(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 948 323**

(21) Número de solicitud: 202230118

(51) Int. CI.:

H04L 9/30 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

15.02.2022

(43) Fecha de publicación de la solicitud:

08.09.2023

(71) Solicitantes:

UNIVERSIDAD DE GRANADA (100.0%)
Hospital Real. Avda. del Hospicio s/n
18071 Granada (Granada) ES

(72) Inventor/es:

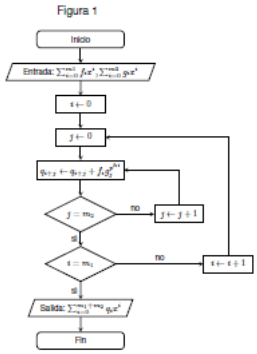
GÓMEZ TORRECILLAS, José;
LOBILLO BORRERO, Francisco Javier y
NAVARRO GARULO, Gabriel

(54) Título: **Procedimiento y dispositivo de cifrado/descifrado post-cuántico usando códigos lineales**

(57) Resumen:

Esta invención es un criptosistema asimétrico, presentado mediante un mecanismo de encapsulamiento de claves, inspirado en el criptosistema de McEliece. La invención consta de tres partes: generación de claves, cifrado (encapsulamiento de clave por parte del emisor) y descifrado (encapsulamiento de clave por parte del receptor). Como se ha explicado en los antecedentes de la invención, ésta se enmarca en lo que se conoce como Criptosistema de McEliece. Se aporta una nueva familia de códigos correctores de errores con algoritmos eficientes de decodificación. De esta forma se incrementa de forma significativa el espacio de búsqueda en este esquema de cifrado.

Figura 1



ES 2 948 323 A1

DESCRIPCIÓN

Procedimiento y dispositivo de cifrado/descifrado post-cuántico usando códigos lineales

SECTOR DE LA TÉCNICA

La presente invención se enmarca en el campo de las disposiciones para las comunicaciones secretas o protegidas utilizando un algoritmo de cifrado, en especial, de los algoritmos de clave pública, siendo imposible de invertir por computador el algoritmo de cifrado, y no exigiéndose secreto a las claves de cifrado de los utilizadores.

Concretamente, la invención está relacionada con los procedimientos generadores de códigos y particularmente, aunque no en forma exclusiva, generadores de códigos para su utilización en sistemas de cifrado asimétricos basados en de claves públicas, más concretamente en sistemas tipo McEliece.

ANTECEDENTES DE LA INVENCIÓN

En 1976, W. Diffie y M. E. Hellman proponen un nuevo tipo de criptosistema cuya principal característica es la presencia de dos claves distintas, una para el proceso de cifrado (pública) y otra para el descifrado (privada), tales que es computacionalmente difícil conocer la clave de descifrado a partir de la clave de cifrado [Whitfield Diffie y Martin Hellman. «New directions in cryptography». En: *IEEE Transactions on Information Theory* 22.6 (1976), págs. 644-654. DOI: 10.1109/TIT.1976.1055638]. Este nuevo paradigma criptográfico recibe el nombre de *criptografía asimétrica* o *criptografía de clave pública*. Los más utilizados a día de hoy son el criptosistema RSA [Ronald L. Rivest, Adi Shamir y Leonard Adleman. «A Method for Obtaining Digital Signatures and Public-Key Cryptosystems». En: *Commun. ACM* 21.2 (feb. de 1978), págs. 120-126. ISSN: 0001-0782. DOI: 10.1145/359340.359342], basado en la dificultad de factorizar enteros con varios factores primos grandes, y aquellos basados en el problema del logaritmo discreto, ya sea en el grupo de las unidades de un cuerpo primo [Taher ElGamal. «A public key cryptosystem and a signature scheme based on discrete logarithms». En: *IEEE Transactions on Information Theory* 31.4 (1985), págs. 469-472. DOI: 10.1109/TIT.1985.1057074] o en el grupo de los puntos de una curva elíptica [Victor S. Miller. «Use of Elliptic Curves in Cryptography». En: *Advances in Cryptology — CRYPTO '85 Proceedings*. Ed. por Hugh C. Williams. Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, págs. 417-426. ISBN: 978-3-540-39799-1; Neal Koblitz. «Elliptic curve cryptosystems». En: *Mathematics of Computation* 48 (1987), págs. 203-209. DOI: 10.1090/S0025-5718-1987-0866109-5]. Éstos pueden ser considerados como criptosistemas asimétricos clásicos.

Debido a la diferencia de rendimiento en los criptosistemas asimétricos frente a los simétricos, lo usual es utilizar la clave pública para cifrar una información aleatoria a partir de la cual se pueda derivar, mediante una función hash criptográficamente segura como SHA-2 o SHA-3 [Quynh Dang. *Secure Hash Standard*. en. Inf. téc. National Institute of Standards y Technology, ago. de 2015. DOI: 10.6028/NIST.FIPS.180-4], una clave de sesión. Dicha clave de sesión será utilizada en un criptosistema simétrico, por ejemplo AES con cualquiera de sus longitudes de clave [National Institute of Standards and Technology. *Advanced Encryption Standard (AES)*. Inf. téc. FIPS PUB 197. National Institute of Standards y Technology, nov. de 2001. DOI:

10.6028/NIST.FIPS.197]. Esto es lo que se conoce como *mecanismo de encapsulamiento de claves* (conocido por sus siglas KEM en inglés).

Paralelamente a la publicación de RSA, Robert McEliece propone en 1978 un criptosistema asimétrico basado en códigos correctores de errores [Robert J. McEliece. *A Public-Key Cryptosystem Based On Algebraic Coding Theory*. Inf. téc. 42–44. National Aeronautics y Space Administration, feb. de 1978]. La idea consiste en usar como clave pública la matriz generadora de un código Goppa binario suficientemente mezclada para que no sea posible deducir a partir de dicha matriz la información necesaria para decodificar. Dicha información se convierte en la clave privada. Harald Niederreiter propone [Harald Niederreiter. «Knapsack-type cryptosystems and algebraic coding theory». En: *Problems of Control and Information Theory.* 15 (1986), págs. 159-166] un criptosistema equivalente pero basado en la matriz de paridad. En realidad Niederreiter propone sustituir los códigos Goppa binarios por códigos de Reed-Solomon generalizados, aunque dicha propuesta fue rota por Sidelnikov y Shestakov en 1992 [V. M. Sidelnikov y S. O. Shestakov. «On insecurity of cryptosystems based on generalized Reed-Solomon codes». En: *Discrete Mathematics and Applications* 2.4 (1992), págs. 439-444. DOI: doi:10.1515/dma.1992.2.4.439]. La formulación de Niederreiter se considera hoy en día parte del estándar del criptosistema de McEliece [Martin R. Albrecht y col. *Classic McEliece: conservative code-based cryptography*. Inf. téc. NIST's Post-Quantum Cryptography Standardization Project, oct. de 2020. URL: https://classic.mceliece.org/].

En los últimos años, los criptosistemas basados en códigos han ganado interés por parte de la comunidad criptográfica debido a la inherente vulnerabilidad de los criptosistemas asimétricos clásicos al desarrollo de ordenadores cuánticos provocada por el algoritmo de Shor [Peter W. Shor. «Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer». En: *SIAM Review* 41.2 (1999), págs. 303-332. DOI: 10.1137/S0036144598347011].

Un ingrediente fundamental del criptosistema de McEliece es la existencia de algoritmos eficientes de decodificación para los códigos binarios de Goppa. Dichos algoritmos están soportados por estructuras aritméticas adicionales más allá de la estructura lineal. Nuestra invención también está soportada por estructuras aritméticas. Concretamente en un caso particular del concepto de polinomio de Ore [Oystein Ore. «Theory of Non-Commutative Polynomials». English. En: *Annals of Mathematics*. Second Series 34.3 (jul. de 1933), págs. 480-508. ISSN: 0003486X. DOI: 10.2307/1968173].

Dada la diferencia de rendimiento entre los criptosistemas de clave publica y los criptosistemas simétricos (tipo AES o cifrados de flujo), los primeros suelen emplearse para transmitir una clave de sesión que será empleada en un criptosistema simétrico acordado de antemano. Una forma de transmitir dicha clave es mediante un mecanismo de encapsulamiento de clave (*KEM: key encapsulation mechanism* en inglés) que funciona de la siguiente forma: el emisor genera de forma aleatoria un secreto $\mathfrak{e}$ en un cierto espacio de búsqueda suficientemente grande. Dicho secreto se envía cifrado con la clave pública del receptor. El receptor descifra el secreto usando su clave privada, por lo que ambos conocen el valor de $\mathfrak{e}$. Mediante el uso de una función hash criptográficamente segura $\mathcal{K}$ que produzca cadenas de K bits, donde K es para una longitud de la clave para el algoritmo simétrico acorado, tanto receptor como receptor pueden derivar la clave común $\mathcal{K}(\mathfrak{e})$. Ejemplos de funciones hash criptográficamente seguras son SHA-2, SHA-3 y SHAKE, con salidas entre 224 y 522 bits.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 contiene el diagrama que describe el modo de realizar la multiplicación no conmutativa en los polinomios-nc.

