de entre un primer conjunto de una misma pluralidad de valores aleatorios, calcular un primer valor numérico producto de composición de esta ley de composición aplicada sucesivamente a los valores aleatorios de ese primer conjunto de valores aleatorios, calcular un segundo valor numérico producto de composición según esta ley de composición aplicada sucesivamente a los valores aleatorios de un segundo conjunto de una misma pluralidad menos uno de valores aleatorios, calcular una segunda imagen de ese secreto mediante aplicación de la ley de composición inversa a la primera imagen de ese secreto y a ese segundo valor numérico, para originar una imagen intermedia de ese secreto, y mediante aplicación posterior de esa ley de composición inversa a esa imagen intermedia y a ese primer valor numérico, para originar esa segunda imagen de dicho secreto, asignar a cada uno de esos sucesivos elementos menos el último de esa pluralidad de elementos el valor aleatorio de orden correspondiente de ese segundo conjunto de al menos un valor aleatorio y al último elemento el valor numérico de esa segunda imagen.

Se comprenderá mejor el procedimiento de codificación de un secreto, objeto de la presente invención, con la lectura de la descripción y con la observación de los dibujos que siguen, en los que:

la figura 1 representa, a título ilustrativo, un organigrama general de puesta en práctica de las etapas constitutivas

del procedimiento objeto de la invención;

la figura 2a representa, a título ilustrativo, una primera y una segunda ley de composición que, aplicable a valores numéricos, permite la puesta en práctica del procedimiento objeto de la presente invención;

la figura 2b representa, a título ilustrativo, un organigrama específico de puesta en práctica del procedimiento objeto de la invención, cuando la ley de composición representada en la figura 2a es una operación O-exclusiva;

la figura 2c representa a título ilustrativo un organigrama específico de puesta en práctica del procedimiento objeto de la invención, cuando la ley de composición representada en la figura 2a es una operación de suma;

la figura 3 es un esquema funcional de un componente de seguridad de un dispositivo criptográfico especialmente adaptado para la puesta en práctica del procedimiento objeto de la invención.

Se dará a continuación, en relación con la figura 1, una descripción más detallada del procedimiento de codificación de un secreto, conforme al objeto de la presente invención.

De una manera general, recordemos que el procedimiento, objeto de la invención, tiene por objeto la codificación de un secreto $\underline{s}$ formado por un valor numérico $\underline{d}$, en un esquema de criptografía de clave secreta o de clave pública.

Éste es de aplicación más concretamente a cualquier proceso de cálculo criptográfico en el que el secreto $\underline{s}$ se subdivide en una pluralidad de un número determinado de elementos de secreto, denotado cada uno de ellos como d_i, de cuya pluralidad de elementos que a continuación se designa $[d_i]_1^N$ una ley de composición denotada como $\otimes$ representa el valor numérico del secreto $\underline{s}$.

Haciendo referencia a la figura 1, el secreto $\underline{s}$ y el valor numérico $\underline{d}$ que representa a este último verifican la relación (1):

$$s = \underline{d}\,;[d_i]_1^N$$

$$\underline{d} = \pi_{i=1}^{\otimes N} \mathrm{d}_i$$

En esta relación $\pi_{i=1}^{\otimes N}$ di representa el producto de composición de la ley de composición $\otimes$ aplicada al conjunto de los N elementos d_i.

Tal y como se representa en la figura 1, el procedimiento objeto de la invención consiste en una etapa A de calcular una primera imagen del secreto $\underline{s}$ mediante aplicación iterativa de la ley de composición término a término entre la primera imagen de orden anterior, denotada como T_{i-1}, y el producto de composición, según esa ley de composición, del elemento de orden i siguiente, denotado como d_i y un valor aleatorio, denotado como R_i, escogido de entre un primer conjunto de una misma pluralidad de valores aleatorios.

En la etapa A de la figura 1, el primer conjunto de una misma pluralidad de valores aleatorios se denota como $[R_i]_1^N$.

