(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 512 115**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 9/30 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.04.2010 E 10767171 (1)**

(97) Fecha y número de publicación de la concesión europea: **03.09.2014 EP 2424155**

(54) Título: **Dispositivo de generación de información, método de generación de información, y programa de generación de información y medio de almacenamiento del mismo**

(30) Prioridad:

24.04.2009 JP 2009106009

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.10.2014

(73) Titular/es:

NIPPON TELEGRAPH AND TELEPHONE CORPORATION (100.0%)
3-1 Otemachi 2-chome Chiyoda-ku
Tokyo 100-8116, JP

(72) Inventor/es:

SUZUKI, KOUTAROU y
NISHIMAKI, RYO

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Dispositivo de generación de información, método de generación de información, y programa de generación de información y medio de almacenamiento del mismo

CAMPO TÉCNICO

La presente invención se refiere a una aplicación de la tecnología de seguridad de la información. Por ejemplo, la presente invención se refiere a una criptografía jerárquica en la cual una clave de descifrado que presenta una capacidad de descifrado limitada se puede obtener a partir de otra clave de descifrado.

ANTECEDENTES DE LA TÉCNICA

La tecnología descrita en la bibliografía no referente a patentes 1 es una tecnología convencional conocida para la criptografía jerárquica.

Okamoto, Tatsuaki et al., "Homomorphic Encryption and Signatures from Vector Decomposition", *Pairing-Based Cryptography – Pairing 2008, Springer Berlin Heidelberg,* 1 de septiembre de 2008, págs. 57 a 74, hacen referencia a un concepto para el cifrado homomórfico, un espacio de autovectores de distorsión el cual es un espacio vectorial (dimensional superior) en el cual hay disponibles emparejamientos bilineales y mapas de distorsión. Un espacio de autovectores de distorsión se puede lograr sobre una curva hiperelíptica supersingular o sobre un producto directo de curvas elípticas supersingulares. Se introduce un problema inextricable (con función trampa) en espacios de autovectores de distorsión, el cual consiste en la generalización dimensional superior del problema de descomposición vectorial (VDP). Puede obtenerse una función trampa biyectiva con propiedades algebraicamente enriquecidas, a partir del VDP sobre espacios de autovectores de distorsión. Se presentan dos aplicaciones de esta función trampa biyectiva; una es el cifrado homomórfico multivariante así como un protocolo bipartito para evaluar de manera segura fórmulas de 2DNF de una manera dimensional superior, y la otra es varios tipos de firmas, tales como firmas ordinarias, firmas ciegas, firmas incontestables genéricamente (de manera selectiva y universal) convertibles y su combinación.

Boneh, Dan et al., "Hierarchical Identity Based Encryption with Constant Size Ciphertext", *Lecture Notes in Computer Science/Computational Science* (CPAIOR 2011), S*pringer Berlin Heidelberg,* vol. 3494, 20 de junio de 2005, págs. 440 a 456, dan a conocer un sistema de Cifrado Jerárquico Basado en Identidades (HIBE) en el que el texto cifrado consta de solamente tres elementos de grupo y el descifrado requiere únicamente dos cálculos de mapas bilineales, con independencia de la profundidad de la jerarquía. El esquema es seguro selectivamente con respecto al ID en el modelo convencional y totalmente seguro en el modelo de oráculo aleatorio.

BIBLIOGRAFÍA DE LA TÉCNICA ANTERIOR

BIBLIOGRAFÍA NO REFERENTE A PATENTES

Bibliografía no referente a patentes 1: Craig Gentry, Alice Siverberg, "Hierarchical ID-Based Cryptography", ASIACRYPT 2002, págs. 548 a 566

EXPOSICIÓN DE LA INVENCIÓN

PROBLEMAS A RESOLVER POR LA INVENCIÓN

En la tecnología descrita en la bibliografía no referente a patentes 1, una clave correspondiente a un nodo hijo en una estructura en árbol se puede obtener a partir de una clave correspondiente a un nodo padre, aunque la obtención de claves no se puede implementar en una estructura semiordenada general s diferente a una estructura en árbol. Por ejemplo, en una estructura que tiene un nodo padre A, un nodo padre B, y un nodo hijo común C, no es posible obtener una clave del nodo hijo común C a partir de una clave del nodo padre A u obtener una clave del nodo hijo común C a partir de una clave del nodo padre B.

MEDIOS PARA RESOLVER LOS PROBLEMAS

Para resolver el problema anterior, se proporcionan un aparato de generación de información según la reivindicación 1 ó la reivindicación 3 y un método de generación de información según la reivindicación 5.

EFECTOS DE LA INVENCIÓN

En una estructura que tiene un nodo padre A, un nodo padre B, y un nodo hijo común C, es posible obtener información del nodo hijo común C a partir de información del nodo padre A y obtener información del nodo hijo común C a partir de información del nodo padre B.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 es un diagrama de bloques funcional a modo de ejemplo de un aparato de generación de información según una primera realización;

la Figura 2 es un diagrama de flujo a modo de ejemplo de generación de información en la primera realización;

la Figura 3 es un diagrama de flujo a modo de ejemplo de obtención de información en la primera realización;
la Figura 4 es un diagrama de bloques funcional a modo de ejemplo de un aparato de generación de información de acuerdo con una segunda realización;
la Figura 5 es un diagrama de flujo a modo de ejemplo de generación de información en la segunda realización; y
la Figura 6 es un diagrama de flujo a modo de ejemplo de obtención de información en la segunda realización.

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES

A continuación se describirán detalladamente realizaciones de la presente invención.

Cifrado basado en predicados

En primer lugar se describirá una visión general del cifrado basado en predicados, el cual es un concepto usado en una primera realización.

Definiciones

Se definirán primero términos y símbolos que se usarán en realizaciones.

Matriz: Una matriz representa una disposición rectangular de elementos de un conjunto en el cual está definida una operación. La matriz la pueden formar no solamente elementos de un anillo sino también elementos de un grupo.

$(\cdot)^T$: Matriz transpuesta de "·"
$(\cdot)^{-1}$: Matriz inversa de "·"
$\wedge$: AND Lógica
$\vee$: OR Lógica
Z: Conjunto de enteros
k: Parámetro de seguridad ($k \in Z$, $k > 0$)
{0, 1}*: Secuencia binaria que tiene una longitud de bits deseada. Un ejemplo es una secuencia formada por enteros 0 y 1. No obstante, {0, 1}* no se limita a secuencias formadas por enteros 0 y 1. {0, 1}* es un cuerpo finito de orden 2 o su campo extendido.
$\{0, 1\}^\zeta$: Secuencia binaria que tiene una longitud de bits ζ ($\zeta \in Z$, $\zeta > 0$). Un ejemplo es una secuencia formada por enteros 0 y 1. No obstante, $\{0, 1\}^\zeta$ no se limita a secuencias formadas por enteros 0 y 1. $\{0, 1\}^\zeta$ es un cuerpo finito de orden 2 (cuando $\zeta = 1$) o un cuerpo extendido obtenido mediante la extensión del cuerpo finito en el grado ζ (cuando $\zeta > 1$).
(+): Operador de OR exclusiva entre secuencias binarias. Por ejemplo, se cumple lo siguiente: 10110011 (+) 11100001 = 01010010.
F_q: Cuerpo finito de orden q, donde q es un entero igual a o mayor que 1. Por ejemplo, el orden q es un número primo de una potencia de un número primo. En otras palabras, el cuerpo finito F_q es un cuerpo primo o un cuerpo extendido de cuerpo primo, por ejemplo. Cuando el cuerpo finito F_q es un cuerpo primo, se pueden llevar fácilmente a cabo, por ejemplo, cálculos de restos con respecto al módulo q. Cuando el cuerpo finito F_q es un cuerpo extendido, se pueden llevar a cabo fácilmente, por ejemplo, cálculos de restos módulo un polinomio irreducible. Se da a conocer un método específico para configurar un cuerpo finito F_q, por ejemplo, en la bibliografía de referencia 1, "ISO/IEC 18033-2: Information technology--Security techniques--Encryption algorithms—Part 2: Asymmetric ciphers".
0_F: Elemento unitario aditivo del cuerpo finito F_q
1_F: Elemento unitario multiplicativo del cuerpo finito F_q
$\delta(i, j)$: Función delta de Kronecker. Cuando $i = j$, $\delta(i, j) = 1_F$.
Cuando $i \neq j$, $\delta(i, j) = 0_F$.
E: Curva elíptica definida en el cuerpo finito F_q. Se define como un punto especial O denominado punto del infinito más un conjunto de puntos (x, y) que cumplen x, $y \in F_q$ y la ecuación de Weierstrass en un sistema de coordenadas afines.

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (1)$$

donde a_1, a_2, a_3, a_4, $a_6 \in F_q$. Se puede definir una operación binaria + denominada adición elíptica para dos puntos cualesquiera en la curva elíptica E, y se puede definir una operación unaria – denominada inverso elíptico para un punto cualquiera en la curva elíptica E. Se sabe bien que un conjunto finito de puntos racionales en la curva elíptica E forman un grupo con respecto a la adición elíptica. Además se sabe también que se puede definir una operación denominada multiplicación escalar elíptica con la adición elíptica. Asimismo se conoce también un método específico de funcionamiento de operaciones elípticas, tales como la adición elíptica, en un ordenador. (Véase, por ejemplo, la bibliografía de referencia 1, la bibliografía de referencia 2, "RFC 5091: Identity-Based Cryptography Standard (IBCS) # 1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems", y la bibliografía de referencia 3, de Ian F. Blake, Gadiel Seroussi, y Nigel P. Smart, "Elliptic Curves in Cryptography", Pearson Education, ISBN 4-89471-431-0).

Un conjunto finito de puntos racionales en la curva elíptica E tiene un subgrupo de orden p ($p \geq 1$). Cuando el número de elementos en un conjunto finito de puntos racionales en la curva elíptica E es #E, y p es un número primo grande que puede dividir a #E sin ningún resto, por ejemplo, un conjunto finito E[p] de p puntos divididos equitativamente en la curva elíptica E forma un subgrupo del conjunto finito de puntos racionales en la curva elíptica E. Los p puntos divididos equitativamente en la curva elíptica E son puntos A en la curva elíptica E que cumplen la multiplicación escalar elíptica pA= O.