La Figura 2 contiene el diagrama que describe la división Euclídea a izquierda de polinomios-nc, con respecto al producto $*_h$ descrito previamente.
La Figura 3 describe el modo de obtener el coeficiente de la primera entrada al emplear algoritmo extendido de Euclides para calcular el máximo común divisor a derecha y los coeficientes de Bezout de dos polinomios-nc. Concretamente, si r es el máximo común divisor a derecha de f y g, y u, v son los polinomios-nc tales que $r = (u *_h f) + (v *_h g)$ entonces el procedimiento descrito en la Figura 3 da como salida el polinomio-nc u.
La Figura 4 contiene el diagrama que describe un procedimiento para calcular el mínimo común múltiplo a izquierda de dos polinomios-nc. Este procedimiento, como el anterior, se basa en el algoritmo extendido de Euclides para el producto $*_h$.
La Figura 5 contiene el diagrama de un procedimiento para hallar la única solución con t posiciones no nulas de la ecuación lineal $\mathfrak{s} = \mathtt{x}H_{\mathrm{pub}}^{\mathtt{T}}$ a partir de una solución cualquiera del mismo, correspondiente al algoritmo DEC.

EXPLICACIÓN DE LA INVENCIÓN

Ambiente, notación, operaciones y procedimientos básicos

Una herramienta básica en la descripción de esta invención es el concepto de cuerpo finito, objeto ampliamente utilizado en todos los procedimientos de codificación y cifrado. Por ejemplo, el espacio de mensajes en RSA es un producto de dos cuerpos primos, mientras que en los protocolos basados en el logaritmo discreto antes mencionados, los grupos utilizados son las unidades de un cuerpo primo o el conjunto de puntos de una curva elíptica sobre un cuerpo primo o un cuerpo finito binario. Además, los alfabetos de los códigos correctores de errores más utilizados son también cuerpos finitos. Una monografía de referencia sobre cuerpos finitos es la escrita por R. Lidl y H. Niederreiter [Rudolf Lidl y Harald Niederreiter. *Finite fields*. Vol. 20. Encyclopedia of mathematics and its applications. Cambridge University Press, 1997. ISBN: 0-521-39231-4]. Sea $\mathbb{F}$ el cuerpo finito de $q = p^d$ elementos, con p primo y $d > 0$ entero. Entendemos que, para la correcta realización de esta invención, es necesario disponer de una forma de representar y operar elementos de distintos cuerpos finitos. Referimos al capítulo 2 de la monografía de Lidl y Niederreiter como guía para elegir dichas representaciones. También va a ser necesario manejar extensiones $\mathbb{F} \subseteq \mathbb{L}$ de cuerpos finitos, donde $\mathbb{L}$ tiene $q^m = p^{dm}$ elementos, para cierto entero $m > 1$. Dar una extensión de cuerpos finitos supone conocer una descripción de los elementos en $\mathbb{F}$ y $\mathbb{L}$, un homomorfismo de cuerpos $\mathrm{emb} : \mathbb{F} \to \mathbb{L}$. Asociada a emb tenemos la construcción inversa $\mathrm{sec}()$ caracterizada por $\mathrm{sec}(\mathrm{emb}(a)) = a$. Dado que $\mathbb{L}$ es un espacio vectorial de dimensión m sobre $\mathbb{F}$, entendemos que disponemos de una forma de asignar a cada elemento de $\mathbb{L}$ sus coordenadas en $\mathbb{F}^m$ con respecto a una base $\mathfrak{C}$ fija. Una posible forma de construir dicha extensión de cuerpos es la siguiente: Denotaremos por $\mathbb{F}[z]$ el anillo de polinomios sobre el cuerpo $\mathbb{F}$ e indeterminada z con la operaciones usuales de suma y producto de polinomios. Entonces, $\mathbb{L} = \frac{\mathbb{F}[z]}{\langle \mathrm{pol} \rangle}$, donde $\mathrm{pol} \in \mathbb{F}[z]$ es un polinomio irreducible en $\mathbb{F}[x]$ de grado m. $\mathbb{L}$ es un $\mathbb{F}$-espacio vectorial de dimensión m y podemos considerar la base $\mathfrak{C} = \{1, z, \ldots, z^{m-1}\}$ de $\mathbb{L}$ sobre $\mathbb{F}$. Además $\mathrm{emb}()$ consiste en ver los elementos de $\mathbb{F}$ como polinomios de grado 0. Otras formas de realizar la extensión pueden consultarse en la monografía referida.
Dado un entero h con $1 \leq h < dm$, denotamos por $\mathbb{K}$ el subcuerpo de $\mathbb{L}$ formado por los elementos $c \in \mathbb{L}$ tales que $c^{p^h} = c$. Utilizaremos también la notación siguiente:

$$[p]_i = \frac{p^{ih} - 1}{p^h - 1} = 1 + p^h + p^{2h} + \cdots + p^{(i-1)h},$$

que simplificará la descripción de algunas operaciones. Dado un número racional $r \in \mathbb{Q}$, denotamos por $\lfloor r \rfloor$ al mayor entero menor o igual que r.
Denotaremos por $\mathbb{L}[x]$ al conjunto de polinomios sobre el cuerpo $\mathbb{L}$ e indeterminada x con la suma usual. Los elementos de $\mathbb{L}$ pueden considerarse como polinomios constantes en $\mathbb{L}[x]$.
Necesitaremos las siguientes operaciones:

- Producto $*_h$ en $\mathbb{L}[x]$ (Figura 1). Definido a partir de la regla $x *_h a = a^{p^h} x$ para cualquier $a \in \mathbb{L}$, este producto es un caso particular del producto de Ore [Ore, «Theory of Non-Commutative Polynomials»]. Este producto es no conmutativo. Para recalcar el uso del producto $*_h$ llamaremos a los elementos de $\mathbb{L}[x]$ *polinomios-nc*.
- Función DIV (Figura 2). Esta función realiza la división a izquierda con respecto al producto $*_h$, es decir, si $c, r = \mathrm{DIV}(f, g)$, entonces c, r son los únicos polinomios-nc tales que $f = (c *_h g) + r$, y $r = 0$ ó $\mathrm{grado}(r) < \mathrm{grado}(g)$.
- Función PCP (Figura 3). Esta función tiene como salida el coeficiente asociado a la primera entrada en el algoritmo extendido de Euclides para el cálculo del máximo común divisor a derecha y los coeficientes de Bezout con respecto al producto $*_h$, es decir, si r es el máximo común divisor a derecha de f y g, y u, v son los polinomios-nc tales que $r = (u *_h f) + (v *_h g)$ entonces el procedimiento $\mathrm{PCP}(f, g)$ da como salida el polinomio-nc u.
- Función MCM (Figura 4). Esta función devuelve el mínimo común múltiplo a izquierda con respecto al producto $*_h$.

También denotamos por $\mathcal{K}$ una función hash criptográficamente segura que actuará como función de derivación de clave.
Es este documento se usarán las siguientes notaciones respecto a conjuntos:

- $\{\}$ es el conjunto vacío, sin elementos.
- $A \cup B$ es la unión de A y B, es decir, los elementos que están en A o en B
- $A \setminus B$ es la diferencia, es decir, los elementos que están en A pero no en B.

La invención descrita en esta memoria es un criptosistema asimétrico basado en códigos correctores de errores, y usado mediante un mecanismo de encapsulamiento de claves. Es, por tanto, necesario describir el procedimiento de generación de claves, el procedimiento de cifrado y el procedimiento de descifrado.
Como se ha explicado en los antecedentes de la invención, ésta se enmarca en lo que se conoce como Criptosistema de McEliece. Se aporta una nueva familia de códigos correctores de errores con algoritmos eficientes de decodificación. De esta forma se incrementa de forma significativa el espacio de búsqueda en este esquema de cifrado.

Generación de claves

En un primer aspecto, la presente invención está relacionada con un procedimiento generación de claves para su uso en un criptosistema.
Concretamente, se describen a continuación un procedimiento para generar claves públicas, para el proceso de cifrado, y otro procedimiento para generar claves privadas, para el proceso de descifrado. Se asume emisor y receptor comparten una función hash criptográficamente segura $\mathcal{K} : \mathbb{F}^n \to \{0,1\}^K$ para una longitud de clave simétrica K a ser usada en un criptosistema simétrico. Tanto la función hash como el criptosistema simétrico pueden ser conocidos.

Así, considerando como parámetros iniciales cuatro enteros positivos n, t, p y d, de forma que p es primo y $2 \leq t \leq \frac{n}{4}$, y dado un cuerpo finito $\mathbb{F}$ con $q = p^d$ elementos, el *"procedimiento de generación de clave privada de la invención"* comprende los siguientes pasos:

- Cálculo de parámetros adicionales k, δ, m, h y μ.
  - Parámetro k: Se define como $k = n - 2t\left\lfloor \frac{n}{4t} \right\rfloor$.
  - Parámetros δ, m: Elección aleatoria de entre todos los pares de enteros positivos (δ, m) tales que

$$\text{máx}\left\{ \frac{n}{10t}, \frac{n\delta}{d(p^\delta - 1)} \right\} \leq m \leq \frac{n}{4t},\ \delta \text{ divide a } dm \text{ y } \delta < dm.$$

  - Parámetro h: Selección aleatoria de un entero h tal que $1 \leq h \leq dm$ y δ es el máximo común divisor de h y dm.
  - Parámetro μ: Se define como $\mu = \frac{dm}{\delta}$.
- Cálculo del cuerpo finito $\mathbb{L}$ a partir de $\mathbb{F}$ tal y como se describe en **Ambiente, notación, operaciones y procedimientos básicos**.
- Selección aleatoria de un elemento primitivo $\gamma \in \mathbb{L}$. Es decir, selección aleatoria de un elemento $\gamma \in \mathbb{L}$ verificando que $\gamma^{\frac{p^{dm}-1}{p_i}} \neq 1$ para cada divisor primo p_i de $p^{dm} - 1$.
- Selección aleatoria de un elemento $\alpha \in \mathbb{L}$ que genere una base normal para extensión de $\mathbb{L}$ sobre el subcuerpo invariante. Es decir, selección aleatoria de un elemento $\alpha \in \mathbb{L}$ tal que

$$\begin{vmatrix} \alpha & \alpha^{p^h} & \cdots & \alpha^{p^{(\mu-1)h}} \\ \alpha^{p^h} & \alpha^{p^{2h}} & \cdots & \alpha \\ \vdots & \vdots & & \vdots \\ \alpha^{p^{(\mu-1)h}} & \alpha & \cdots & \alpha^{p^{(\mu-2)h}} \end{vmatrix} \neq 0.$$