Con referencia a la etapa A de la figura 1, la operación de cálculo de la primera imagen TN verifica la relación (2):

$$[T_i = T_{i-1} \otimes (d_i \otimes R_i)]_1^N \rightarrow T_N$$

En la relación anterior,

-- T_i designa la primera imagen corriente de orden i;

-- T_{i-1} designa la primera imagen anterior de orden i−1;

-- d_i designa el elemento corriente de orden i;

-- R_i designa el valor aleatorio de orden i del primer conjunto de valores aleatorios;

-- T_N designa la primera imagen obtenida tras cálculo iterativo.

La etapa A de la figura 1 viene seguida de una etapa B consistente en calcular un primer valor numérico, denotado

como S_1, producto de composición de la misma antedicha ley de composición aplicada sucesivamente a los valores aleatorios del primer conjunto de valores aleatorios anteriormente mencionado.

En la etapa B de la figura 1, el primer valor numérico S_1 verifica la relación (3):

$$S_1 = \overset{\otimes N}{\underset{i=1}{\pi}} R_i$$

La etapa B de la figura 1 viene seguida de una etapa C consistente en calcular un segundo valor numérico, denotado como S_2, producto de composición, según la misma antedicha ley de composición, aplicada sucesivamente a los valores aleatorios de un segundo conjunto de una misma pluralidad menos uno de valores aleatorios.

En consecuencia, el segundo conjunto de una misma pluralidad menos uno de valores aleatorios se denota como $[A_j]_1^{N-1}$.

El segundo valor numérico verifica la relación (4):

$$S_2 = \overset{\otimes N-1}{\underset{j=1}{\pi}} A_j$$

La etapa C de la figura 1 viene seguida entonces de una etapa D consistente en calcular una segunda imagen del secreto denotada como T'.

Con referencia a la etapa D de la figura 1, se indica que la segunda imagen T' antedicha se calcula mediante aplicación de la ley de composición inversa aplicada a la primera imagen del secreto T_N y a ese segundo valor numérico S_2, para originar una imagen intermedia denotada como T_x, y mediante aplicación posterior de esa misma ley de composición inversa aplicada a la imagen intermedia T_x y al primer valor numérico S_1, para originar la segunda imagen del secreto, denotada como T'. La ley de composición inversa se denota como $\overline{\otimes}$.

En la etapa D de la figura 1, el cálculo de la segunda imagen T' verifica la relación (5):

$$T_x = T_N \,\overline{\otimes}\, S_2$$

$$T' = T_x \,\overline{\otimes}\, S_1$$

La etapa D de la figura 1 viene seguida entonces de una etapa E consistente en asignar, a cada uno de los sucesivos elementos de la pluralidad de elementos $[d_i]_1^N$, menos el último, el valor aleatorio de orden correspondiente al del segundo conjunto de al menos un valor aleatorio, conjunto denotado como $[A_j]_1^{N-1}$ y en asignar al último elemento el valor numérico de la segunda imagen antedicha T'.

En consecuencia, la etapa de asignaciones representadas en la etapa E verifica la relación (6):

$$\{[d_i]_1^{N-1} = [A_j]_1^{N-1}$$

$$\{d_N = T'$$

Se dará a continuación una descripción más detallada de una primera y de una segunda variante de puesta en práctica del procedimiento objeto de la invención en relación con la figura 2a y las figuras 2b y 2c, respectivamente.

De una manera general, se indica que la ley de composición anteriormente citada se forma mediante una operación aritmética o lógica distributiva, dotada de un elemento neutro. Se puede aplicar así una correspondiente ley de composición a cualquier secreto y a cualquier elemento de secreto formado por un valor numérico constituido bien por un número entero, o bien por un número real.

Así, en este supuesto, para un secreto s formado por un valor numérico d de longitud L determinada, cada valor aleatorio R_i del primer y respectivamente A_j del segundo conjunto de valores aleatorios se elige de longitud inferior a 2^{L-N+1}.

A título de ejemplo no limitativo, la antedicha ley de composición puede consistir, tal y como se representa en la

figura 2a, en una operación O-exclusiva, por ejemplo. Puede consistir además en una operación aritmética tal como la suma.

Se señala naturalmente que la antedicha ley de composición está dotada entonces de una operación inversa, la operación O-exclusiva invariante, cuando la operación O-exclusiva constituye la antedicha ley de composición, y respectivamente la operación de resta, cuando la operación de suma constituye la ley de composición anteriormente citada.