G_1, G_2, G_T: Grupos cíclicos de orden q. Los ejemplos de los grupos cíclicos G_1 y G_2 incluyen el conjunto finito E[p] de p puntos divididos equitativamente en la curva elíptica E y sus subgrupos. G_1 puede ser igual a G_2, o G_1 puede no ser igual a G_2. Los ejemplos del grupo cíclico G_T incluyen un conjunto finito que constituyen un cuerpo extendido del cuerpo finito F_q. Un ejemplo específico del mismo es un conjunto finito de la raíz p-ésima de 1 en la clausura algebraica del cuerpo finito F_q.

En las realizaciones, operaciones definidas en los grupos cíclicos G_1 y G_2 se expresan como adiciones, y una operación definida en el grupo cíclico G_T se expresa como una multiplicación. Más específicamente, $\chi \cdot \Omega \in G_1$ para $\chi \in F_q$ y $\Omega \in G_1$ significa que la operación definida en el grupo cíclico G_1 se aplica a $\Omega \in G_1$ χ veces, y $\Omega_1 + \Omega_2 \in G_1$ para $\Omega_1, \Omega_2 \in G_1$ significa que la operación definida en el grupo cíclico G_1 se aplica a $\Omega_1 \in G_1$ y $\Omega_2 \in G_1$. De la misma manera, $\chi \cdot \Omega \in G_2$ para $\chi \in F_q$ y $\Omega \in G_2$ significa que la operación definida en el grupo cíclico G_2 se aplica a $\Omega \in G_2$ χ veces, y $\Omega_1 + \Omega_2 \in G_2$ para $\Omega_1, \Omega_2 \in G_2$ significa que la operación definida en el grupo cíclico G_2 se aplica a $\Omega_1 \in G_2$ y $\Omega_2 \in G_2$. Por contraposición, $\Omega^{\chi} \in G_T$ para $\chi \in F_q$ y $\Omega \in G_T$ significa que la operación definida en el grupo cíclico G_T se aplica a $\Omega \in G_T$ χ veces, y $\Omega_1 \cdot \Omega_2 \in G_T$ para $\Omega_1, \Omega_2 \in G_T$ significa que la operación definida en el grupo cíclico G_T se aplica a $\Omega_1 \in G_T$ y $\Omega_2 \in G_T$.

G_1^{n+1}: Producto directo de (n + 1) grupos cíclicos G_1 ($n \geq 1$)
G_2^{n+1}: Producto directo de (n + 1) grupos cíclicos G_2
g_1, g_2, g_T: Generadores cíclicos G_1, G_2, G_T
V: Espacio vectorial (n + 1)-dimensional formado por el producto directo de los (n + 1) grupos cíclicos G_1
V*: Espacio vectorial (n + 1)-dimensional formado con el producto directo de los (n + 1) grupos cíclicos G_2
e: Función (función bilineal) para calcular un mapa bilineal no degenerado que establece una correspondencia del producto directo $G_1^{n+1} \times G_2^{n+1}$ del producto directo G_1^{n+1} y el producto directo G_2^{n+1} con el grupo cíclico G_T. La función bilineal e recibo (n + 1) elementos γ_L (L = 1, ..., n + 1) ($n \geq 1$) del grupo cíclico G_1 y (n + 1) elementos γ_L* (L = 1, ..., n + 1) del grupo cíclico G_2 y da salida a un elemento del grupo cíclico G_T.

$$e: \quad G_1^{n+1} \times G_2^{n+1} \rightarrow G_T \qquad (2)$$

La función bilineal e satisface las siguientes características:

- Bilinealidad: La siguiente relación se cumple para todo $\Gamma_1 \in G_1^{n+1}$, $\Gamma_2 \in G_2^{n+1}$, y $\nu, \kappa \in F_q$

$$e(\nu \cdot \Gamma_1, \kappa \cdot \Gamma_2) = e(\Gamma_1, \Gamma_2)^{\nu\kappa} \qquad (3)$$

- No generación: estación función no establece una correspondencia de todo

$$\Gamma_1 \in G_1^{n+1}, \Gamma_2 \in G_2^{n+1} \qquad (4)$$

sobre el elemento unitario del grupo cíclico G_T.

- Computabilidad: existe un algoritmo para calcular eficientemente $e(\Gamma_1,\Gamma_2)$ para todo $\Gamma_1 \in G_1^{n+1}$, $\Gamma_2 \in G_2^{n+1}$.

En las realizaciones, la siguiente función para calcular un mapa bilineal no degenerado que establece una correspondencia del producto directo $G_1 \times G_2$ del grupo cíclico G_1 y el grupo cíclico G_2 con el grupo cíclico G_T constituye la función bilineal e.

Emparejamiento: $G_1 \times G_2 \rightarrow G_T$ (5)

La función bilineal e recibe un vector (n + 1)-dimensional (γ_1,...γ_{n+1}) formado con (n + 1) elementos γ_L (L = 1, ..., n + 1) del grupo cíclico G_1 y un vector (n + 1)-dimensional (γ_1*,...γ_{n+1}*) formado por (n + 1) elementos γ_L* (L = 1, ..., n + 1) del grupo cíclico G_2 y da salida a un elemento del grupo cíclico G_T.

$$e = \Pi_{L=1}^{n+1} \text{Emparejamiento}(\gamma_L, \gamma_L^*) \qquad (6)$$

Función bilineal Emparejamiento recibe un elemento del grupo cíclico G_1 y un elemento del grupo cíclico G_2 y da

salida a un elemento del grupo cíclico G_T, y cumple las siguientes características:

- Bilinealidad: Se cumple la siguiente relación para todo $\Omega_1 \in G_1$, $\Omega_2 \in G_2$, y ν, $\kappa \in F_q$

$$\text{Emparejamiento}(\nu \cdot \Omega_1, \nu \cdot \Omega_2) = \text{Emparejamiento}(\Omega_1, \Omega_2)^{\nu * \kappa} \quad (7)$$

- No degeneración: Esta función no establece una correspondencia de todo

$$\Omega_1 \in G_1, \Omega_2 \in G_2 \quad (8)$$

sobre el elemento unitario del grupo cíclico G_T.

- Computabilidad: Existe un algoritmo para calcular eficientemente Emparejamiento(Ω_1,Ω_2) para todo $\Omega_1 \in G_1$, $\Omega_2 \in G_2$.

Un ejemplo específico de la función bilineal Emparejamiento es una función para llevar a cabo una operación de emparejamiento tal como un emparejamiento de Weil o un emparejamiento de Tate. (Véase la bibliografía de referencia 4, de Alfred. J. Menezes, “Elliptic Curve Public Key Cryptosystems”, Kluwer Academic Publishers, ISBN 0-7923-9368-6, págs. 61 a 81, por ejemplo). Como la función bilineal Emparejamiento se puede usar una función de emparejamiento modificada e(Ω_1, phi(Ω_2)) ($\Omega_1 \in G_1$, $\Omega_2 \in G_2$) obtenida mediante la combinación de una función para llevar a cabo una operación de emparejamiento, tal como un Emparejamiento de Tate, y una función predeterminada phi según el tipo de la curva elíptica E (véase, por ejemplo, la bibliografía de referencia 2). Como algoritmo para llevar a cabo una operación de emparejamiento en un ordenador, se puede usar el algoritmo de Miller (véase la bibliografía de referencia 5, V.S., Miller, “Short Programs for Functions on Curves”, 1986, http://crypto.stanford.edu/miller/miller.pdf) o algún otro algoritmo conocido. Se han dado a conocer métodos para configurar un grupo cíclico y una curva elíptica usados para llevar a cabo eficientemente una operación de emparejamiento. (Por ejemplo, véase la bibliografía de referencia 2; la bibliografía de referencia 6, A. Miyaji, M. Nakabayashi, y S. Takano, “New Explicit Conditions of Elliptic Curve Traces for FR Reduction”, IEICE Trans. Fundamentals, Vol. E84-A, n.º 5, págs. 1234 a 1243, mayo de 2001; la bibliografía de referencia 7, P. S. L. M. Barreto, B. Lynn, M. Scott, “Constructing Elliptic Curves with Prescribed Embedding Degrees”, Proc. SCN ‘2002, LNCS 2576, págs. 257 a 267, Springer-Verlag. 2003; y la bibliografía de referencia 8, R. Dupont, A. Enge, E. Morain, “Building Curves with Arbitrary Small MOV Degree over Finite Prime Fields”, http://eprint.iacr.org/2002/094/).

a_i (i = 1,..., n + 1): vectores base (n + 1)-dimensionales que tienen (n + 1) elementos del grupo cíclico G_1 como elementos. Un ejemplo de los vectores base a_i es un vectores base (n + 1)-dimensional que tiene $\kappa_1 \cdot g_1 \in G_1$ como un elemento i-dimensional y el elemento unitario (expresado como “0” en la expresión aditiva) del grupo cíclico G_1 como los restantes n elementos. En ese caso, los elementos de los vectores base (n + 1)-dimensionales a_i (i = 1, ..., n + 1) se pueden enumerar de la manera siguiente:

$$\begin{aligned} a_1 &= (\kappa_1 \cdot g_1, 0, 0, ..., 0) \\ a_2 &= (0, \kappa_1 \cdot g_1, 0, ..., 0) \\ &..... \\ a_{n+1} &= (0, 0, 0, ..., \kappa_1 \cdot g_1) \end{aligned} \quad (9)$$

En este caso, κ_1 es una constante formada por un elemento del cuerpo finito F_q diferente al elemento unitario aditivo 0_F. Un ejemplo de $\kappa_1 \in F_q$ es $\kappa_1 = 1_F$. Los vectores base a_i son bases ortogonales. Cada vector (n + 1)-dimensional que tiene (n + 1) elementos del grupo cíclico G_1 como elementos se expresa mediante una suma lineal de vectores base (n + 1)-dimensionales a_i (i = 1, ..., n + 1). Por lo tanto, los vectores (n + 1)-dimensionales a_i abarcan el espacio vectorial V, descrito anteriormente.

a_i^* (i = 1, ..., n + 1): vectores base (n + 1)-dimensionales que tienen (n + 1) elementos del grupo cíclico G_2 como elementos. Un ejemplo de los vectores base a_i^* es un vector base (n + 1)-dimensional que tiene $\kappa_2 \cdot g_2 \in G_2$ como un elemento i-dimensional y el elemento unitario (expresado como “0” en la expresión aditiva) del grupo cíclico G_2 como los n elementos restantes. En ese caso, los elementos de los vectores base (n + 1)-dimensionales a_i^* (i = 1, ..., n + 1) se pueden enumerar de la siguiente manera:

$$a_1^* = (\kappa_2 \cdot g_2, 0, 0, \ldots, 0)$$
$$a_2^* = (0, \kappa_2 \cdot g_2, 0, \ldots, 0) \qquad (10)$$
$$\ldots\ldots$$
$$a_{n+1}^* = (0, 0, 0, \ldots, \kappa_2 \cdot g_2)$$

En este caso, κ_2 es una constante formada por un elemento del cuerpo finito F_q diferente al elemento unitario aditivo 0_F. Un ejemplo de $\kappa_2 \in F_q$ es $\kappa_2 = 1_F$. Los vectores base a_i^* son bases ortogonales. Cada vector (n + 1)-dimensional que tiene (n + 1) elementos del grupo cíclico G_2 como elementos se expresa mediante una suma lineal de vectores base (n + 1)-dimensionales a_i^* (i = 1, ..., n + 1). Por lo tanto, los vectores (n + 1)-dimensionales a_i^* abarcan el espacio vectorial V*, descrito anteriormente.