- Selección aleatoria de n elementos distintos $\alpha_0, \ldots, \alpha_{n-1}$ en el conjunto

$$\{\gamma^j \alpha^{p^{hi}(p^h-1)} \text{ tales que } 0 \leq j \leq p^\delta - 2, 0 \leq i \leq \mu - 1\}.$$

  Se define el conjunto de *"puntos posicionales"* como $E = [\alpha_0, \ldots, \alpha_{n-1}]$.
- Selección de forma aleatoria, con repetición o no, de n elementos no nulos en $\mathbb{L}$ para formar la lista $\eta = [\eta_0, \ldots, \eta_{n-1}]$.
- Selección aleatoria de un polinomio $g \in \mathbb{L}[x]$, que se llamará *"polinomio-nc modular"*, definido por las siguientes propiedades:
  - el grado de g es $2t$,
  - g es invariante (*twosided* en terminología inglesa) con respecto al producto $*_h$, es decir, dado cualquier polinomio-nc f, existen polinomios-nc f', f'' tales que $f *_h g = g *_h f'$ y $g *_h f = f'' *_h g$,
  - para cada $0 \leq i \leq n-1$, los máximo común divisor a izquierda y derecha de g y $x - \alpha_i$ valen 1.

  Dicho polinomio se puede calcular de la siguiente forma: denotamos $l = \left\lfloor \frac{2t}{\mu} \right\rfloor$ y $a = 2t - l\mu$. Seleccionamos l elementos $g_0, g_1, \ldots, g_{l-1}$ mediante el siguiente proceso:

I) Seleccionamos aleatoriamente l elementos $\overline{g}_0, \overline{g}_1, \ldots, \overline{g}_{l-1}$ en $\mathbb{L}$.

II) Para cada $k = 0, \ldots, l-1$, calculamos

$$g_k = \overline{g_k} + \overline{g_k}^{p^h} + \overline{g_k}^{p^{2h}} + \ldots + \overline{g_k}^{p^{(\mu-1)h}}.$$

Llamamos $g_l = 1$.

III) Si

$$\sum_{k=0}^{l} g_k \alpha_i^{[p]_{k\mu+a}} \neq 0$$

para todo $i = 1, \ldots, n$, terminamos. Si no, repetimos desde el punto I).

El polinomio-nc modular es

$$g = \sum_{k=0}^{l} g_k x^{k\mu+a} \in \mathbb{L}[x].$$

- Cálculo de *polinomios-nc de paridad*: Se calcula el conjunto de polinomios-nc $h_0, \ldots, h_{n-1}$ de forma que $h_i = \mathrm{PCP}(x - \alpha_i, g)$ para cada $i = 0, \ldots, n-1$.

Así, tras la realización de este procedimiento la clave privada objeto de la invención estará formada por los elementos:

- la extensión $\mathbb{F} \subseteq \mathbb{L}$,
- el entero h,
- la lista de puntos posicionales $E = [\alpha_0, \ldots, \alpha_{n-1}]$,
- la lista $\eta = [\eta_0, \ldots, \eta_{n-1}]$,
- el polinomio-nc modular g y
- los polinomios-nc de paridad $h_0, \ldots, h_{n-1}$.

En otro aspecto, la presente invención también se refiere a un *"procedimiento de generación de clave pública de la invención"*. Este procedimiento comprende los siguientes pasos:

- Cálculo de una matriz de paridad, H, a partir de los n polinomios-nc de paridad calculados en el procedimiento de generación de clave privada de la invención, siguiendo el siguiente procedimiento:
  (1) Para cada $0 \leq j \leq n-1$, denotamos por h_{ij} al coeficiente de grado i de h_j, es decir, $h_j = \sum_{i=0}^{2t-1} h_{ij} x^i$.
  (2) Para cada $0 \leq j \leq n-1$ y cada $0 \leq i \leq 2t-1$, se calcula $\tilde{h}_{ij} = (h_{ij})^{p^{((\mu-i) \mod \mu)h}} \eta_j$.
  (3) Para cada $0 \leq j \leq n-1$ y cada $0 \leq i \leq 2t-1$, se calculan las coordenadas de $\tilde{h}_{ij} \in \mathbb{L}$ con respecto a la base $\mathfrak{C}$, obteniendo $(h_{0,ij}, \ldots, h_{m-1,ij}) \in \mathbb{F}^m$.
  (4) Para cada $0 \leq j \leq n-1$ y cada $0 \leq i \leq 2mt-1$, se denota $H_{ij} = h_{b,aj}$, donde a y b son el cociente y el resto, respectivamente, obtenidos al dividir i entre m.
  (5) La matriz H es la matriz con $2tm$ filas, numeradas de 0 a $2tm-1$, y n columnas, numeradas de 0 a $n-1$, con valores en $\mathbb{F}$, cuyo valor en la fila i y columna j es H_{ij}.
- Cálculo de la matriz H_{pub} a partir de la matriz de paridad H siguiendo el siguiente procedimiento:

(1) Calculamos el rango r_H de H. Si $r_H = n-k$, H_{pub} es la forma escalonada reducida por filas de H y terminamos.

(2) De forma aleatoria, seleccionamos una matriz R con $n-k-r_H$ filas, n columnas y coeficientes en $\mathbb{F}$.

(3) Consideramos Q la matriz formada por las filas de H y R.

(4) Calculamos la matriz escalonada reducida por filas de Q, Q_{rref}.

(5) Fijamos como H_{pub} la matriz compuesta por las filas no nulas de Q_{rref}.

(6) Si el rango de H_{pub} es $n-k$, terminamos. Si no, repetimos el proceso desde (2).

Así, tras la realización de este procedimiento la clave pública objeto de la invención estará formada por la matriz H_{pub}.

Realizaciones preferentes en función de los parámetros iniciales:

En una realización preferente del procedimiento de generación de clave privada de la invención, el parámetro inicial p se fija en $p = 2$.

En otra realización preferente del procedimiento de generación de clave privada de la invención, el parámetro inicial p se fija en $p = 2$ y el parámetro inicial d se fija en los valores $d = 4$ o $d = 8$. De esta forma se identifican de forma unívoca los elementos de $\mathbb{F}$ con caracteres hexadecimales o con bytes respectivamente.

Procedimiento de cifrado de la invención

En otros aspecto, la invención se refiere a un procedimiento de cifrado a partir de una clave pública generada por el procedimiento de generación de clave pública de la invención, que comprende seleccionar un vector aleatorio en $\mathbb{F}^n$ con t componentes no nulas, y multiplicarlo por la traspuesta de la matriz H_{pub}.

Procedimiento de descifrado de la invención

El otro aspecto, la invención también se refiere a un procedimiento de descifrado que comprende aplicar un algoritmo de decodificación empleando la clave privada generada por el procedimiento de la invención.

En una realización particular, el procedimiento de descifrado del criptograma, $\mathfrak{s}$, cifrado usando una clave pública generada por el procedimiento de generación de clave pública de la invención, comprende resolver el sistema lineal $\mathfrak{s} = yH_{\text{pub}}^{\mathsf{T}}$ y aplicar un algoritmo de decodificación a la solución, y.

En una realización preferente, el algoritmo de decodificación empleado es el algoritmo DEC presentado a continuación (Figura 5):

Algoritmo DEC :

Entrada un vector $y = (y_0, \ldots, y_{n-1}) \in \mathbb{F}^n$

Salida un vector $\mathfrak{e} = (e_0, \ldots, e_{n-1}) \in \mathbb{F}^n$

$\mathfrak{s} \leftarrow \sum_{k=0}^{n-1} h_k *_h (\eta_k \operatorname{emb}(y_k)) \in \mathbb{L}[x]$

$r_{(0)} \leftarrow g$, $r_{(1)} \leftarrow \mathfrak{s}$, $v_{(0)} \leftarrow 0$, $v_{(1)} \leftarrow 1$