Las leyes de composición anteriormente mencionadas y su correspondiente operación están representadas en el dibujo de la figura 2a, ilustrada mediante la relación (7):

$$\otimes = \oplus; \overline{\otimes} = \oplus$$

$$\otimes = +; \overline{\otimes} = -$$

En la relación anterior,

$\oplus$ representa la operación O-exclusiva, llevada a cabo bit a bit sobre los números enteros o reales constituyentes de los elementos de secreto o del secreto, así como los números aleatorios;

+ y − representan la operación de suma y la operación inversa de resta para la ley de composición formada por la suma aritmética. Además, el elemento neutro es 0 para las dos operaciones.

Se describe a continuación, en relación con la figura 2b, una forma específica de puesta en práctica del procedimiento objeto de la invención, en el caso de la puesta en práctica no limitativa de una ley de composición formada por la operación O-exclusiva.

En la etapa A de la figura 2b, la operación de cálculo de la primera imagen T_N viene dada por la relación (8):

$$[T_i = T_{i-1} \oplus (d_i \oplus R_i)]_{i=1}^{i=N} \rightarrow T_N$$

En la etapa B de la figura 2b, la operación de cálculo del primer valor numérico viene dada por la relación (9):

$$S_1 = \pi_{i=1}^{\oplus N} \mathrm{R_i};$$

En la etapa C de la figura 2b, la operación de cálculo del segundo valor numérico viene dada por la relación (10):

$$S_2 = \pi_{j=1}^{\oplus N-1} A_j$$

En la etapa D de la figura 2b, la operación de cálculo de la segunda imagen T' viene dada por la relación (11):

$$T_x = T_N \oplus S_2$$

$$T' = T_x \oplus S_1$$

Finalmente, la etapa E de asignación queda inalterada con respecto a la etapa E de asignación de la figura 1.

Además, a título de ejemplo no limitativo, la antedicha ley de composición puede consistir, tal y como se representa en la figura 2c, en una operación de suma aritmética.

En la etapa A de la figura 2c, la operación de cálculo de la primera imagen T_N viene dada por la relación (12):

$$\left[T_i = T_{i-1} + (d_i + R_i)\right]_{i=1}^{i=N} \rightarrow T_N$$

En la etapa B de la figura 2c, la operación de cálculo del primer valor numérico viene dada por la relación (13):

$$S_1 = \sum_{i=1}^{N} R_i$$

En la etapa C de la figura 2c, la operación de cálculo del segundo valor numérico viene dada por la relación (14):

$$S_2 = \sum_{j=1}^{N-1} A_j$$

En la etapa D de la figura 2c, la operación de cálculo de la segunda imagen T' viene dada por la relación (15):

$$T_x = T_N - S_2$$

$$T' = T_x - S_1$$

Haciendo referencia a la figura 2c, puede observarse que la etapa de asignación E de la figura 1 se subdivide entonces en dos sub-etapas si cada elemento d_i del secreto debe ser positivo. Esta sub-etapa E_0 es una prueba de comparación de superioridad de la segunda imagen T' frente al valor cero y una sub-etapa E_1 de asignación propiamente dicha, la cual queda asimismo inalterada con relación a la etapa de asignaciones E de la figura 1.

La sub-etapa de prueba E_0 tiene por objeto verificar que la segunda imagen T' es significativa. El carácter significativo de la segunda imagen T' se obtiene cuando el valor numérico representativo de esta última es estrictamente superior a cero.

Así, ante una respuesta positiva a la prueba de comparación de la sub-etapa E_0, la sub-etapa de asignación propiamente dicha E_1 es invocada y realizada de la misma manera que en el caso de la figura 1 o de la figura 2b.

Por el contrario, ante una respuesta negativa a la sub-etapa de prueba E_0, siendo entonces negativa la segunda imagen T', se ejecuta un retorno a la etapa A para llevar a cabo nuevamente el proceso de cálculo hasta la obtención de un valor positivo que represente a la segunda imagen T'.