Los vectores base a_i y los vectores base a_i^* cumplen la siguiente expresión para un elemento $\tau = \kappa_1 \cdot \kappa_2$ del cuerpo finito F_q diferente de 0_F:

$$e(a_i, a_j^*) = g_T^{\tau\delta(i,j)} \qquad (11)$$

Cuando i = j, se cumple la siguiente expresión a partir de las Expresiones (6) y (7).

$$e(a_i, a_j^*) = \text{Emparejamiento}(\kappa_1 \cdot g_1, \kappa_2 \cdot g_2) \cdot \text{Emparejamiento}(0, 0) \cdot \ldots \cdot \text{Emparejamiento}(0,0)$$
$$= \text{Emparejamiento}(g_1, g_2)^{\kappa_1\kappa_2} \cdot \text{Emparejamiento}(g_1, g_2)^{0 \cdot 0} \cdot \ldots \cdot \text{Emparejamiento}(g_1, g_2)^{0 \cdot 0}$$
$$= \text{Emparejamiento}(g_1, g_2)^{\kappa_1\kappa_2} = g_T^{\tau}$$

Cuando $i \neq j$, $e(a_i, a_j^*)$ no incluye Emparejamiento($\kappa_1 \cdot g_1$, $\kappa_2 \cdot g_2$) y es el producto de Emparejamiento ($\kappa_1 \cdot g_1$, 0), Emparejamiento (0, $\kappa_2 \cdot g_2$), y Emparejamiento(0, 0). Adicionalmente, se cumple la siguiente expresión a partir de la Expresión (7).

$$\text{Emparejamiento}(g_1, 0) = \text{Emparejamiento}(0, g_2) = \text{Emparejamiento}(g_1, g_2)^0$$

Por lo tanto, cuando $i \neq j$, se cumple la siguiente expresión.

$$e(a_i, a_j^*) = e(g_1, g_2)^0 = g_T^0$$

Especialmente, cuando $\tau = \kappa_1 \cdot \kappa_2 = 1_F$ (por ejemplo, $\kappa_1 = \kappa_2 = 1_F$), se cumple la siguiente expresión.

$$e(a_i, a_j^*) = g_T^{\delta(i,j)} \qquad (12)$$

En este caso, $g_T^0 = 1$ es el elemento unitario del grupo cíclico G_T, y $g_T^1 = g_T$ es un generador del grupo cíclico G_T. En ese caso, los vectores base a_i y los vectores base a_i^* son bases ortogonales normales duales, y el espacio vectorial V y el espacio vectorial V* son un espacio vectorial dual que constituye un establecimiento de correspondencias (*mapping*) bilineal (espacio vectorial de emparejamientos duales (DPVS)).

A: Una matriz de (n + 1) filas por (n + 1) columnas que tiene los vectores base a_i (i = 1, ..., n + 1) como elementos. Cuando los vectores base a_i (i = 1, ..., n + 1) se expresan mediante la Expresión (9), por ejemplo, la matriz A es la siguiente:

$$A = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n+1} \end{pmatrix} = \begin{pmatrix} \kappa_1 \cdot g_1 & 0 & \cdots & 0 \\ 0 & \kappa_1 \cdot g_1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \kappa_1 \cdot g_1 \end{pmatrix} \qquad (13)$$

A*: Una matriz de (n + 1) filas por (n + 1) columnas que tiene los vectores base a_i^* (i = 1, ..., n + 1) como elementos. Cuando los vectores base a_i^* (i = 1, ..., n + 1) se expresan mediante la Expresión (10), por ejemplo, la matriz A* es la siguiente:

$$A^* = \begin{pmatrix} a_1^* \\ a_2^* \\ \vdots \\ a_{n+1}^* \end{pmatrix} = \begin{pmatrix} \kappa_2 \cdot g_2 & 0 & \cdots & 0 \\ 0 & \kappa_2 \cdot g_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \kappa_2 \cdot g_2 \end{pmatrix} \qquad (14)$$

X: Una matriz de (n + 1) filas por (n + 1) columnas que tiene, como elementos, elementos del cuerpo finito F_q. La matriz X se usa para aplicar conversión de coordenadas a los vectores base a_i. Cuando el elemento situado en la fila i-ésima y la columna j-ésima de la matriz X se expresa como $\chi_{i,j} \in Fq$, la matriz X es la siguiente:

$$X = \begin{pmatrix} \chi_{1,1} & \chi_{1,2} & \cdots & \chi_{1,n+1} \\ \chi_{2,1} & \chi_{2,2} & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+1,1} & \chi_{n+1,2} & \cdots & \chi_{n+1,n+1} \end{pmatrix} \qquad (15)$$

En este caso, cada elemento $\chi_{i,j}$ de la matriz X se denomina coeficiente de conversión.

X*: Matriz transpuesta de la matriz inversa de la matriz X. $X^* = (X^{-1})^T$. La matriz X* se usa para aplicar una conversión de coordenadas a los vectores base a_i^*. Cuando el elemento situado en la fila i-ésima y la columna j-ésima de la matriz X* se expresa como $\chi_{i,j}^* \in Fq$, la matriz X* es la siguiente:

$$X^* = \begin{pmatrix} \chi_{1,1}^* & \chi_{1,2}^* & \cdots & \chi_{1,n+1}^* \\ \chi_{2,1}^* & \chi_{2,2}^* & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+1,1}^* & \chi_{n+1,2}^* & \cdots & \chi_{n+1,n+1}^* \end{pmatrix} \qquad (16)$$

En este caso cada elemento $\chi_{i,j}^*$ de la matriz X* se denomina coeficiente de conversión.

En tal caso, cuando a una matriz unidad de (n + 1) filas por (n + 1) columnas se le denomina I, $X \cdot (X^*)^T = I$. En otras palabras, para la matriz unidad que se muestra a continuación,

$$I = \begin{pmatrix} 1_F & 0_F & \cdots & 0_F \\ 0_F & 1_F & & \vdots \\ \vdots & & \ddots & 0_F \\ 0_F & 0_F & \cdots & 1_F \end{pmatrix} \qquad (17)$$

se cumple la siguiente expresión.

$$\begin{pmatrix} \chi_{1,1} & \chi_{1,2} & \cdots & \chi_{1,n+1} \\ \chi_{2,1} & \chi_{2,2} & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+1,1} & \chi_{n+1,2} & \cdots & \chi_{n+1,n+1} \end{pmatrix} \cdot \begin{pmatrix} \chi_{1,1}^* & \chi_{2,1}^* & \cdots & \chi_{n+1,1}^* \\ \chi_{1,2}^* & \chi_{2,2}^* & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{1,n+1}^* & \chi_{2,n+1}^* & \cdots & \chi_{n+1,n+1}^* \end{pmatrix} = \begin{pmatrix} 1_F & 0_F & \cdots & 0_F \\ 0_F & 1_F & & \vdots \\ \vdots & & \ddots & 0_F \\ 0_F & 0_F & \cdots & 1_F \end{pmatrix} \qquad (18)$$

En este caso, a continuación se definirán vectores (n + 1)-dimensionales.

$$\chi_i^{\rightarrow} = (\chi_{i,1}, \ldots, \chi_{i,n+1}) \qquad (19)$$

$$\chi_j^{\rightarrow} = (\chi_{j,1}^*, \ldots, \chi_{j,n+1}^*) \qquad (20)$$

El producto interno de los vectores (n + 1)-dimensionales $\chi_i^{\rightarrow}$ y $\chi_i^{\rightarrow *}$ cumple la siguiente expresión a partir de la Expresión (18).

$$\chi_i^{\rightarrow} \cdot \chi_j^{\rightarrow *} = \delta(i, j) \qquad (21)$$

b_i: vectores base (n + 1)-dimensionales que tienen (n + 1) elementos del grupo cíclico G_1 como elementos. Los vectores base b_i se obtienen aplicando una conversión de coordenadas a los vectores base a_i (i = 1, ..., n + 1) mediante el uso de la matriz X. Específicamente, los vectores base b_i se obtienen mediante el siguiente cálculo

$$b_i = \sum_{j=1}^{n+1} \chi_{i,j} \cdot a_j \qquad (22)$$

Cuando los vectores base a_j (j = 1, ..., n + 1) se expresan por medio de la Expresión (9), cada elemento de los vectores base b_i se muestra de la manera siguiente.

$$b_i = (\chi_{i,1} \cdot \kappa_1 \cdot g_1, \chi_{i,2} \cdot \kappa_1 \cdot g_1, \ldots, \chi_{i,n+1} \cdot \kappa_1 \cdot g_1) \qquad (23)$$

Cada vector (n + 1)-dimensional que tiene (n + 1) elementos del grupo cíclico G_1 como elementos, se expresa mediante una suma lineal de vectores base (n + 1)-dimensionales b_i (i = 1, ..., n + 1). Por lo tanto, los vectores (n + 1)-dimensionales b_i abarcan el espacio vectorial V, descrito anteriormente.

b_i^*: vectores base (n + 1)-dimensionales que tienen (n + 1) elementos del grupo cíclico G_2 como elementos. Los vectores base b_i^* se obtienen aplicando una conversión de coordenadas a los vectores base a_i^* (i = 1, ..., n + 1) mediante el uso de la matriz X*. Específicamente, los vectores base b_i^* se obtienen mediante el siguiente cálculo

$$b_i^* = \sum_{j=1}^{n+1} \chi_{i,j}^* \cdot a_j^* \qquad (24)$$

Cuando los vectores base a_j (j = 1, ..., n + 1) se expresan por medio de la Expresión (10), cada elemento de los vectores base b_i^* se muestra de la manera siguiente.

$$b_i^* = (\chi_{i,1}^* \cdot \kappa_2 \cdot g_2, \chi_{i,2}^* \cdot \kappa_2 \cdot g_2, \ldots, \chi_{i,n+1}^* \cdot \kappa_2 \cdot g_2) \qquad (25)$$

Cada vector (n + 1)-dimensional que tiene (n + 1) elementos del grupo cíclico G_2 como elementos, se expresa mediante una suma lineal de vectores base (n + 1)-dimensionales b_i^* (i = 1, ..., n + 1). Por lo tanto, los vectores (n + 1)-dimensionales b_i^* abarcan el espacio vectorial V*, descrito anteriormente.