Mientras $\operatorname{grado}(r_{(1)}) \geq t$ **hacer**

$c, r \leftarrow \mathrm{DIV}(r_{(0)}, r_{(1)})$

$r_{(0)} \leftarrow r_{(1)}$, $r_{(1)} \leftarrow r$

$v_{(2)} \leftarrow v_{(0)} - (c *_h v_{(1)})$

$v_{(0)} \leftarrow v_{(1)}$, $v_{(1)} \leftarrow v_{(2)}$

$v = \sum_{k=0}^{\nu} v_k x^k \leftarrow v_{(1)}$, $r \leftarrow r_{(1)}$
$A \leftarrow \{\}$, $B \leftarrow \{0, 1, \ldots, n-1\}$
Para $0 \leq i \leq n-1$ **hacer**
  Si $\sum_{k=0}^{\nu} v_k \alpha_i^{[p]_k} = 0$ **entonces**
    $A \leftarrow A \cup \{i\}$, $B \leftarrow B \setminus \{i\}$
Mientras $\mathrm{grado}(v) > \mathrm{Cardinal}(A)$ **hacer**
  $f \leftarrow v$, $gr \leftarrow \mathrm{grado}(f)$
  $i \leftarrow$ menor entero en B
  $B \leftarrow B \setminus \{i\}$
  $f \leftarrow \mathrm{MCM}(f, x - \alpha_i)$
  Mientras $\mathrm{grado}(f) > gr$ **hacer**
    $gr \leftarrow gr + 1$
    $i \leftarrow$ menor entero en B
    $B \leftarrow B \setminus \{i\}$
    $f \leftarrow \mathrm{MCM}(f, x - \alpha_i)$
  $A \leftarrow A \cup \{i\}$, $B \leftarrow \{0, 1, \ldots, n-1\} \setminus A$
  $\overline{v} \leftarrow \mathrm{MCM}(v, x - \alpha_i)$
  $c, u \leftarrow \mathrm{DIV}(\overline{v}, v)$
  $v \leftarrow \overline{v}$, $\overline{r} \leftarrow c *_h r$, $r \leftarrow \overline{r}$
  Para $i \in B$ **hacer**
    Si $\sum_{k=0}^{\nu} v_k \alpha_i^{[p]_k} = 0$ **entonces**
      $A \leftarrow A \cup \{i\}$, $B \leftarrow B \setminus \{i\}$
$\tau \leftarrow \mathrm{Cardinal}(A)$
Denotamos $A = \{i_1, i_2, \ldots, i_\tau\}$ con $i_1 < i_2 < \ldots < i_\tau$.
Para $j \in A$ **hacer**
  $\rho_j = \sum_{k=0}^{\tau-1} \rho_{j,k} x^k$, $u_j \leftarrow \mathrm{DIV}(v, x - \alpha_j)$
Resolver el sistema lineal

$$\begin{pmatrix} (r_0)^{a_0} \\ (r_1)^{a_1} \\ \vdots \\ (r_{\tau-1})^{a_{\tau-1}} \end{pmatrix} = \begin{pmatrix} (\rho_{i_1,0})^{a_0}\eta_{i_1} & (\rho_{i_2,0})^{a_0}\eta_{i_2} & \cdots & (\rho_{i_\tau,0})^{a_0}\eta_{i_\tau} \\ (\rho_{i_1,1})^{a_1}\eta_{i_1} & (\rho_{i_2,1})^{a_1}\eta_{i_2} & \cdots & (\rho_{i_\tau,1})^{a_1}\eta_{i_\tau} \\ \vdots & \vdots & \ddots & \vdots \\ (\rho_{i_1,\tau-1})^{a_{\tau-1}}\eta_{i_1} & (\rho_{i_2,\tau-1})^{a_{\tau-1}}\eta_{i_2} & \cdots & (\rho_{i_\tau,\tau-1})^{a_{\tau-1}}\eta_{i_\tau} \end{pmatrix} \begin{pmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_\tau} \end{pmatrix},$$

donde $a_i = p^{h(\mu-i) \bmod \mu}$ para $0 \leq i < \tau$ y $r = \sum_{k=0}^{\tau-1} r_i x^i$. Si el grado de r es menor que $\tau - 1$, los coeficientes hasta grado $\tau - 1$ se considerarán nulos.
Devolver $(\overline{e}_0, \ldots, \overline{e}_{n-1}) \in \mathbb{F}^n$, donde $\overline{e}_i = \begin{cases} \sec(e_i), & \text{si } i \in A, \\ 0 & \text{en otro caso} \end{cases}$, para $i = 0, \ldots, n-1$.

Sistemas y aparatos de la invención

En otro aspecto, la presente invención también contempla los aparatos y sistemas que permiten llevar a cabo los procedimientos previamente descritos. Un claro ejemplo de aparato es un ordenador.

Así, es objeto de la invención un sistema o aparato apto para el proceso de datos que comprende los medios necesarios para llevar a cabo los lleve a cabo alguno de los procedimientos de la invención: Procedimientos de generación de clave pública o privada, procedimiento de cifrado o procedimiento de descifrado.

Más concretamente, se consideran objeto de la invención los siguientes sistemas y aparatos:

- Un sistema o un aparato apto para el procesado de datos que comprende los medios necesarios para llevar a cabo los siguientes pasos:

- Medios para introducir en el sistema/aparato los parámetros iniciales n, t, p y d, enteros positivos, de forma que p es primo y $2 \leq t \leq \frac{n}{4}$.
- Medios para generar un cuerpo finito $\mathbb{F}$ con p^d elementos.
- Medios para calcular los parámetros adicionales k, δ, m, h y μ.
- Medios para calcular el cuerpo finito $\mathbb{L}$ como extensión de $\mathbb{F}$.
- Medios para llevar a cabo una selección aleatoria de un elemento primitivo $\gamma \in \mathbb{L}$, una selección aleatoria de un elemento $\alpha \in \mathbb{L}$ que genere una base normal para extensión de $\mathbb{L}$ sobre el subcuerpo invariante, una selección aleatoria de n elementos distintos $\alpha_0, \ldots, \alpha_{n-1}$ en el conjunto

$$\{\gamma^j \alpha^{p^{hi}(p^h-1)} \text{ tales que } 0 \leq j \leq p^\delta - 2, 0 \leq i \leq \mu - 1\},$$

  y una selección de forma aleatoria, con repetición o no, de n elementos no nulos en $\mathbb{L}$ para formar la lista $\eta = [\eta_0, \ldots, \eta_{n-1}]$.
- Medios para seleccionar de forma aleatoria un polinomio-nc modular $g \in \mathbb{L}[x]$ definido por las siguientes propiedades:
  - el grado de g es $2t$,
  - g es invariante (*twosided* en terminología inglesa) con respecto al producto $*_h$, es decir, dado cualquier polinomio-nc f, existen polinomios-nc f', f'' tales que $f *_h g = g *_h f'$ y $g *_h f = f'' *_h g$,
  - para cada $0 \leq i \leq n-1$, los máximo común divisor a izquierda y derecha de g y $x - \alpha_i$ valen 1.
- Medios para calcular los *polinomios-nc de paridad* $h_0, \ldots, h_{n-1}$ de forma que $h_i = \mathrm{PCP}(x - \alpha_i, g)$ para cada $i = 0, \ldots, n-1$.
- Medios para proporcionar como salida la siguiente información que da lugar a una clave privada:
  - la extensión $\mathbb{F} \subseteq \mathbb{L}$,
  - el entero h,
  - la lista de puntos posicionales $E = [\alpha_0, \ldots, \alpha_{n-1}]$,
  - la lista $\eta = [\eta_0, \ldots, \eta_{n-1}]$,
  - el polinomio-nc modular g y
  - los polinomios-nc de paridad $h_0, \ldots, h_{n-1}$.

- Un sistema o un aparato apto para el procesado de datos que comprende los medios necesarios para llevar a cabo los siguientes pasos:
  - Medios para introducir en el sistema/aparato los siguientes datos: los parámetros n, t, p, d, k, δ, m, h y μ; la extensión $\mathbb{F} \subseteq \mathbb{L}$, y los polinomios-nc de paridad $h_0, \ldots, h_{n-1}$.
  - Medios para realizar el cálculo de una matriz de paridad, H, a partir de los n polinomios-nc de paridad siguiendo el siguiente procedimiento:
    (1) Para cada $0 \leq j \leq n-1$, denotamos por h_{ij} al coeficiente de grado i de h_j, es decir, $h_j = \sum_{i=0}^{2t-1} h_{ij} x^i$.
    (2) Para cada $0 \leq j \leq n-1$ y cada $0 \leq i \leq 2t-1$, se calcula $\tilde{h}_{ij} = (h_{ij})^{p^{((\mu-i) \bmod \mu)h}} \eta_j$.
    (3) Para cada $0 \leq j \leq n-1$ y cada $0 \leq i \leq 2t-1$, se calculan las coordenadas de $\tilde{h}_{ij} \in \mathbb{L}$ con respecto a la base $\mathfrak{C}$, obteniendo $(h_{0,ij}, \ldots, h_{m-1,ij}) \in \mathbb{F}^m$.
    (4) Para cada $0 \leq j \leq n-1$ y cada $0 \leq i \leq 2mt-1$, se denota $H_{ij} = h_{b,aj}$, donde a y b son el cociente y el resto, respectivamente, obtenidos al dividir i entre m.

(5) La matriz H es la matriz con $2tm$ filas, numeradas de 0 a $2tm-1$, y n columnas, numeradas de 0 a $n-1$, con valores en $\mathbb{F}$, cuyo valor en la fila i y columna j es H_{ij}.

- Medios para calcular la matriz H_{pub} a partir de la matriz de paridad H siguiendo el siguiente procedimiento:
  (1) Calculamos el rango r_H de H. Si $r_H = n-k$, H_{pub} es la forma escalonada reducida por filas de H y terminamos.
  (2) De forma aleatoria, seleccionamos una matriz R con $n-k-r_H$ filas, n columnas y coeficientes en $\mathbb{F}$.
  (3) Consideramos Q la matriz formada por las filas de H y R.
  (4) Calculamos la matriz escalonada reducida por filas de Q, Q_{rref}.
  (5) Fijamos como H_{pub} la matriz compuesta por las filas no nulas de Q_{rref}.
  (6) Si el rango de H_{pub} es $n-k$, terminamos. Si no, repetimos desde (2).
- Medios para proporcionar como salida la matriz H_{pub} que da lugar a la clave pública asociada a la clave privada anterior.