Se dará a continuación, en relación con la figura 3, una descripción de un componente de seguridad de dispositivo criptográfico que comprende un procesador seguro, una memoria no volátil, una memoria de trabajo, una memoria de programa y un bus con acceso protegido en lectura-escritura.

En la antedicha figura 3, el microprocesador seguro se denota como µPS, la memoria de trabajo se denota como RAMS, la memoria de programa se denota como PROGS, la memoria no volátil se denota como NVS y el bus interno se denota como I/O.

El componente de seguridad objeto de la invención es notable por el hecho de que la memoria de programa PROGS comprende un programa de ordenador que incluye una serie de instrucciones memorizadas en esta memoria de programa.

En la ejecución de esas instrucciones, el procesador seguro µPS ejecuta las etapas de puesta en práctica del procedimiento de codificación de un secreto formado por el valor numérico d en cualquier esquema de criptografía de clave secreta, o de clave pública, tal y como anteriormente se ha descrito en la descripción en relación con las figuras 1 a 2b.

Así, el procesador de seguridad µPS entrega en el bus con acceso protegido en lectura-escritura denotado como I/O tan sólo los elementos de secreto denotados como di sucesivamente, bajo el control del dispositivo criptográfico, no representado en el dibujo de la figura 3.

Se comprende, en especial, que el procedimiento y el componente de seguridad objetos de la invención operan sobre cualquier secreto formado por un valor numérico d que constituye total o parcialmente ya sea una clave secreta en un esquema de criptografía de clave secreta, o bien una clave privada en cualquier esquema de criptografía de clave pública.

Por supuesto, el procedimiento y el componente de seguridad antedichos objetos de la invención son susceptibles de ser puestos en práctica para el cálculo de cualquier valor de código de acceso, de identificación con vocación secreta de un proceso de autenticación, de no repudio o de firma.

REIVINDICACIONES

1. Procedimiento de codificación de un secreto formado por un valor numérico $\underline{d}$, en un esquema de criptografía de clave secreta o de clave pública, en el que el secreto se subdivide en una pluralidad de un número N determinado de elementos $\underline{d}_i$, $[\underline{d}_i]_1^N$ del cual una ley de composición representa el valor numérico $\underline{d}$ de dicho secreto, caracterizado porque dicho procedimiento consiste además en:

-- calcular una primera imagen T_N de dicho secreto mediante aplicación iterativa de la ley de composición término a término entre dicha primera imagen T_{i-1} de orden i−1 y el producto de composición según dicha ley de composición del elemento $\underline{d}_i$ de orden i siguiente y un valor aleatorio R_i de orden i escogido de entre un primer conjunto de una pluralidad de N valores aleatorios

$$[T_i = T_{i-1} \otimes (d_i \otimes R_i)]_{i=1}^{i=N} \rightarrow T_N ;$$

-- calcular un primer valor numérico S_1 producto de composición de dicha ley de composición aplicada sucesivamente a dichos valores aleatorios R_i de dicho primer conjunto de N valores aleatorios

$$S_1 = \overset{\otimes N}{\underset{i=1}{\pi}} \mathrm{R_i} ;$$

-- calcular un segundo valor numérico S_2 producto de composición según dicha ley de composición aplicada sucesivamente a los valores aleatorios A_j de un segundo conjunto de N−1 valores aleatorios

$$S_2 = \overset{\otimes N-1}{\underset{j=1}{\pi}} A_j ;$$

-- calcular una segunda imagen T' de dicho secreto mediante aplicación de la ley de composición inversa a dicha primera imagen T_N de dicho secreto y a dicho segundo valor numérico S_2, para originar una imagen intermedia T_x de dicho secreto, y mediante aplicación posterior de dicha ley de composición inversa a dicha imagen intermedia T_x y a dicho primer valor numérico S_1, para originar dicha segunda imagen T' de dicho secreto

$$T_x = T \overline{\otimes} S_2$$

$$T' = T_x \overline{\otimes} S_1$$

-- asignar a cada uno de los N−1 primeros elementos sucesivos $\underline{d}_i$ de dicha pluralidad de elementos $[\underline{d}_i]$ el valor aleatorio A_j de orden correspondiente de dicho segundo conjunto de al menos un valor aleatorio y al elemento $\underline{d}_N$ de orden N el valor numérico de dicha segunda imagen T'.