Los vectores base b_i y los vectores base b_i^* cumplen la siguiente expresión para los elementos $\tau = \kappa_1 \cdot \kappa_2$ del cuerpo finito F_q diferente de 0_F:

$$e(b_i, b_j^*) = g_T^{\tau\delta(i, j)} \qquad (26)$$

La siguiente expresión se cumple a partir de las Expresiones (6), (21), (23), y (25).

$$e\left(b_i, b_j^*\right) = \prod_{L=1}^{n+1} \text{Emparejamiento}\left(\chi_{i,L} \cdot \kappa_1 \cdot g_1, \chi_{j,L}^* \cdot \kappa_2 \cdot g_2\right)$$

$$= \text{Emparejamiento}\left(\chi_{i,1} \cdot \kappa_1 \cdot g_1, \chi_{j,1}^* \cdot \kappa_2 \cdot g_2\right) \cdot \cdots \cdot \left(\chi_{i,n} \cdot \kappa_1 \cdot g_1, \chi_{j,n}^* \cdot \kappa_2 \cdot g_2\right)$$

$$\times \text{Emparejamiento}\left(\chi_{j,n+1} \cdot \kappa_1 \cdot g_1, \chi_{j,n+1}^* \cdot \kappa_2 \cdot g_2\right)$$

$$= \text{Emparejamiento}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,1} \cdot \chi_{j1}^*} \cdot \cdots \cdot \text{Emparejamiento}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,z} \cdot \chi_{j,z}^*}$$

$$\times \text{Emparejamiento}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,n+1} \cdot \chi_{j,n+1}^*}$$

$$= \text{Emparejamiento}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \left(\chi_{i,1} \cdot \chi_{j1}^* + \chi_{i2} \cdot \chi_{j2}^* + \cdots + \chi_{i,n+1} \cdot \chi_{j,n+1}^*\right)}$$

$$= \text{Emparejamiento}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_i \cdot \chi_j^*}$$

$$= \text{Emparejamiento}(g_1, g_2)^{\tau \cdot \delta(i,j)} = g_T^{\tau \cdot \delta(i,j)}$$

Especialmente, cuando $\tau = \kappa_1 \cdot \kappa_2 = 1_F$ (por ejemplo, $\kappa_1 = \kappa_2 = 1_F$), se cumple la siguiente expresión.

$$e(b_i, b_j^*) = g_T^{\delta(i,j)} \qquad (27)$$

En tal caso, los vectores base b_i y los vectores base b_i^* son la base ortogonal normal dual de un espacio vectorial de emparejamientos duales (el espacio vectorial V y el espacio vectorial V*).

Siempre que se cumpla la Expresión (26) se pueden usar los vectores base a_i y a_i^* que no sean los correspondientes mostrados en las Expresión (9) y (10) como ejemplos, y los vectores ase b_i y b_i^* que no sean los correspondientes mostrados en las Expresión (22) y (24) como ejemplos.

A: Una matriz de (n + 1) filas por (n + 1) columnas que tiene los vectores base a_i (i = 1, ..., n + 1) como elementos. Cuando los vectores base a_i (i = 1, ..., n + 1) se expresan mediante la Expresión (9), por ejemplo, la matriz A es la siguiente:

B: Una matriz de (n + 1) filas por (n + 1) columnas que tiene los vectores base b_i (i = 1, ..., n + 1) como elementos. Se cumple B = X·A. Cuando los vectores base b_i se expresan mediante la Expresión (23), por ejemplo, la matriz B es la siguiente:

$$B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} \chi_{1,1} \cdot \kappa_1 \cdot g_1 & \chi_{1,2} \cdot \kappa_1 \cdot g_1 & \cdots & \chi_{1,n+1} \cdot \kappa_1 \cdot g_1 \\ \chi_{2,1} \cdot \kappa_1 \cdot g_1 & \chi_{2,2} \cdot \kappa_1 \cdot g_1 & & \vdots \\ \vdots & & \ddots & \chi_{n,n+1} \cdot \kappa_1 \cdot g_1 \\ \chi_{n+1,1} \cdot \kappa_1 \cdot g_1 & \cdots & \chi_{n+1,n} \cdot \kappa_1 \cdot g_1 & \chi_{n+1,n+1} \cdot \kappa_1 \cdot g_1 \end{pmatrix} \qquad (28)$$

B*: Una matriz de (n + 1) filas por (n + 1) columnas que tiene los vectores base b_i^* (i = 1, ..., n + 1) como elementos. Se cumple B* = X*·A*. Cuando los vectores base b_i^* (i = 1, ..., n + 1) se expresan mediante la Expresión (25), por ejemplo, la matriz B* es la siguiente:

$$B^* = \begin{pmatrix} b_1^* \\ b_2^* \\ \vdots \\ b_{n+1}^* \end{pmatrix} = \begin{pmatrix} \chi_{1,1}^* \cdot \kappa_2 \cdot g_2 & \chi_{1,2}^* \cdot \kappa_2 \cdot g_2 & \cdots & \chi_{1,n+1}^* \cdot \kappa_2 \cdot g_2 \\ \chi_{2,1}^* \cdot \kappa_2 \cdot g_2 & \chi_{2,2}^* \cdot \kappa_2 \cdot g_2 & & \vdots \\ \vdots & & \ddots & \chi_{n,n+1}^* \cdot \kappa_2 \cdot g_2 \\ \chi_{n+1,1}^* \cdot \kappa_2 \cdot g_2 & \cdots & \chi_{n+1,n}^* \cdot \kappa_2 \cdot g_2 & \chi_{n+1,n+1}^* \cdot \kappa_2 \cdot g_2 \end{pmatrix} \quad (29)$$

$\vec{w}$: Un vector n-dimensional que, como elementos, tiene elementos del cuerpo finito F_q.

$$\vec{w} = (w_1, \ldots, w_n) \in F_q^n \quad (30)$$

w_μ: el elemento μ-ésimo (μ = 1, ..., n) del vector n-dimensional.

$\vec{v}$: Un vector n-dimensional que tiene elementos del cuerpo finito F_q como elementos.

$$\vec{v} = (v_1, \ldots, v_n) \in F_q^n \quad (31)$$

v_μ: el elemento μ-ésimo (μ = 1, ..., n) del vector n-dimensional.

Función resistente a colisiones: Una función h que cumple la siguiente condición con respecto a un parámetro de seguridad k suficientemente mayor, o una función considerada como tal.

$$\Pr[A(h) = (x, y) | h(x) = h(y) \wedge x \neq y] < \varepsilon(k) \quad (32)$$

En este caso, Pr[·] es la probabilidad del evento [·]; A(h) es un algoritmo de tiempo polinómico probabilístico para calcular x e y ($x \neq y$) que cumplen h(x) = h(y) para una función h; y $\varepsilon(k)$ es un polinomio para el parámetro de seguridad k. Una función resistente a colisiones a modo de ejemplo es una función *hash* tal como la función *hash* criptográfica dada a conocer en la bibliografía de referencia 1.

Función inyectiva: Una función mediante la cual cada elemento perteneciente a un intervalo de valores se expresa como la imagen de solamente un elemento del intervalo de definición, o una función considerada como tal.

Función cuasi-aleatoria: Una función perteneciente a un subconjunto ϕ_ζ cuando un algoritmo de tiempo polinómico probabilístico no puede diferenciar entre el subconjunto ϕ_ζ y subconjunto completo Φ_ζ, o una función considerada como tal. El conjunto Φ_ζ es un conjunto de todas las funciones que establecen una correspondencia de un elemento de un conjunto $\{0, 1\}^\zeta$ con un elemento del conjunto $\{0, 1\}^\zeta$. Una función cuasi-aleatoria a modo de ejemplo es una función *hash* tal como la correspondiente descrita anteriormente.

H_1: Una función resistente a colisiones que recibe dos secuencias binarias $(\omega_1, \omega_2) \in \{0, 1\}^k \times \{0, 1\}^*$ y da salida a dos elementos $(\psi_1, \psi_2) \in F_q \times F_q$ del cuerpo finito F_q.

$$H_1: \quad \{0, 1\}^k \times \{0, 1\}^* \rightarrow F_q \times F_q \quad (33)$$

Un ejemplo de la función H_1 es una función que da salida a dos elementos $(\psi_1, \psi_2) \in F_q \times F_q$ del cuerpo finito F_q como respuesta a los bits conectados $\omega_1 || \omega_2$ de entrada ω_1 y ω_2. Esta función incluye cálculos con una función *hash*, tal como la función *hash* criptográfica dada a conocer en la bibliografía de referencia 1, una función de conversión de secuencia-binaria-a-entero (conversión de cadena de octetos/entero), y una función de conversión de secuencia-binaria-a-elemento-de-cuerpo-finito (conversión de cadena de octectos y entero/cuerpo finito). Se prefiere que la función H_1 sea una función cuasi-aleatoria.