- Un sistema o un aparato apto para el procesado de datos que comprende los medios necesarios para llevar a cabo un procedimiento de cifrado a partir de una clave pública realizando los siguientes pasos:
  - Medios para introducir en el sistema/aparato los siguientes datos: los parámetros n, t, p y d; el cuerpo $\mathbb{F}$, y la matriz H_{pub}.
  - Medios para seleccionar un vector aleatorio $\mathfrak{e}$ en $\mathbb{F}^n$ con t componentes no nulas.
  - Medios para calcular el producto del vector $\mathfrak{e}$ por la traspuesta de la matriz H_{pub}, produciendo el criptograma $\mathfrak{s}$.
  - Medios para proporcionar como salida el criptograma $\mathfrak{s}$.

- Un sistema o un aparato apto para el procesado de datos que comprende los medios necesarios para llevar a cabo un procedimiento de descifrado a partir de una clave privada realizando los siguientes pasos:
  - Medios para introducir en el sistema/aparato los siguientes datos: los parámetros n, t, p, d, k, δ, m, h y μ; la extensión $\mathbb{F} \subseteq \mathbb{L}$; los puntos posicionales $E = [\alpha_0, \ldots, \alpha_{n-1}]$; la lista $\eta = [\eta_0, \ldots, \eta_{n-1}]$; el polinomio-nc modular g y los polinomios-nc de paridad $h_0, \ldots, h_{n-1}$.
  - Medios para resolver el sistema lineal $\mathfrak{s} = yH_{\text{pub}}^{\mathrm{T}}$.
  - Medios para aplicar el algoritmo de decodificación DEC a la solución y, obteniendo el vector $\mathfrak{e}$.
  - Medios para proporcionar como salida el vector $\mathfrak{e}$.

IMPLEMENTACIÓN DE LOS PROCEDIMIENTOS DE LA INVENCIÓN

En otro aspecto, la invención se refiere a los programas de ordenador que comprenden instrucciones para hacer que un ordenador, o un sistema o aparato apto para el procesado de datos, lleve a cabo alguno de los procedimientos de la invención (Procedimientos de generación de clave pública o privada, procedimiento de cifrado, procedimiento de descifrado) cuando se carga en dicho ordenador, sistema o aparato apto para el proceso de datos.

La invención abarca programas de ordenador que pueden estar en forma de código fuente, de código objeto o en un código intermedio entre código fuente y código objeto, tal como en forma parcialmente compilada, o en cualquier otra forma adecuada para usar en la implementación de los procesos de acuerdo con la invención. En particular, los programas de ordenador también abarcan aplicaciones en la nube que implementen alguno de los procedimientos de la invención.

Estos programas pueden estar dispuestos sobre o dentro de un soporte apto para su lectura, en adelante, "medio portador" o "portador". El medio portador puede ser cualquier entidad o dispositivo capaz de portar el programa. Cuando el programa va incorporado en una señal que puede ser transportada directamente por un cable u otro dispositivo o medio, el medio portador puede estar constituido por dicho cable u otro dispositivo o medio. Como variante, el medio portador podría ser un circuito integrado en el que va incluido el programa, estando el circuito integrado adaptado para ejecutar, o para ser utilizado en la ejecución de, los procesos correspondientes.

A modo de ejemplo, los programas podrían estar incorporados en un medio de almacenamiento, como una memoria ROM, una memoria CD ROM o una memoria ROM de semiconductor, una memoria USB, o un soporte de grabación magnética, por ejemplo, un disco flexible o un disco duro. Alternativamente, los programas podrían estar soportados en una señal portadora transmisible. Por ejemplo, podría tratarse de una señal eléctrica u óptica que podría transportarse a través de cable eléctrico u óptico, por radio o por cualesquiera otros medios.

En este sentido, otro objeto de la invención es un medio de almacenamiento legible por un ordenador que comprende instrucciones de programa capaces de hacer que un ordenador o un sistema o aparato apto para el procesado de datos lleve a cabo alguno de los procedimientos de la invención cuando se carga en dicho ordenador, sistema o aparato apto para el proceso de datos.

Finalmente, un último objeto de la invención se refiere a una señal transmisible que comprende instrucciones de programa capaces de hacer que un ordenador o un sistema o aparato apto para el procesado de datos lleve a cabo alguno de los procedimientos de la invención cuando se carga en dicho ordenador, sistema o aparato apto para el proceso de datos.

REALIZACIÓN PREFERENTE DE LA INVENCIÓN

A continuación se describe una implementación de un ejemplo de juguete de cómo seleccionar las claves del criptosistema, el proceso de cifrado y el proceso de descifrado. Se ha implementado en una Notebook de Jupyter del sistema algebraico computacional Sagemath (Python) en un ordenador con procesador Intel Core i7 de doble núcleo a 3GHz bajo el sistema operativo macOS Big Sur versión 11.6.

1. Selección de parámetros básicos. Para nuestro ejemplo trabajaremos sobre $\mathbb{F}$, el cuerpo finito de 16 elementos (esto es, $p = 2$ y $d = 4$), $n = 16$ y $t = 2$. Denotamos por a un generador de $\mathbb{F}$ verificando que $a^4 + a + 1 = 0$. Los elementos de $\mathbb{F}$ se representan, por tanto, como polinomios en a de grado menor que 4, es decir, un elemento de $\mathbb{F}$ viene determinado por una cadena de 4 bits, o un carácter hexadecimal. Utilizaremos caracteres hexadecimales para etiquetar los elementos de $\mathbb{F}$ según el siguiente esquema: $a^3 + a + 1 = 1011 = \texttt{B}$.

   En este caso, dado el reducido tamaño de la clave pública, la única posibilidad es considerar $m = 2$ y $\delta = 4$. Para claves de mayor tamaño, se seleccionaría aleatoriamente un par de valores (m, δ) entre todos los posibles casos. Por ejemplo, con parámetros $n = 4096$ y $t = 30$, el conjunto de pares posibles es

(14, 14), (14, 28), (15, 10), (15, 12), (15, 15), (15, 20), (15, 30), (16, 16), (16, 32), (17, 17), (17, 34), (18, 12), (18, 18), (18, 24), (18, 36), (19, 19), (19, 38), (20, 10), (20, 16), (20, 20), (20, 40), (21, 12), (21, 14), (21, 21), (21, 28), (21, 42), (22, 11), (22, 22), (22, 44), (23, 23), (23, 46), (24, 12), (24, 16), (24, 24), (24, 32), (24, 48), (25, 10), (25, 20), (25, 25), (25, 50), (26, 13), (26, 26), (26, 52), (27, 9), (27, 12), (27, 18), (27, 27), (27, 36), (27, 54), (28, 14), (28, 16), (28, 28), (28, 56), (29, 29), (29, 58), (30, 10), (30, 12), (30, 15), (30, 20), (30, 24), (30, 30), (30, 40), (30, 60), (31, 31), (31, 62), (32, 16), (32, 32), (32, 64), (33, 11), (33, 12), (33, 22), (33, 33), (33, 44), (33, 66), (34, 8), (34, 17), (34, 34), (34, 68)

Para h seleccionamos aleatoriamente $h = 4$ y, por tanto, $\mu = 2$. Para el cálculo de la extensión $\mathbb{L}$, seleccionamos aleatoriamente un polinomio irreducible en $\mathbb{F}$, $\mathrm{pol} = x^2 + \mathtt{F}x + \mathtt{B}$, entonces $\mathbb{L} = \frac{\mathbb{F}[x]}{\langle \mathrm{pol} \rangle}$. Denotamos por b a una raíz de pol, por lo que los elementos de $\mathbb{L}$ pueden ser representados como polinomios en b de grado menor que 2 y con coeficientes en $\mathbb{F}$.

2. Elemento primitivo. Seleccionamos aleatoriamente $\gamma = \mathtt{B}b + 2$, un elemento primitivo de $\mathbb{L}$.

3. Base normal. Seleccionamos aleatoriamente $\alpha = 9b + 8 \in \mathbb{L}$.

4. Puntos posicionales. De forma aleatoria seleccionamos 16 elementos de $\mathbb{L}$:

$$\begin{aligned} \alpha_0 &= 4b + 5 & \alpha_1 &= 1b + \mathtt{F} \\ \alpha_2 &= 8b + 3 & \alpha_3 &= 3b + \mathtt{D} \\ \alpha_4 &= 3b + 7 & \alpha_5 &= 9 \\ \alpha_6 &= 8b + \mathtt{B} & \alpha_7 &= 3b + \mathtt{A} \\ \alpha_8 &= 4b + 9 & \alpha_9 &= 5b + 2 \\ \alpha_{10} &= \mathtt{C}b + 6 & \alpha_{11} &= 7b + 6 \\ \alpha_{12} &= 2b + 4 & \alpha_{13} &= \mathtt{A}b + \mathtt{B} \\ \alpha_{14} &= \mathtt{C}b + 1 & \alpha_{15} &= 1b + 1 \end{aligned}$$

5. Elementos. De forma aleatoria seleccionamos 16 elementos no nulos

$$\begin{aligned} \eta_0 &= \mathtt{F}b + \mathtt{D} & \eta_1 &= 5b + \mathtt{F} \\ \eta_2 &= 1b + 9 & \eta_3 &= 3b + 4 \\ \eta_4 &= 3b + 4 & \eta_5 &= 1b + \mathtt{D} \\ \eta_6 &= 4b + \mathtt{F} & \eta_7 &= 7b + \mathtt{B} \\ \eta_8 &= 7b & \eta_9 &= 2b + 8 \\ \eta_{10} &= \mathtt{D}b + \mathtt{F} & \eta_{11} &= 9b + 7 \\ \eta_{12} &= 2b + 6 & \eta_{13} &= \mathtt{A}b + \mathtt{B} \\ \eta_{14} &= 3b + 6 & \eta_{15} &= \mathtt{A}b + 8 \end{aligned}$$