2. Procedimiento según la reivindicación 1, en el que dicha ley de composición está formada por una operación aritmética o lógica distributiva, dotada de un elemento neutro.

3. Procedimiento según la reivindicación 2, caracterizado porque dicha operación lógica es la operación O-exclusiva bit a bit.

4. Procedimiento según la reivindicación 2, caracterizado porque dicha operación aritmética es la suma, estando formada la ley de composición inversa por la resta.

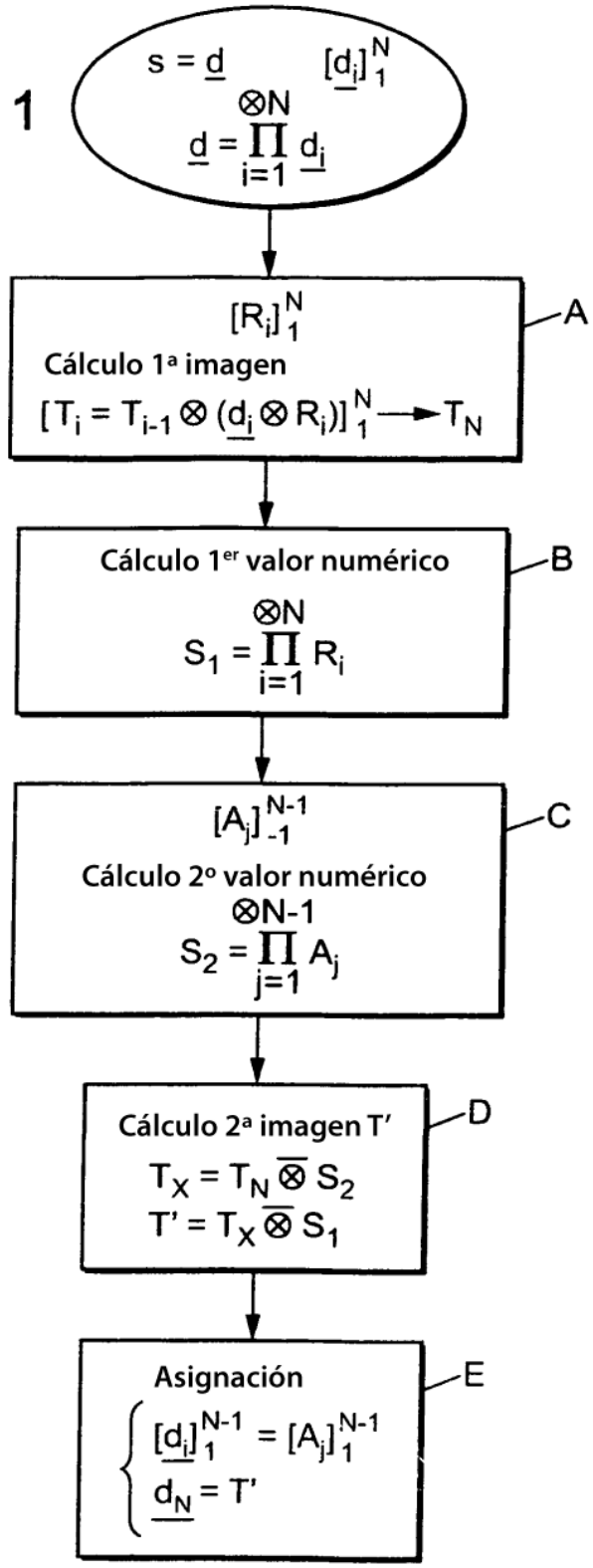
5. Procedimiento según una de las anteriores reivindicaciones, caracterizado porque, para un secreto formado por un valor numérico $\underline{d}$ de longitud L determinada, cada valor aleatorio R_i del primer y respectivamente A_j del segundo conjunto de valores aleatorios se elige de longitud inferior a 2^{L-N+1}.