H_2: Una función resistente a colisiones que recibe un elemento del grupo cíclico G_T y una secuencia binaria $(\xi, \omega_2) \in G_T \times \{0, 1\}^*$ y da salida a un elemento $\psi \in F_q$ del cuerpo finito F_q.

$$H_2: \quad G_T \times \{0, 1\}^* \rightarrow F_q \qquad (34)$$

Un ejemplo de la función H_2 es una función que recibe un elemento $\xi \in G_T$ del grupo cíclico G_T y una secuencia binaria $\omega_2 \in \{0, 1\}^*$, introduce el elemento $\xi \in G_T$ del grupo cíclico G_T en una función de conversión de elemento-de-cuerpo-finito-a-secuencia-binaria (conversión de cadena de octetos y entero/cuerpo finito) dada a conocer en la bibliografía de referencia 1 para obtener una secuencia binaria, aplica una función *hash* tal como la función *hash* criptográfica dada a conocer en la bibliografía de referencia 1 a los bits conectados de la secuencia binaria obtenida y de la secuencia binaria $\omega_2 \in \{0, 1\}^*$, ejecuta la función de conversión de secuencia-binaria-a-elemento-de-cuerpo-finito (conversión de cadena de octetos y entero/cuerpo finito), y da salida a un elemento $\psi \in F_q$ del cuerpo finito F_q. Desde un punto de vista de la seguridad se prefiere que la función H_2 sea una función cuasi-aleatoria.

R: Una función inyectiva que recibe un elemento $\xi \in G_T$ del grupo cíclico G_T y da salida a una secuencia binaria $\omega \in \{0, 1\}^k$.

$$R: \quad G_T \rightarrow \{0, 1\}^k \qquad (35)$$

Un ejemplo de la función inyectiva R es una función que recibe un elemento $\xi \in G_T$ del grupo cíclico G_T, lleva a cabo cálculos con la función de conversión de elemento-de-cuerpo-finito-a-secuencia-binaria (conversión de cadena de octetos y entero/cuerpo finito) y, a continuación, con una función *hash*, tal como la KDF (función de obtención de claves) dada a conocer en la bibliografía de referencia 1, y da salida a una secuencia binaria $\omega \in \{0, 1\}^k$. Desde el punto de vista de la seguridad, se prefiere que la función R sea una función resistente a colisiones, y es más preferible que la función R sea una función cuasi-aleatoria.

Enc: Una función de cifrado con claro común que indica el procesado de cifrado de un criptosistema con clave común. Son ejemplos de criptosistemas con clave común el Camellia y AES.

$Enc_k(M)$: Texto cifrado obtenido mediante el cifrado de texto en claro M por medio de la función de cifrado con clave común Enc con el uso de una clave común K.

Dec: Una función de descifrado con clave común que indica el procesado de descifrado del criptosistema con clave común.

$Dec_k(C)$: Un resultado del descifrado, obtenido descifrando texto cifrado C por medio de la función de descifrado con clave común Dec con el uso de la clave común K.

Cifrado basado en predicados con producto interno

A continuación se describirá la configuración básica del cifrado basado en predicados con producto interno.

Cifrado basado en predicados

Cifrado basado en predicados (denominado en ocasiones cifrado funcional) significa que se puede descifrar el texto cifrado cuando una combinación de información de atributos e información de predicados hace que una expresión lógica predeterminada sea verdadera. Una de entre la información de atributos y la información de predicados está incrustada en el texto cifrado y la otra está incrustada en información de claves. La configuración del cifrado convencional basado en predicados se da a conocer, por ejemplo, en la bibliografía de referencia 9, del Jonathan Katz, Amit Sahai y Brent Waters, “Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products”, uno de los cuatro documentos de Eurocrypt 2008 con invitación del *Journal of Cryptology*.

Cifrado basado en predicados con producto interno

Cifrado basado en predicados con producto interno significa que el texto cifrado se puede descifrar cuando el producto interno de la información de atributos y la información de predicados, gestionadas como vectores, es cero. En el cifrado basado en predicados con producto interno, un producto interno de cero es equivalente a una expresión lógica de verdadero.

Relación entre expresión lógica y polinomio

En el cifrado basado en predicados con producto interno, una expresión lógica formada por una OR(s) lógica(s) y/o una AND(s) lógica(s) se expresa mediante un polinomio.

La OR lógica $(x = \eta_1) \vee (x = \eta_2)$ de la sentencia 1 que indica que x es η_1 y la sentencia 2 que indica que x es η_2 se expresa mediante el siguiente polinomio.

$$(x - \eta_1)\cdot(x - \eta_2) \qquad (36)$$

A continuación, en la siguiente tabla se muestran las relaciones entre valores de verdadero y los valores de función de la Expresión (36).

Tabla 1

Sentencia 1 $(x = \eta_1)$	Sentencia 2 $(x = \eta_2)$	OR Lógica $(x = \eta_1) \vee (x = \eta_2)$	Valor de función $(x = \eta_1) \cdot (x = \eta_2)$
Verdadero	Verdadero	Verdadero	0
Verdadero	Falso	Verdadero	0
Falso	Verdadero	Verdadero	0
Falso	Falso	Falso	Diferente a 0

Tal como se entiende a partir de la Tabla 1, cuando la OR lógica $(x = \eta_1) \vee (x = \eta_2)$ es verdadera, el valor de función correspondiente a la Expresión (36) es cero; y cuando la OR lógica $(x = \eta_1) \vee (x = \eta_2)$ es falsa, el valor de función correspondiente a la Expresión (36) es un valor diferente de cero. En otras palabras, la OR lógica $(x = \eta_1) \vee (x = \eta_2)$ de verdadero es equivalente al valor de función de cero en la Expresión (36). Por lo tanto, la OR lógica se puede expresar mediante la Expresión (36).

La AND lógica $(x = \eta_1) \wedge (x = \eta_2)$ de la sentencia 1 que indica que x es η_1 y la sentencia 2 que indica que x es η_2 se expresa mediante el siguiente polinomio.

$$\iota_1\cdot(x - \eta_1) + \iota_2\cdot(x - \eta_2) \qquad (37)$$

donde ι_1 y ι_2 son números aleatorios. A continuación, en la siguiente tabla se muestran las relaciones entre valores de verdadero y los valores de función correspondientes a la Expresión (37).

Tabla 2

Sentencia 1 $(x = \eta_1)$	Sentencia 2 $(x = \eta_2)$	AND Lógica $(x = \eta_1) \wedge (x = \eta_2)$	Valor de función $\iota_1 \cdot (x - \eta_1) + \iota_2 \cdot (x - \eta_2)$
Verdadero	Verdadero	Verdadero	0
Verdadero	Falso	Falso	Diferente a 0
Falso	Verdadero	Falso	Diferente a 0
Falso	Falso	Falso	Diferente a 0

Tal como se entiende a partir de la Tabla 2, cuando la AND lógica $(x = \eta_1) \wedge (x = \eta_2)$ es verdadera, el valor de función correspondiente a la Expresión (37) es cero; y cuando la AND lógica $(x = \eta_1) \wedge (x = \eta_2)$ es falsa, el valor de función correspondiente a la Expresión (37) es un valor diferente de cero. En otras palabras, una AND lógica $(x = \eta_1) \wedge (x = \eta_2)$ de verdadero es equivalente al valor de función de cero en la Expresión (37). Por lo tanto, la AND lógica se puede expresar mediante la Expresión (37).

Como se ha descrito anteriormente, usando las Expresión (36) y (37), una expresión lógica formada por una OR(s) lógica(s) y/o una AND(s) lógica(s) se puede expresar mediante un polinomio f(x). A continuación se mostrará un ejemplo.

Expresión lógica: $\{(x = \eta_1) \vee (x = \eta_2) \vee (x = \eta_3)\} \wedge (x = \eta_4) \wedge (x = \eta_5)$

Polinomio: $f(x) = \iota_1\cdot\{(x - \eta_1)\cdot(x - \eta_2)\cdot(x - \eta_3)\} + \iota_2\cdot(x - \eta_4) + \iota_3\cdot(x - \eta_5)$

(38)

En la Expresión (36), se usa un elemento indeterminado x para expresar la OR lógica. También se puede usar una pluralidad de elementos indeterminados para expresar una OR lógica. Por ejemplo, se usan dos elementos indeterminados x_0 y x_1 para expresar la OR lógica $(x_0 = \eta_0) \vee (x_1 = \eta_1)$ de la sentencia 1 que indica que x_0 es η_0 y de la sentencia 2 que indica que x_1 es η_1 mediante siguiente polinomio.

$$(x_0 - \eta_0)\cdot(x_1 - \eta_1)$$

Se puede usar tres o más elementos indeterminados para expresión una OR lógica mediante un polinomio.