6. Calculamos un polinomio g nc-modular

$$g = x^4 + 7x^2 + 9 \in \mathbb{L}[x].$$

7. Calculamos los polinomios-nc de paridad

$$
\begin{aligned}
h_0 &= 2x^3 + (8b + \mathtt{B})\, x^2 \\
h_1 &= \mathtt{D}x^3 + \mathtt{D}bx^2 + 3x + 3b \\
h_2 &= \mathtt{D}x^3 + (2b + 9)\, x^2 + 3x + \mathtt{B}b + 6 \\
h_3 &= 8x^3 + (\mathtt{B}b + 1)\, x^2 + 8x + \mathtt{B}b + 1 \\
h_4 &= 3x^3 + (5b + \mathtt{F})\, x^2 + x + 3b + 5 \\
h_5 &= 9x^3 + \mathtt{D}x^2 + 5x + \mathtt{B} \\
h_6 &= \mathtt{F}x^3 + (b + \mathtt{C})\, x^2 + x + 8b + \mathtt{A} \\
h_7 &= 3x^3 + (5b + \mathtt{B})\, x^2 + 8x + \mathtt{B}b + \mathtt{C} \\
h_8 &= 3x^3 + \mathtt{C}bx^2 + 8x + 6b \\
h_9 &= 9x^3 + (\mathtt{B}b + 2)\, x^2 + 5x + 2b + 7 \\
h_{10} &= 8x^3 + (\mathtt{A}b + 9)\, x^2 + 5x + 9b + 3 \\
h_{11} &= 2x^3 + (\mathtt{E}b + 9)\, x^2 \\
h_{12} &= \mathtt{F}x^3 + (\mathtt{D}b + \mathtt{E})\, x^2 + \mathtt{A}x + 7b + 5 \\
h_{13} &= \mathtt{B}x^3 + (2b + 4)\, x^2 + \mathtt{A}x + 8b + 3 \\
h_{14} &= 9x^3 + (6b + \mathtt{D})\, x^2 + \mathtt{F}x + 8b + \mathtt{E} \\
h_{15} &= \mathtt{E}x^3 + (\mathtt{E}b + \mathtt{B})\, x^2 + \mathtt{F}x + \mathtt{F}b + 5
\end{aligned}
$$

8. Matriz de paridad. De los coeficientes de los polinomios de paridad obtenemos los coeficientes $\tilde{h}_{ij}$, que representamos mediante la siguiente matriz, con coeficientes en $\mathbb{L}$,

$$
\left(\begin{array}{cccccccc|}
0 & 8b+3 & 9b+\mathtt{A} & \mathtt{C}b+\mathtt{C} & 5b+6 & \mathtt{B}b+6 & \mathtt{B}b+3 & 2b+7 \\
0 & \mathtt{F}b+2 & 3b+8 & \mathtt{B}b+6 & 3b+4 & 5b+\mathtt{C} & 4b+\mathtt{F} & \mathtt{D}b+7 \\
\mathtt{E}b+\mathtt{D} & \mathtt{F}b+\mathtt{D} & 5b+8 & \mathtt{C}b+\mathtt{C} & \mathtt{F}b+\mathtt{A} & \mathtt{D}b+\mathtt{E} & 3b+2 & 4b+\mathtt{E} \\
\mathtt{D}b+9 & \mathtt{C}b+7 & \mathtt{D}b+\mathtt{F} & \mathtt{B}b+6 & 5b+\mathtt{C} & 9b+\mathtt{F} & 9b+\mathtt{A} & 9b+\mathtt{E}
\end{array}\right|
$$

$$
\left|\begin{array}{cccccccc}
\mathtt{F}b+\mathtt{B} & 4b+7 & 1 & 0 & \mathtt{E}b+5 & \mathtt{D} & 7b+\mathtt{B} & \mathtt{D}b+3 \\
\mathtt{D}b & \mathtt{A}b+\mathtt{E} & \mathtt{C}b+6 & 0 & 7b+9 & 8b+2 & 2b+4 & \mathtt{C}b+1 \\
\mathtt{D}b+5 & 5b+2 & 7 & \mathtt{A}b+\mathtt{E} & 9b+\mathtt{E} & \mathtt{E} & \mathtt{F}b+\mathtt{A} & \mathtt{F}b+8 \\
9b & b+4 & 2b+1 & b+\mathtt{E} & \mathtt{D}b+4 & 2b+9 & 8b+3 & 6b+9
\end{array}\right)
$$

Expandiendo a coeficientes en $\mathbb{F}$ obtenemos la matriz de paridad

$$
H = \begin{pmatrix}
0 & 3 & \mathtt{A} & \mathtt{C} & 6 & 6 & 3 & 7 & \mathtt{B} & 7 & 1 & 0 & 5 & \mathtt{D} & \mathtt{B} & 3 \\
0 & 8 & 9 & \mathtt{C} & 5 & \mathtt{B} & \mathtt{B} & 2 & \mathtt{F} & 4 & 0 & 0 & \mathtt{E} & 0 & 7 & \mathtt{D} \\
0 & 2 & 8 & 6 & 4 & \mathtt{C} & \mathtt{F} & 7 & 0 & \mathtt{E} & 6 & 0 & 9 & 2 & 4 & 1 \\
0 & \mathtt{F} & 3 & \mathtt{B} & 3 & 5 & 4 & \mathtt{D} & \mathtt{D} & \mathtt{A} & \mathtt{C} & 0 & 7 & 8 & 2 & \mathtt{C} \\
\mathtt{D} & \mathtt{D} & 8 & \mathtt{C} & \mathtt{A} & \mathtt{E} & 2 & \mathtt{E} & 5 & 2 & 7 & \mathtt{E} & \mathtt{E} & \mathtt{E} & \mathtt{A} & 8 \\
\mathtt{E} & \mathtt{F} & 5 & \mathtt{C} & \mathtt{F} & \mathtt{D} & 3 & 4 & \mathtt{D} & 5 & 0 & \mathtt{A} & 9 & 0 & \mathtt{F} & \mathtt{F} \\
9 & 7 & \mathtt{F} & 6 & \mathtt{C} & \mathtt{F} & \mathtt{A} & \mathtt{E} & 0 & 4 & 1 & \mathtt{E} & 4 & 9 & 3 & 9 \\
\mathtt{D} & \mathtt{C} & \mathtt{D} & \mathtt{B} & 5 & 9 & 9 & 9 & 9 & 1 & 2 & 1 & \mathtt{D} & 2 & 8 & 6
\end{pmatrix}
$$

9. Cálculo de la clave pública. Puesto que $k = 8$ y el rango de H es $n - k = 8$, la clave

pública H_{pub} es simplemente la forma escalonada reducida por filas de H, es decir,

$$H_{\text{pub}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & C & 2 & 3 & 2 & 9 & 9 & A & 4 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 9 & 1 & A & C & 7 & 3 & 8 & 6 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & A & 8 & 2 & 4 & D & 6 & 5 & B \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 9 & 0 & 1 & 3 & B & 7 & 8 & 9 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & E & 9 & B & C & F & 2 & 6 & 6 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & A & B & 1 & 6 & 9 & 1 & 1 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 3 & F & 1 & 2 & F & B & E & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & A & D & 8 & 6 & 4 & 1 & 2 & B \end{pmatrix}$$

10. Seleccionamos aleatoriamente el secreto compartido, un vector $\mathfrak{e} \in \mathbb{F}^{16}$ con $t = 2$ componentes no nulas,

$$(4, 0, 0, 0, 0, 0, 0, 0, 0, C, 0, 0, 0, 0, 0, 0).$$

En este caso, las componentes no nulas corresponden con las posiciones 0 y 9.

11. Cifrado. Ciframos el mensaje multiplicando por la transpuesta de la matriz H_{pub} y obteniendo un mensaje cifrado

$$\mathfrak{s} = (F, C, A, 0, 6, D, 8, 3) \in \mathbb{F}^8.$$

12. Descifrado. El receptor resuelve el sistema lineal $\mathfrak{s} = yH_{\text{pub}}^{\mathrm{T}}$ obteniendo, por ejemplo,

$$y = (F, C, A, 0, 6, D, 8, 3, 0, 0, 0, 0, 0, 0, 0, 0).$$

Aplicando el algoritmo $\mathrm{DEC}()$ a y, obtenemos el vector $\mathfrak{e}$, descifrando el mensaje.