6. Procedimiento según las reivindicaciones 4 y 5, caracterizado porque, para una operación aritmética formada por la suma, dicho procedimiento comprende además, previamente a dicha etapa consistente en asignar, una etapa de comparación de superioridad del valor numérico de dicha segunda imagen T' frente al valor cero, viniendo una respuesta positiva a dicha etapa de comparación seguida de dicha etapa consistente en asignar, viniendo dicha etapa de comparación seguida de una etapa de retorno a dicha etapa consistente en calcular dicha primera imagen T_N de dicho secreto para iteración del procedimiento, en caso contrario.

7. Procedimiento según una de las reivindicaciones 1 a 6, caracterizado porque dicho secreto formado por un valor numérico $\underline{d}$ es bien una clave secreta en un esquema de criptografía de clave secreta, bien una clave privada en un esquema de criptografía de clave pública, o bien incluso cualquier valor de código de acceso, de identificación con vocación secreta de un proceso de autenticación, de no repudio o de firma.

8. Componente de seguridad de un dispositivo criptográfico que comprende un procesador seguro, una memoria no volátil, una memoria de trabajo, una memoria de programa y un bus con acceso protegido en lectura-escritura, caracterizado porque dicha memoria de programa comprende un programa de ordenador que incluye una serie de instrucciones memorizadas en dicha memoria de programa y porque, en la ejecución de dichas instrucciones, dicho procesador seguro ejecuta las etapas del procedimiento según una de las reivindicaciones 1 a 7, entregando dicho procesador de seguridad en el bus con acceso protegido en lectura-escritura tan sólo los elementos $\underline{d}_i$ sucesivamente, bajo el control de dicho dispositivo criptográfico.

FIG. 1


s = d [d_i]_1^N
⊗N
d = ∏ d_i
i=1
[R_i]_1^N
Cálculo 1ª imagen
[T_i = T_i-1 ⊗ (d_i ⊗ R_i)]_1^N → T_N
A
Cálculo 1er valor numérico
⊗N
S_1 = ∏ R_i
i=1
B
[A_j]_-1^N-1
Cálculo 2º valor numérico
⊗N-1
S_2 = ∏ A_j
j=1
C
Cálculo 2ª imagen T'
T_X = T_N ⊗̄ S_2
T' = T_X ⊗̄ S_1
D
Asignación
[d_i]_1^N-1 = [A_j]_1^N-1
d_N = T'
E