En la Expresión (37), se usa un elemento indeterminado x para expresar la AND lógica. También se puede usar una pluralidad de elementos indeterminados para expresar una AND lógica. Por ejemplo, la AND lógica ($x_0 = \eta_0$)$\wedge$($x_1 = \eta_1$) de la sentencia 1 que indica que x_0 es η_0 y la sentencia 2 que indica que x_1 es η_1 se puede expresar mediante el siguiente polinomio.

$$\iota_0\cdot(x_0 - \eta_0) + \iota_1\cdot(x_1 - \eta_1)$$

También se pueden usar tres o más elementos indeterminados para expresar una AND lógica mediante un polinomio. $f(x_0, ..., x_{H-1}) = 0 \longleftrightarrow \vec{w}\cdot\vec{v} = 0$

Una expresión lógica que incluye una OR(s) lógica(s) y/o una AND(s) lógica(s) se expresa con H (H $\geq$ 1) tipos de elementos indeterminados x_0, ..., x_{H-1} en forma del polinomio $f(x_0, ..., x_{H-1})$. Se supone que una sentencia para cada uno de los elementos indeterminados x_0, ..., x_{H-1} es "x_h es η_h", donde η_h (h = 0, ..., H - 1) es una constante determinada para cada sentencia. A continuación, en el polinomio $f(x_0, ..., x_{H-1})$ que indica la expresión lógica, la sentencia que indica que un elemento indeterminado x_h es una constante η_h se expresa mediante polinomio que indica la diferencia entre el elemento indeterminado x_h y la constante η_h; la OR lógica de sentencias se expresa mediante el producto de los polinomios que indican las sentencias; y la AND lógica de sentencias o las ORs lógicas de sentencias se expresa mediante una OR lineal de los polinomios que indican las sentencias o las ORs lógicas de sentencias. Por ejemplo, se usan cinco elementos indeterminados x_0, ..., x_4 para expresar una expresión lógica

$$\{(x_0 = \eta_0) \vee (x_1 = \eta_1) \vee (x_2 = \eta_2)\} \wedge (x_3 = \eta_3) \wedge (x_4 = \eta_4)$$

por medio del siguiente polinomio

$$f(x_0, ..., x_4) = \iota_0\cdot\{(x_0 - \eta_0)\cdot(x_1 - \eta_1)\cdot(x_2 - \eta_2)\} + \iota_1\cdot(x_3 - \eta_3) + \iota_2\cdot(x_4 - \eta_4)$$

Relación entre polinomio y producto interno

El polinomio $f(x_0, ..., x_{H-1})$ que indica una expresión lógica se puede expresar mediante el producto interno de dos vectores n-dimensionales. Más específicamente, un vector que tiene los elementos indeterminados de los términos del polinomio $f(x_0, ..., x_{H-1})$ como elementos,

$$\vec{v} = (v_1, ..., v_n)$$

y un vector que tiene los coeficientes de los términos del polinomio $f(x_0, ..., x_{H-1})$ como elementos,

$$\vec{w} = (w_1, ..., w_n)$$

se usan para generar el producto interno de los mismos,

$$f(x_0, ..., x_{H-1}) = \vec{w}\cdot\vec{v}$$

que es igual al polinomio $f(x_0, ..., x_{H-1})$. En otras palabras, la condición de que el polinomio $f(x_0, ..., x_{H-1})$ que indica una expresión lógica sea cero es equivalente a la condición de que el producto interno del vector $\vec{v}$ que tiene los elementos indeterminados de los términos de polinomio $f(x_0, ..., x_{H-1})$ como elementos y el vector $\vec{w}$ que tiene los coeficientes de los términos del polinomio $f(x_0, ..., x_{H-1})$ como elementos sea cero.

Por ejemplo, un polinomio $f(x) = \theta_0\cdot x^0 + \theta_1\cdot x + ... + \theta_{n-1}\cdot x^{n-1}$ expresado con un elemento indeterminado x se puede expresar con dos vectores n-dimensionales

$$\vec{w} = (w_1, \ldots, w_n) = (\theta_0, \ldots, \theta_{n-1}) \quad (39)$$

$$\vec{v} = (v_1, \ldots, v_n) = (x^0, \ldots, x^{n-1}) \quad (40)$$

mediante su producto interno.

$$f(x) = \vec{w} \cdot \vec{v} \quad (41)$$

En otras palabras, la condición de que el polinomio f(x) que indica una expresión lógica sea cero es equivalente a la condición de que el producto interno de la Expresión (41) sea cero.

$$f(x) = 0 \longleftrightarrow \vec{w} \cdot \vec{v} = 0 \quad (42)$$

Cuando un vector que tiene los elementos indeterminados de los términos del polinomio $f(x_0, \ldots, x_{H-1})$ como elementos se expresa mediante

$$\vec{w} = (w_1, \ldots, w_n)$$

y un vector que tiene los coeficientes de los términos del polinomio $f(x_0, \ldots, x_{H-1})$ como elementos se expresa mediante

$$\vec{v} = (v_1, \ldots, v_n)$$

la condición de que el polinomio $f(x_0, \ldots, x_{H-1})$ que indica una expresión lógica sea cero es equivalente a la condición de que el producto interno del vector $\vec{w}$ y el vector $\vec{v}$ sea cero.

Por ejemplo, cuando se usan las siguiente expresiones en lugar de las Expresiones (39) y (40)

$$\vec{w} = (w_1, \ldots, w_n) = (x^0, \ldots, x^{n-1}) \quad (43)$$

$$\vec{v} = (v_1, \ldots, v_n) = (\theta_0, \ldots, \theta_{n-1}) \quad (44)$$

la condición de que el polinomio f(x) que indica una expresión lógica sea cero es equivalente a la condición de que el producto interno de la Expresión (41) sea cero.

En el cifrado basado en predicados con producto interno, uno de los vectores $\vec{v} = (v_0, \ldots, v_{n-1})$ y $\vec{w} = (w_0, \ldots, w_{n-1})$ se usa como información de atributos y el otro se usa como información de predicados. Una de la información de atributos y la información de predicados está incrustada en el texto cifrado y la otra está incrustada en la información de claves. Por ejemplo, un vector n-dimensional $(\theta_0, \ldots, \theta_{n-1})$ se usa como información de predicados, otro vector n-dimensional $(x^0, \ldots, x^{n-1})$ se usa como información de atributos, una de entre la información de atributos y la información de predicados se incrusta en texto cifrado, y la otra se incrusta en la información de claves. En la siguiente descripción se supone que un vector n-dimensional incrustado en información de claves es $\vec{w} = (w_1, \ldots, w_n)$ y otro vector n-dimensional incrustado en texto cifrado es $\vec{v} = (v_1, \ldots, v_n)$.

Por ejemplo,

Información de predicados: $\vec{w} = (w_1, \ldots, w_n) = (\theta_0, \ldots, \theta_{n-1})$

Información de atributos: $\vec{v} = (v_1, \ldots, v_n) = (x^0, \ldots, x^{n-1})$

Alternativamente,

Información de predicados: $\vec{v} = (v_1, \ldots, v_n) = (\theta_0, \ldots, \theta_{n-1})$

Información de atributos: $\vec{w} = (w_1, \ldots, w_n) = (x^0, \ldots, x^{n-1})$

Configuración básica del cifrado basado en predicados con producto interno

A continuación se describirá una configuración básica a modo de ejemplo de un mecanismo de encapsulado de claves (KEM) que usa un cifrado basado en predicados con producto interno. Esta configuración incluye Setup(1^k), GenKey(MSK, $\vec{w}$), Enc(PA, $\vec{v}$), y Dec(SKw, C_2).

Configuración de Setup(1^k)

Entrada: Parámetro de seguridad k
Salida: Información de clave maestra MSK, parámetro público PK

En un ejemplo de Setup(1^k), como n se usa un parámetro de seguridad k, y se seleccionan una matriz A de (n + 1) filas por (n + 1) columnas que tiene vectores base (n + 1)-dimensionales a_i (i = 1, ..., n + 1) como elementos, una matriz A* de (n + 1) filas por (n +1) columnas que tiene vectores base a_i* (i = 1, ..., n+ 1) como elementos, y matrices X y X* de (n + 1) filas por (n + 1) columnas usadas para la conversión de coordenadas. A continuación, se calculan vectores base (n + 1)-dimensionales b_i (i = 1, ..., n + 1) a través de la conversión de coordenadas mediante la Expresión (22), y se calculan vectores base (n + 1)-dimensionales b_i* (i = 1, ..., n + 1) a través de la conversión de coordenadas por medio de la Expresión (24). A continuación, como información de clave maestra MSK se da salida a una matriz B* de (n + 1) filas por (n + 1) columnas que tiene como elementos los vectores base b_i* (i = 1, ..., n + 1); y, como parámetro público PK, se da salida a vectores espaciales V y V*, a una matriz B de (n + 1) filas por (n + 1) columnas que tiene, como elementos, los vectores base b_i (i = 1, ..., n + 1), al parámetro de seguridad k, a un cuerpo finito F_q, a una curva elíptica E, a grupo cíclicos G_1, G_2, y G_T, a generadores g_1, g_2, y g_T, a una función bilineal e, y otros.

Generación de información de claves GenKey(MSK, $\vec{w}$)

Entrada: Información de clave maestra MSK, vector $\vec{w}$
Salida: Información de clave D* correspondiente al vector $\vec{w}$

En un ejemplo de GenKey(MSK, $\vec{w}$), del cuerpo finito F_q se selecciona un elemento $\alpha \in F_q$. A continuación, la matriz B*, que es la información de clave maestra MSK, se usa para generar y dar salida a información de claves D* correspondiente al vector $\vec{w}$ de la siguiente manera.

$$D^* = \alpha \cdot (\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*) + b_{n+1}^* \in G_2^{n+1} \qquad (45)$$

Si resulta difícil resolver un problema logarítmico discreto sobre el grupo cíclico G_2, resulta difícil separar y extraer los componentes de $w_\mu \cdot b_\mu^*$ y b_{n+1}^* de la información de claves D*.

Cifrado Enc(PA, $\vec{v}$)

Entrada: Parámetro público PK, vector $\vec{v}$
Salida: Texto cifrado C_2, clave común K

En un ejemplo de Enc(PA, $\vec{v}$), se generan una clave común K y un número aleatorio υ_1, el cual es un elemento del cuerpo finito F_q. A continuación, se usan el parámetro público PK, tal como la matriz B, un elemento υ_2 correspondiente a un valor que incluye la clave común K, en el cuerpo finito F_q, el vector $\vec{v}$, y el número aleatorio υ_1 para generar texto cifrado C_2 de la siguiente manera.

$$C_2 = \upsilon_1 \cdot (\sum_{\mu=1}^{n} v_\mu \cdot b_\mu) + \upsilon_2 \cdot b_{n+1} \in G_1^{n+1} \qquad (46)$$

Se da salida al texto cifrado C_2 y a la clave común K. Un ejemplo de la clave común K es $g_T^{\tau \cdot \upsilon 2} \in G_T$, donde $\upsilon 2$ significa υ_2. Un ejemplo de τ es 1_F, tal como se ha descrito anteriormente. Si resulta difícil resolver un problema logarítmico discreto sobre el grupo cíclico G_1, resulta difícil separar y extraer los componentes de $v_\mu \cdot b_\mu$ y $\upsilon_2 \cdot b_{n+1}$ del texto cifrado C_2.