REIVINDICACIONES

1. Procedimiento de generación de clave privada que comprende los siguientes pasos:

   - Selección parámetros iniciales n, t, p y d enteros positivos, de forma que p es primo y $2 \leq t \leq \frac{n}{4}$.
   - Generación de un cuerpo finito $\mathbb{F}$ con $q = p^d$ elementos.
   - Cálculo de parámetros adicionales k, δ, m, h y μ.
     - Parámetro k: Se define como $k = n - 2t \left\lfloor \frac{n}{4t} \right\rfloor$.
     - Parámetros δ, m: Elección aleatoria de entre todos los pares de enteros positivos (δ, m) tales que

       $$\text{máx}\left\{ \frac{n}{10t}, \frac{n\delta}{d(p^\delta - 1)} \right\} \leq m \leq \frac{n}{4t},\ \delta \text{ divide a } dm \text{ y } \delta < dm.$$

     - Parámetro h: Selección aleatoria de un entero h tal que $1 \leq h \leq dm$ y δ es el máximo común divisor de h y dm.
     - Parámetro μ: Se define como $\mu = \frac{dm}{\delta}$.
   - Cálculo del cuerpo finito $\mathbb{L}$ como extensión de $\mathbb{F}$.
   - Selección, de forma aleatoria, de un elemento primitivo $\gamma \in \mathbb{L}$.
   - Selección aleatoria de un elemento $\alpha \in \mathbb{L}$ que genere una base normal para extensión de $\mathbb{L}$ sobre el subcuerpo invariante.
   - Selección, de forma aleatoria, de los n elementos distintos $E = [\alpha_0, \ldots, \alpha_{n-1}]$ en el conjunto $\{\gamma^j \alpha^{p^{hi}(p^h-1)}$ tales que $0 \leq j \leq p^\delta - 2, 0 \leq i \leq \mu - 1\}$.
   - Selección de forma aleatoria, con repetición o no, de n elementos no nulos en $\mathbb{L}$ para formar la lista $\eta = [\eta_0, \ldots, \eta_{n-1}]$.
   - Selección aleatoria de un polinomio-nc modular $g \in \mathbb{L}[x]$ definido por las siguientes propiedades:
     - el grado de g es $2t$,
     - g cumple la siguiente propiedad: dado cualquier polinomio-nc f, existen polinomios-nc f', f'' tales que $f *_h g = g *_h f'$ y $g *_h f = f'' *_h g$,
     - para cada $0 \leq i \leq n-1$, los máximo común divisor a izquierda y derecha de g y $x - \alpha_i$ valen 1.
   - Cálculo de polinomios-nc de paridad: Se calculan los polinomios-nc $h_0, \ldots, h_{n-1}$ de forma que $h_i = \text{PCP}(x - \alpha_i, g)$ para cada $i = 0, \ldots, n-1$.

2. Procedimiento según reivindicación 1 en el que en una realización preferente del procedimiento de generación de clave pública de la invención, $p = 2$.

3. Procedimiento según reivindicación 2 en el que $d = 4$ o $d = 8$.

4. Clave privada formada por los siguientes elementos obtenibles según cualquiera de las reivindicaciones 1 a 3: la extensión $\mathbb{F} \subseteq \mathbb{L}$, el entero h, la lista de puntos posicionales $E = [\alpha_0, \ldots, \alpha_{n-1}]$, la lista $\eta = [\eta_0, \ldots, \eta_{n-1}]$, el polinomio-nc modular g y los polinomios-nc de paridad $h_0, \ldots, h_{n-1}$.

5. Procedimiento de generación de la clave pública consistente en la matriz H_{pub} que comprende el cálculo de la matriz de paridad H a partir de los polinomios de paridad que forman parte de la clave privada y, a partir de ella, el cálculo de la matriz H_{pub} según el procedimiento siguiente:

- Cálculo de una matriz de paridad, H, a partir de los n polinomios-nc de paridad calculados en el procedimiento de generación de clave privada de la invención, siguiendo el siguiente procedimiento:
  (1) Para cada $0 \leq j \leq n-1$, denotamos por h_{ij} al coeficiente de grado i de h_j, es decir, $h_j = \sum_{i=0}^{2t-1} h_{ij} x^i$.
  (2) Para cada $0 \leq j \leq n-1$ y cada $0 \leq i \leq 2t-1$, se calcula $\tilde{h}_{ij} = (h_{ij})^{p^{((\mu-i) \mod \mu)h}} \eta_j$.
  (3) Para cada $0 \leq j \leq n-1$ y cada $0 \leq i \leq 2t-1$, se calculan las coordenadas de $\tilde{h}_{ij} \in \mathbb{L}$ con respecto a la base $\mathfrak{C}$, obteniendo $(h_{0,ij}, \ldots, h_{m-1,ij}) \in \mathbb{F}^m$.
  (4) Para cada $0 \leq j \leq n-1$ y cada $0 \leq i \leq 2mt-1$, se denota $H_{ij} = h_{b,aj}$, donde a y b son el cociente y el resto, respectivamente, obtenidos al dividir i entre m.
  (5) La matriz H es la matriz con $2tm$ filas, numeradas de 0 a $2tm-1$, y n columnas, numeradas de 0 a $n-1$, con valores en $\mathbb{F}$, cuyo valor en la fila i y columna j es H_{ij}.
- Cálculo de la matriz H_{pub} a partir de la matriz de paridad H siguiendo el siguiente procedimiento:
  (1) Calculamos el rango r_H de H. Si $r_H = n-k$, H_{pub} es la forma escalonada reducida por filas de H y terminamos.
  (2) De forma aleatoria, seleccionamos una matriz R con $n-k-r_H$ filas, n columnas y coeficientes en $\mathbb{F}$.
  (3) Consideramos Q la matriz formada por las filas de H y R.
  (4) Calculamos la matriz escalonada reducida por filas de Q, Q_{rref}.
  (5) Fijamos como H_{pub} la matriz compuesta por las filas no nulas de Q_{rref}.
  (6) Si el rango de H_{pub} es $n-k$, terminamos. Si no, repetimos desde (2).

6. Clave pública, H_{pub}, obtenible por el procedimiento según reivindicación 5.

7. Procedimiento de cifrado a partir de una clave pública generada por el procedimiento según la reivindicación 4, que comprende seleccionar un vector aleatorio en $\mathbb{F}^n$ con t componentes no nulas, y multiplicarlo por la traspuesta de la matriz H_{pub}.

8. Procedimiento de descifrado que comprende aplicar un algoritmo de decodificación empleando la clave privada generada por el procedimiento de la invención.

9. Procedimiento de descifrado, a partir de una clave privada generada según cualquiera de las reivindicaciones 1 a 3, de un criptograma cifrado a partir de una clave pública generada por el procedimiento según la reivindicación 4, que comprende resolver el sistema lineal $\mathfrak{s} = yH_{\text{pub}}^{\mathrm{T}}$ y aplicar un algoritmo de decodificación a la solución.

10. Procedimiento, según reivindicación anterior, en el que el algoritmo de decodificación aplicado a la solución es el algoritmo DEC.

11. Programa de ordenador que comprende instrucciones para hacer que un ordenador lleve a cabo cualquiera de los procedimientos según reivindicaciones 1 a 10.

12. Medio de almacenamiento legible por un ordenador que comprende instrucciones de programa capaces de hacer que un ordenador lleve a cabo cualquiera de los procedimientos según reivindicaciones 1 a 10.

13. Señal transmisible que comprende instrucciones de programa capaces de hacer que un ordenador lleve a cabo cualquiera de los procedimientos según reivindicaciones 1 a 10.