$\otimes = \oplus$; $\overline{\otimes} = \oplus$

$\otimes = +$; $\overline{\otimes} = -$

FIG. 2a

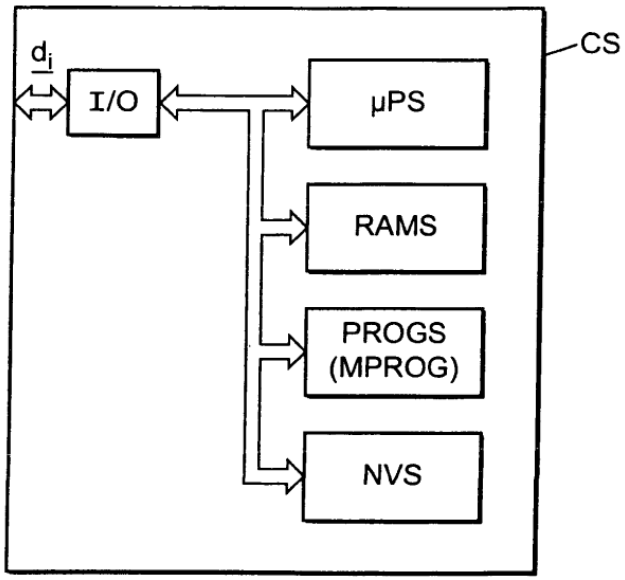


FIG. 3

FIG. 2b

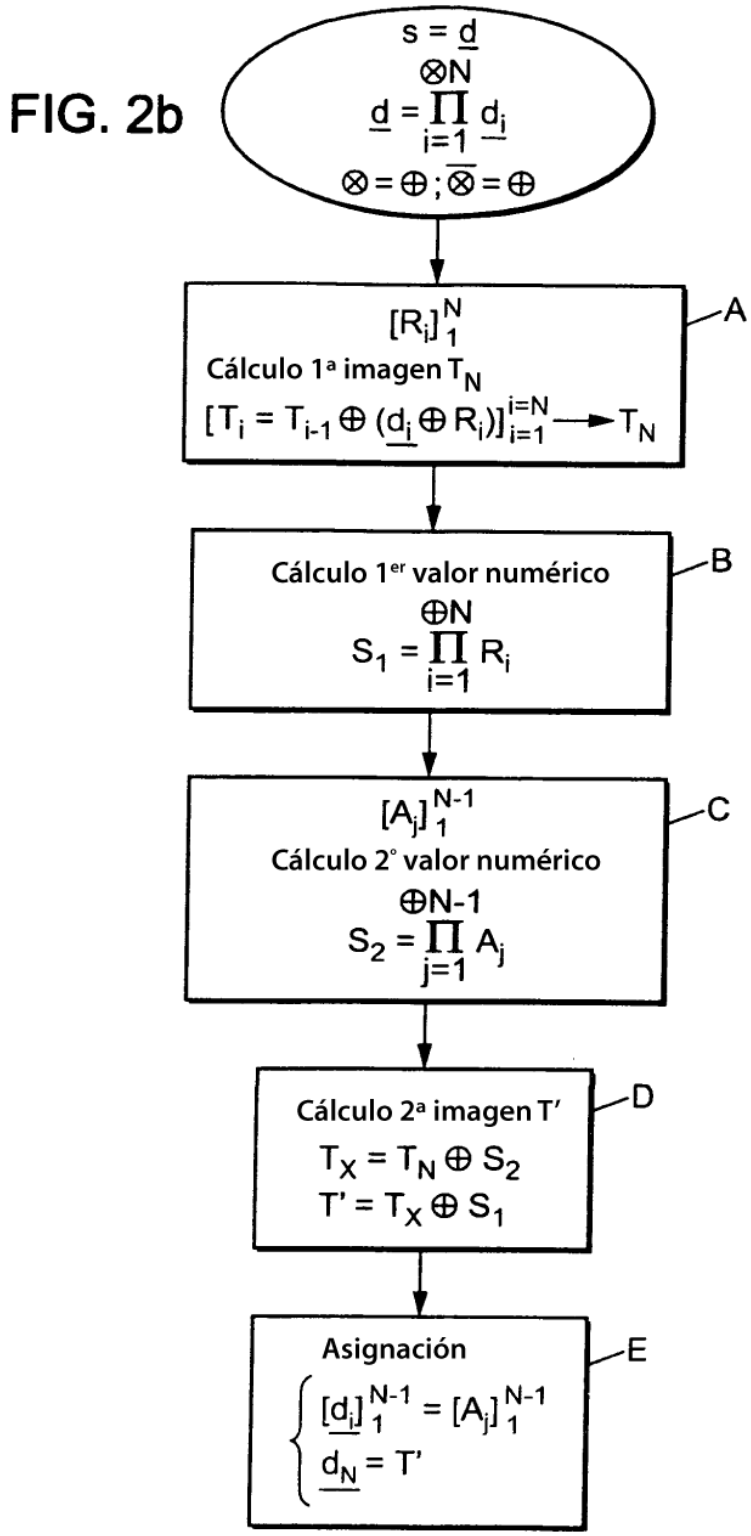
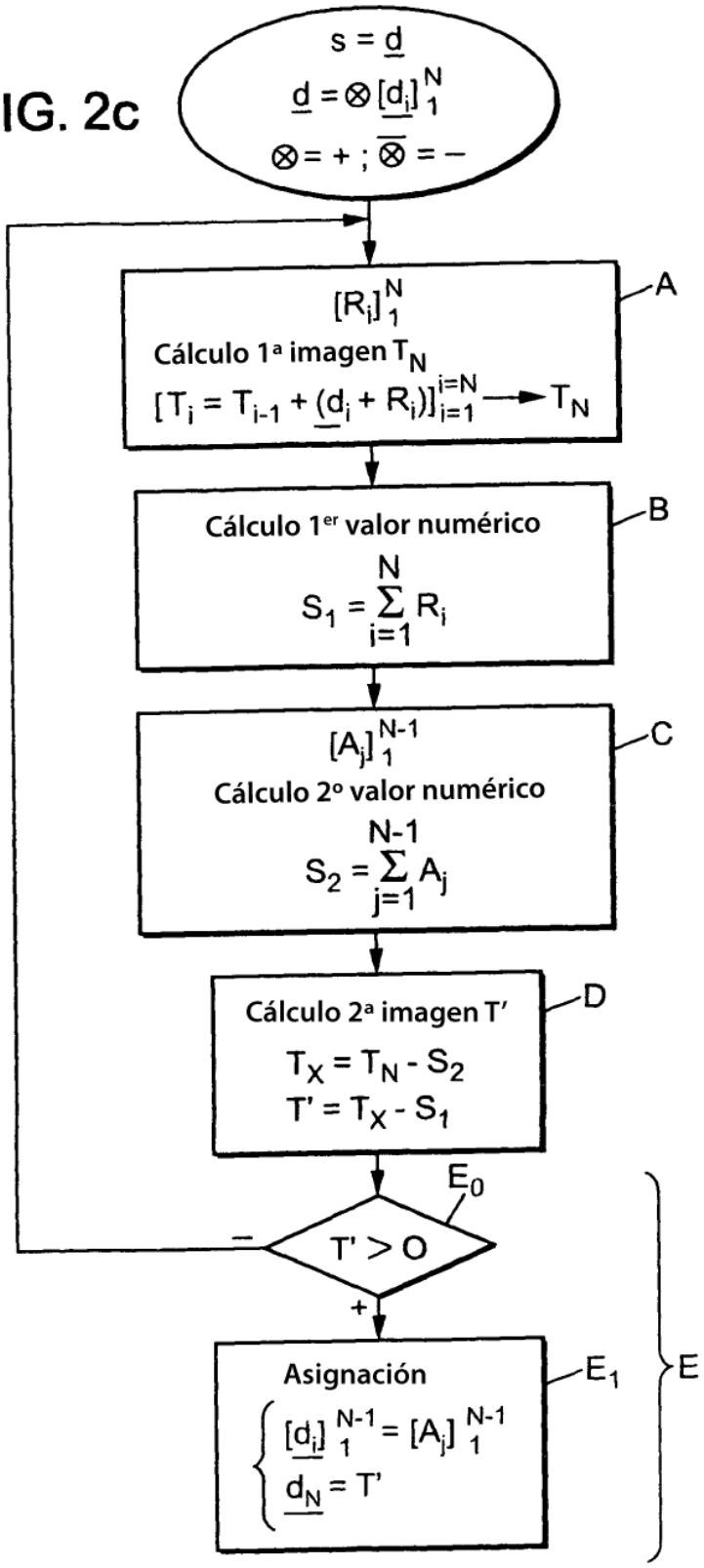