Descifrado y compartición de claves Dec(SKw, C_2)

Entrada: Información de claves D_1* correspondiente al vector $\vec{w}$, texto cifrado C_2
Salida: Clave común K

En un ejemplo de Dec(SKw, C_2), el texto cifrado C_2 y la información de claves D_1* se introducen en la función bilineal e de la Expresión (2). A continuación, a partir de las características de las Expresiones (3) y (26), se cumple lo siguiente.

$$\begin{aligned} e(C_2, D^*) &= e(\upsilon_1 \cdot (\textstyle\sum_{\mu=1}^{n} v_\mu \cdot b_\mu) + \upsilon_2 \cdot b_{n+1}, \alpha \cdot (\textstyle\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*) + b_{n+1}^*) \\ &= e(\upsilon_1 \cdot v_1 \cdot b_1, \alpha \cdot w_1 \cdot b_1^*) \cdot \ldots \cdot e(\upsilon_1 \cdot v_n \cdot b_n, \alpha \cdot w_n \cdot b_n^*) \\ &\quad \times e(\upsilon_2 \cdot b_{n+1}, b_{n+1}^*) \\ &= e(b_1, b_1^*)^{\upsilon_1 \cdot v_1 \cdot \alpha \cdot w_1} \cdot \ldots \cdot e(b_n, b_n^*)^{\upsilon_1 \cdot v_n \cdot \alpha \cdot w_n} \cdot e(b_{n+1}, b_{n+1}^*)^{\upsilon_2} \\ &= g_T^{\tau \cdot \upsilon_1 \cdot v_1 \cdot \alpha \cdot w_1} \cdot \ldots \cdot g_T^{\tau \cdot \upsilon_1 \cdot v_n \cdot \alpha \cdot w_n} \cdot g_T^{\tau \cdot \upsilon_2} \\ &= g_T^{\tau \cdot \upsilon_1 \cdot \alpha \cdot \vec{v} \cdot \vec{w}} \cdot g_T^{\tau \cdot \upsilon_2} \end{aligned} \quad (47)$$

Cuando el producto interno $\vec{w} \cdot \vec{v}$ es cero, la Expresión (47) se puede cambiar a lo siguiente.

$$\begin{aligned} e(C_2, D^*) &= g_T^{\tau \cdot \upsilon_1 \cdot \alpha \cdot 0} \cdot g_T^{\tau \cdot \upsilon_2} \\ &= g_T^{\tau \cdot \upsilon_2} \end{aligned} \quad (48)$$

A partir de este resultado, se genera y se da salida a la clave común K. Un ejemplo de la clave común K es $g_T^{\tau \cdot \upsilon 2} \in G_T$.

Primera realización

Un aparato y un método de generación de información según una primera realización implementan la criptografía jerárquica usando el cifrado basado en predicados descrito anteriormente. Más específicamente, utilizan la base b* usada en el cifrado basado en predicados descrito anteriormente para implementar una obtención de información expresada en estructuras semiordenadas generales que no son estructuras en árbol.

La Figura 1 es un ejemplo de un diagrama de bloques funcional del aparato de generación de información según la primera realización.

A cada elemento de información se le asigna un índice $v = (v_1, ..., v_{N-1}) \in I = (F_q \cup \{*\})^{N-1}$, y se define un conjunto $w(v) = \{i | v_i = *\}$ correspondiente al índice v, donde * indica un carácter indeterminado. Los índices que se describirán a continuación, tales como un índice u y un índice Y, tienen la misma estructura que el índice v: $u = (u_1, ..., u_{N-1}) \in I = (F_q \cup \{*\})^{N-1}$ e $Y = (Y_1, ..., Y_{N-1}) \in I = (F_q \cup \{*\})^{N-1}$. Cuando $w(u) \subset w(v)$ y $v_i = u_i$ ($i \in \{1, ..., N - 1\} \setminus w(v)$) para el índice u $\in I$ y el índice $v \in I$, en otras palabras, cuando $w(u) \subset w(v)$ y $v_i = u_i$ para cualquier $i \in \{1, ..., N - 1\} \setminus w(v)$, el índice u $\leq$ el índice v y el v es información superior al índice u, donde el símbolo \ indica la sustracción del conjunto y, por ejemplo, $A \setminus B = \{2, 3\}$ cuando el conjunto $A = \{1, 2, 3\}$ y el conjunto $B = \{1\}$.

Cuando el índice $v = \{v_1, v_2, v_3\} = \{2, *, *\}$ y el índice $u = \{u_1, u_2, u_3\} = \{2, *, 4\}$, por ejemplo, $w(v) = \{2, 3\}$ y $w(u) = \{2\}$ y se cumple $w(u) \subset w(v)$. En este caso, $v_1 = u_1 = 2$. Por lo tanto, el índice u $\leq$ el índice v y el índice v es información superior al índice u

En la siguiente descripción, el índice Y se corresponde con información generada a partir de la base b_i*, el índice v se corresponde con información de una base de obtención, y el índice u se corresponde con información obtenida a partir de información de la base de obtención.

Generación de información

El aparato y el método de generación de información generan información K_Y correspondiente al índice Y usando la base b_i* en la Etapa A1 a la Etapa A3 de la Figura 2. La información K_Y incluye información principal k_Y e información de obtención k_{Yj}. La información principal k_Y se usa como clave de descifrado, por ejemplo, en el cifrado basado en predicados. La información de obtención k_{Yj} se usa para generar información inferior a la información K_Y correspondiente al índice Y.

El aparato de generación de información recibe el índice $Y \in I$.

Un generador 1 de números aleatorios genera un número aleatorio $\sigma_Y \in Z_q$ y un número aleatorio $\sigma_{Yj} \in Z_q$ correspondiente a cada elemento $j \in w(Y)$ de un conjunto w(Y) (en la etapa A1). El número aleatorio generado σ_Y se envía a un generador 2 de información principal. El número aleatorio generador σ_{Yj} se envía a un generador 3 de

información de obtención. Cuando el conjunto w(Y) = {2, 3}, por ejemplo, el generador de números aleatorios 1 genera σ_Y, σ_{Y2}, y σ_{Y3}.

El generador de información principal 2 usa el número aleatorio generado σ_Y para calcular información principal k_Y que cumple $k_Y = \sigma_Y \Sigma_{i \in \{1,..., N-1\} \setminus w(Y)} Y_i b_i^* + b_N^*$ (en la etapa A2). La información principal calculada k_Y se almacena en unos medios 4 de almacenamiento.

El generador 3 de información de obtención usa el número aleatorio generado σ_{Yj} para calcular información de obtención k_{Yj} que cumple $k_{Yj} = \sigma_{Yj} \Sigma_{i \in \{1,..., N-1\} \setminus w(Y)} Y_i b_i^* + b_j^*$ para cada elemento $j \in w(Y)$ del conjunto w(Y) (en la etapa A3). La información de obtención calculada k_{Yj} se almacena en los medios 4 de almacenamiento.

Obtención de información

El aparato y el método de generación de información generan información K_u correspondiente a un índice inferior u a partir de información K_v correspondiente a un índice superior v, donde $u \leq v$, en la etapa B1 a la etapa B3 mostradas en la Figura 3.

La información K_v correspondiente al índice v incluye información principal k_v e información de obtención k_{vj}. La información principal k_v se usa como clave de descifrado, por ejemplo, en el cifrado basado en predicados. La información de obtención k_{vj} se usa para generar información inferior a la información K_v correspondiente al índice v. Por ejemplo, el índice v = Y y la información $K_v = K_Y$. La información K_u generada en el procesado de las etapas B1 a B3 se puede considerar como información nueva K_v para generar información $K_{u'}$ ($u' \leq u$) inferior a la información K_u correspondiente al índice u.

La información K_u correspondiente al índice u incluye información principal k_u e información de obtención k_{uj}. La información principal k_u se usa como clave de descifrado, por ejemplo, en el cifrado basado en predicados. La información de obtención k_{uj} se usa para generar información inferior a la información K_u correspondiente al índice u.

El aparato de generación de información recibe el índice v y el índice u.

Se supone que los medios 4 de almacenamiento han almacenado la información K_v correspondiente al índice v.

El generador 1 de números aleatorios genera un número aleatorio $\sigma_u \in Z_q$ y un número aleatorio $\sigma_{uj} \in Z_q$ correspondiente a cada elemento $j \in w(u)$ de un conjunto w(u) (en la etapa B1). El número aleatorio generado σ_u se envía a una unidad 5 de obtención de información principal. El número aleatorio generado σ_{uj} se envía a una unidad 6 de obtención de información de obtención.

La unidad 5 de obtención de información principal usa la información principal k_v y la información de obtención k_{vi}, que se leen ambas a partir de los medios 4 de almacenamiento, y el número aleatorio generado σ_u para calcular información principal k_u correspondiente al índice u, que cumple $k_u = \sigma_u \Sigma_{i \in w(v) \setminus w(u)} u_i k_{vi} + k_v$ (en la etapa B2). La información principal calculada k_u se almacena en los medios 4 de almacenamiento.

La unidad 6 de obtención de información de obtención usa la información de obtención k_{vj} leída de los medios 4 de almacenamiento y el número aleatorio generado σ_{uj} para calcular información de obtención k_{uj} que cumple $k_{uj} = \sigma_{uj} \Sigma_{i \in w(v) \setminus w(u)} u_i k_{vi} + k_{vj}$ para cada elemento $j \in w(u)$ del conjunto w(u) (en la etapa B3). La información de obtención calculada k_{uj} se almacena en los medios 4 de almacenamiento.

Tal como se ha descrito anteriormente, se genera la información K_Y correspondiente al índice Y y, a partir de la información K_Y, se obtiene información correspondiente a un índice inferior. Esto significa que, para un nodo padre A y un nodo padre B que tengan, los dos, un nodo hijo común C, se puede obtener información del nodo hijo común C a partir de información del nodo padre A y se puede obtener información del nodo hijo común C a partir de información del nodo padre B.

Caso específico 1

Se describirá a continuación un caso en el cual información de cada nodo sirve como clave en el cifrado basado en predicados, e información de un índice v^3, generada a partir de información de un índice v^1, coincide con la información del índice v^3, generada a partir de información de un índice v^2 en términos de una clave en el cifrado basado en predicados. Los índices v^1, v^2, y v^3, que se describen a continuación, son ejemplos, y se pueden aplicar los mismos aspectos a los otros índices.