Figura 1: Producto $*_h$ en $\mathbb{L}[x]$

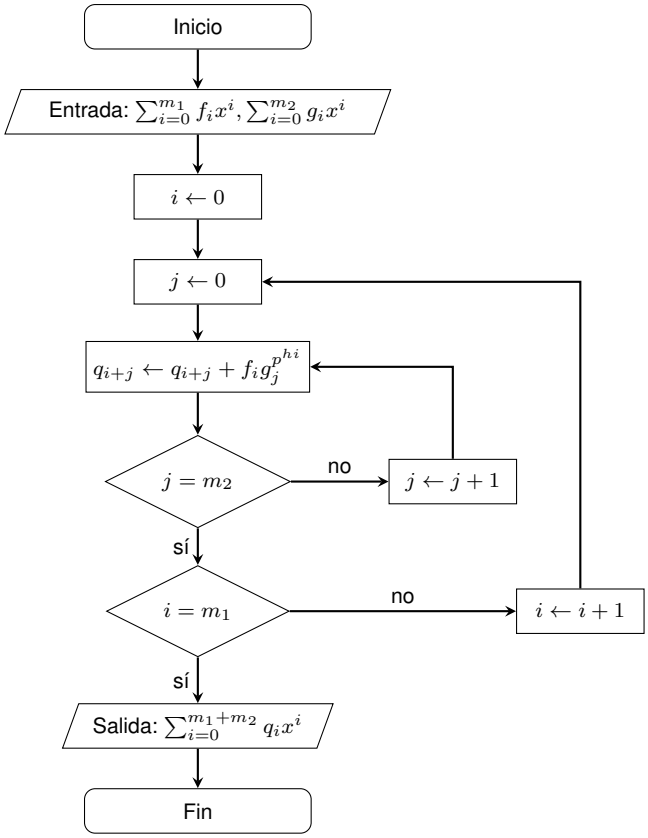


Figura 2: $\mathrm{DIV}(f, g)$

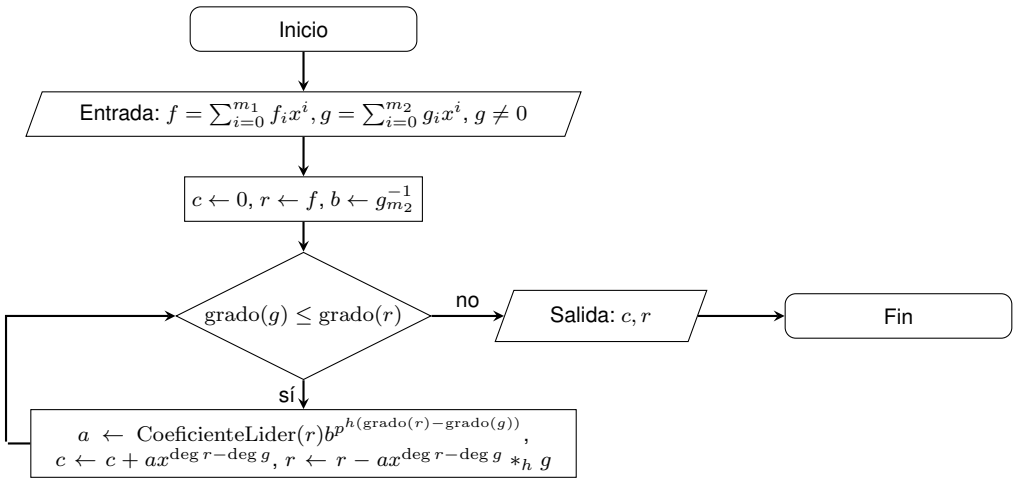


Figura 3: $\mathrm{PCP}(f, g)$

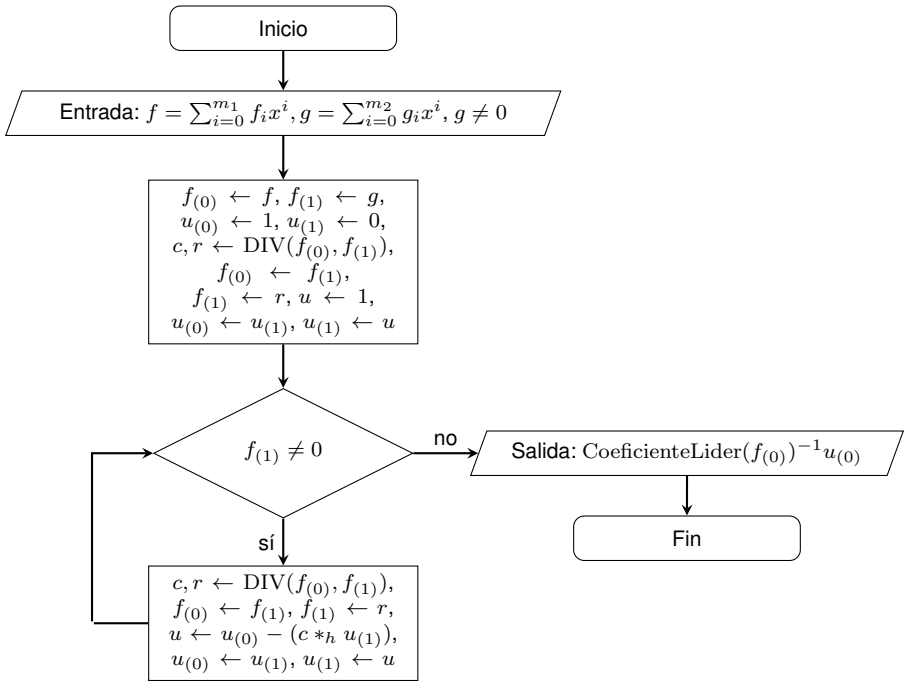


Figura 4: $\mathrm{MCM}(f, g)$

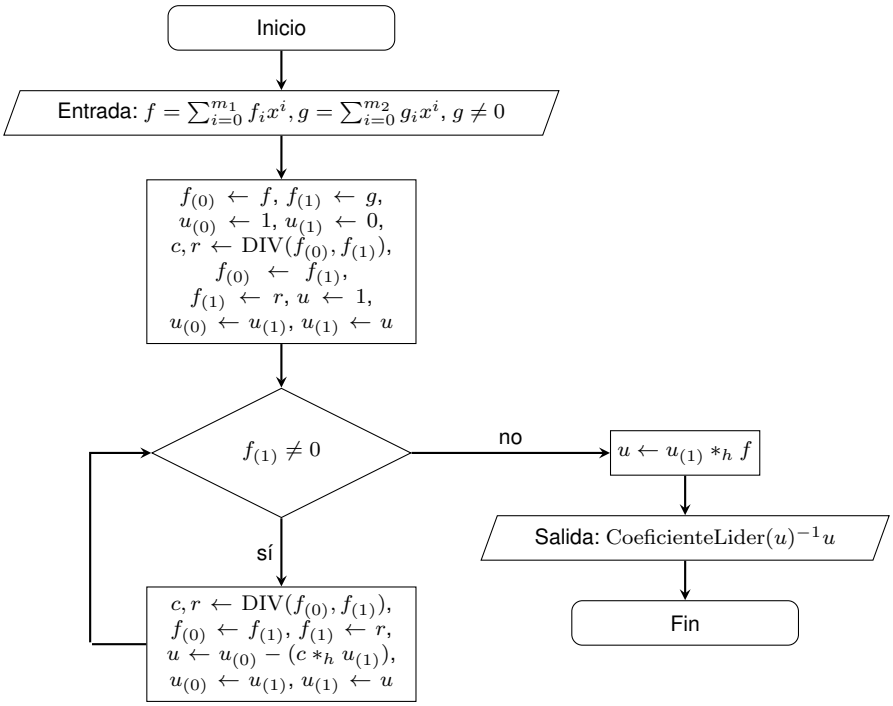
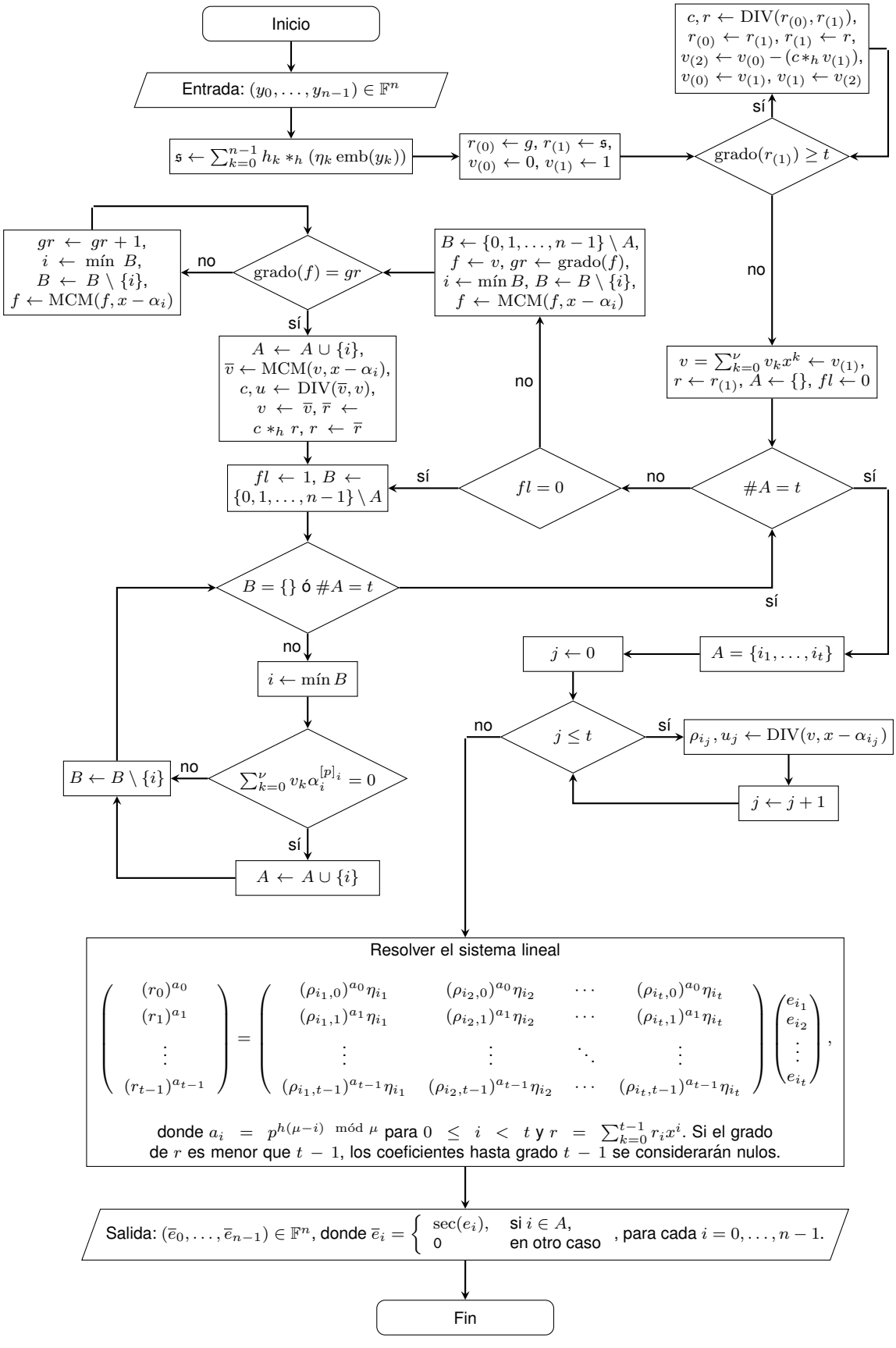


Figura 5: $\mathrm{DEC}(y)$



OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 202230118

(22) Fecha de presentación de la solicitud: 15.02.2022

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) Int. CI.: ***H04L9/30*** (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) Documentos citados	Reivindicaciones afectadas
A	US 2021203502 A1 (CHEUNG, ANDREW) 01/07/2021	1-13
A	US 2020028674 A1 (BAO, KYLE XINGKAI et al.) 23/01/2020	1-13
A	WO 9808323 A1 (NTRU CRYPTOSYSTEMS INC) 26/02/1998	1-13
A	WO 2012139919 A2 (UNIV ZUERICH et al.) 18/10/2012	1-13
A	WANG YONGGE.: "Quantum resistant random linear code based public key encryption scheme RLCE". 2016 IEEE International Symposium on Information Theory (ISIT), 20160710 IEEE, 10/07/2016, Páginas 2519 - 2523, <DOI: doi:10.1109/ISIT.2016.7541753>	1-13

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
15.03.2023	S. Sánchez Paradinas	1/2

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04L

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, NPL, INTERNET