s = d
⊗N
d = ∏ d_i
i=1
⊗ = ⊕ ; ⊗̄ = ⊕
[R_i]_1^N
Cálculo 1ª imagen T_N
[T_i = T_i-1 ⊕ (d_i ⊕ R_i)]_i=1^i=N → T_N
A
Cálculo 1er valor numérico
⊕N
S_1 = ∏ R_i
i=1
B
[A_j]_1^N-1
Cálculo 2° valor numérico
⊕N-1
S_2 = ∏ A_j
j=1
C
Cálculo 2ª imagen T'
T_X = T_N ⊕ S_2
T' = T_X ⊕ S_1
D
Asignación
[d_i]_1^N-1 = [A_j]_1^N-1
d_N = T'
E

FIG. 2c


s = d
d = ⊗ [d_i]_1^N
⊗ = + ; ⊗ = −
[R_i]_1^N
Cálculo 1ª imagen T_N
[T_i = T_{i-1} + (d_i + R_i)]_{i=1}^{i=N} → T_N
A
Cálculo 1er valor numérico
S_1 = Σ_{i=1}^{N} R_i
B
[A_j]_1^{N-1}
Cálculo 2º valor numérico
S_2 = Σ_{j=1}^{N-1} A_j
C
Cálculo 2ª imagen T'
T_X = T_N - S_2
T' = T_X - S_1
D
E_0
T' > O
−
+
Asignación
[d_i]_1^{N-1} = [A_j]_1^{N-1}
d_N = T'
E_1
E