Se supone que el índice $v^1 = \{v_1, v_2, *, *\}$, el índice $v^2 = \{*, *, v_3, v_4\}$ y el índice $v^3 = \{v_1, v_2, v_3, v_4\}$. A partir de la definición, $v^1 \geq v^3$ y $v^2 \geq v^3$ y el índice v^1, que actúa como nodo padre, y el índice v^2, que actúa como nodo padre, tienen el índice v^3 como nodo hijo común. En la siguiente descripción, v^i (i = 1, 2, 3) se puede indicar mediante v^i, y el elemento j-ésimo del índice v^i se puede indicar mediante v^ij.

N se fija a 5, y, a partir de N bases b_1^*, b_2^*, b_3^*, b_4^*, y b_5^*, se generan información K_{v^1} correspondiente al índice v^1 e información K_{v^2} correspondiente al índice v^2. El generador 1 de números aleatorios genera números aleatorios σ_{v^1}, σ_{v^13}, σ_{v^14}, σ_{v^2}, σ_{v^23}, σ_{v^24}, σ_{v^3}, y σ_{v^3}'.

La información K_{v^1} (información principal k_{v^1} e información de obtención k_{v^13} y k_{v^14}) correspondiente al índice v^1 es tal como se describe a continuación.

$$k_{v^1}=\sigma_{v^1}(v_1 b_1^*+v_2 b_2^*)+ b_5^*$$

$$k_{v^13}=\sigma_{v^13}(v_1 b_1^*+v_2 b_2^*)+b_3^*$$

$$k_{v^14}=\sigma_{v^14}(v_1 b_1^*+v_2 b_2^*)+b_4^*$$

La información K_{v^2} (información principal k_{v^2} e información de obtención k_{v^21} y k_{v^22}) correspondiente al índice v^2 es tal como se describe a continuación.

$$k_{v^2}=\sigma_{v^2}(v_3 b_3^*+v_4 b_4^*)+b_5^*$$

$$k_{v^21}=\sigma_{v^23}(v_3 b_3^*+v_4 b_4^*)+b_1^*$$

$$k_{v^22}=\sigma_{v^24}(v_3 b_3^*+v_4 b_4^*)+b_2^*$$

La información principal k_{v^3} correspondiente al índice v^3 se obtiene a partir de la información K_{v^1} correspondiente al índice v^1 tal como se describe a continuación.

$$\begin{aligned} k_{v^3} &= \sigma_{v^3}(v_3 k_{v^13}+v_4 k_{v^14})+ k_{v^1} \\ &=\sigma_{v^3}(v_3 \sigma_{v^13}+v_4 \sigma_{v^14})+ \sigma_{v^1})(v_1 b_1^*+ v_2 b_2^*)+\sigma_{v^3}(v_3 b_3^*+v_4 b_4^*)+b_5^* \\ &=a(v_1 b_1^*+v_2 b_2^*)+b(v_3 b_3^*+v_4 b_4^*)+b_5^* \qquad \cdots(A) \end{aligned}$$

donde $a = (\sigma_{v^3}(v_3 \sigma_{v^13} + v_4 \sigma_{v^14})+ \sigma_{v^1})$ y $b = \sigma_{v^3}$.

Se obtiene información principal k_{v^3} correspondiente al índice v^3 a partir de la información K_{v^2} correspondiente al índice v^2.

$$\begin{aligned} k_{v^3} &= \sigma_{v^3}'(v_1 k_{v^21}+v_2 k_{v^22})+k_{v^2} \\ &=(\sigma_{v^3}'(v_1\sigma_{v^23} + v_4\sigma_{v^24})+\sigma_{v^2})(v_3 b_3^*+v_4 b_4^*)+\sigma_{v^3}'(v_1 b_1^*+v_2 b_2^*)+b_5^* \\ &=c(v_1 b_1^*+v_2 b_2^*)+d(v_3 b_3^*+v_4 b_4^*)+b_5^* \qquad \cdots(B) \end{aligned}$$

donde $c = \sigma_{v^3}'$ y $d = (\sigma_{v^3}' (v_1 \sigma_{v^23} + v_4 \sigma_{v^24})+ \sigma_{v^2})$.

La información principal k_{v^3} obtenida a partir de la información K_{v^1}, mostrada en la Expresión (A), y la información principal k_{v^3} obtenida a partir de la información K_{v^2}, mostrada en la Expresión (B), no son iguales en cuanto al valor aunque son una clave del mismo valor en el cifrado basado en predicados. Más específicamente, cuando $(v_1 b_1^* + v_2 b_2^*)$ se considera como el producto interno de un vector (b_1^*, b_2^*) y un vector (v_1, v_2), la dirección del vector (v_1, v_2) con respecto al vector (b_1^*, b_2^*) es la misma en las dos Expresiones (A) y (B); cuando $(v_3 b_3^* + v_4 b_4^*)$ se considera como el producto interno de un vector (b_3^*, b_4^*) y un vector (v_3, v_4), la dirección del vector (v_3, v_4) con respecto al vector (b_3^*, b_4^*) es la misma en las dos Expresiones (A) y (B). Esto significa que las dos claves son una clave del mismo valor en el cifrado basado en predicados.

Segunda realización

La Figura 4 es un diagrama de bloques funcional a modo de ejemplo de un aparato de generación de información de acuerdo con una segunda realización.

Se supone que los grupos cíclicos G y G_T tienen un orden de número primo q; el grupo cíclico G tiene un generador g; el grupo cíclico G tiene una función de emparejamiento e: $G \times G \rightarrow G_T$, lo cual hace a $g_T = e(g, g)$ un generador del grupo cíclico G_T; un número aleatorio a se selecciona de entre Z_p de manera aleatoria; y g, $g_1 = g^a \in G$, y g_2, g_3, h_1, ..., $h_{N-1} \in G$ seleccionado aleatoriamente del grupo cíclico G se hace que estén disponibles públicamente como claves públicas.

Generación de información

El aparato de generación de información y un método de generación de información generan información K_Y correspondiente a un índice Y usando las claves públicas en la etapa C1 a la etapa C4 de la Figura 5. La información K_Y incluye primera información principal k_Y, segunda información principal g^{rY}, e información de obtención k_{Yj}. La primera información principal k_Y y la segunda información principal g^{rY} se usan, por ejemplo, como claves de descifrado. La información de obtención k_{Yj} se usa para generar información inferior a la información K_Y correspondiente al índice Y.

El aparato de generación de información recibe el índice $Y \in I$.

Un generador 1 de números aleatorios genera un número aleatorio $r_Y \in Z_q$ (en la etapa C1). El número aleatorio generado r_Y se envía a un primer generador 21 de información principal, a un segundo generador 22 de información principal, y a un generador 3 de información de obtención.

El primer generador 21 de información principal usa el número aleatorio generado r_Y para calcular primera información principal k_Y que cumple $k_Y = g_2^a(g_3\Pi_{i \in \{1,..., N-1\} \setminus w(Y)}h_i^{Yi})^{rY}$ (en la etapa C2). La primera información principal calculada k_Y se almacena en unos medios 4 de almacenamiento.

El segundo generador 22 de información principal usa el número aleatorio generado r_Y para calcular segunda información principal g^{rY}(en la etapa C3). La segunda información principal calculada g^{rY} se almacena en los medios 4 de almacenamiento.

El generador 3 de información de obtención usa el número aleatorio generado r_Y para calcular información de obtención k_{Yj} que cumple $k_{Yj} = h_j^{rY}$ para cada elemento $j \in w(Y)$ de un conjunto w(Y) (en la etapa C4). La información de obtención calculada k_{Yj} se almacena en los medios 4 de almacenamiento.

Obtención de información

El aparato y el método de generación de información generan información K_u correspondiente a un índice inferior u a partir de información K_v correspondiente a un índice superior v, donde $u \leq v$, en la etapa D1 a la etapa D4 mostradas en la Figura 6.

La información K_v correspondiente al índice v incluye primera información principal k_v, segunda información principal g^{rv}, e información de obtención k_{vj}. La primera información principal k_v y la segunda información principal g^{rv} se usan, por ejemplo, como claves de descifrado. La información de obtención k_{vj} se usa para generar información inferior a la información K_v correspondiente al índice v. Por ejemplo, el índice v = Y y la información $K_v = K_Y$. La información K_u generada en el procesado de las etapas D1 a D4 se puede considerar como información nueva K_v para generar información $K_{u'}$ ($u' \leq u$) inferior a la información K_u correspondiente al índice u.

La información K_u correspondiente al índice u incluye primera información principal k_u, segunda información principal g^{ru}, e información de obtención k_{uj}. La primera información principal k_u y la segunda información principal g^{ru} se usan, por ejemplo, como claves de descifrado. La información de obtención k_{uj} se usa para generar información inferior a la información K_u correspondiente al índice u.

El aparato de generación de información recibe el índice v y el índice u.
Se supone que los medios 4 de almacenamiento han almacenado la información K_v correspondiente al índice v.

El generador 1 de números aleatorios genera un número aleatorio r_u (en la etapa D1). El número aleatorio generado se envía a una primera unidad 51 de obtención de información principal, a una segunda unidad 52 de obtención de información principal, y a una unidad 6 de obtención de información de obtención.

La primera unidad 51 de obtención de información principal, usa la primera información principal k_v y la información de obtención k_{vi}, que se leen las dos a partir de los medios 4 de almacenamiento, y el número aleatorio generado r_u para calcular primera información principal k_u correspondiente al índice u, que cumple $k_u = k_v(\Pi_{i \in w(v) \setminus w(u)}k_{vi}^{ui})(g_3\Pi_{i \in \{1,..., N-1\} \setminus w(v)}h_i^{vi}\Pi_{i \in w(v) \setminus w(u)}h_i^{ui})^{ru}$ (en la etapa D2). La primera información principal calculada k_u se almacena en los medios 4 de almacenamiento.

La segunda unidad 52 de obtención de información principal usa el número aleatorio generado r_u para generar segunda información principal g^{ru} (en la etapa D3). La segunda información principal calculada g^{ru} se almacena en los medios 4 de almacenamiento.

La unidad 6 de obtención de información de obtención usa la información de obtención k_{vi} leída de los medios de almacenamiento y el número aleatorio generado r_u para calcular información de obtención k_{uj} que cumple $k_{uj} = k_{vj}h_j^{ru}$ para cada elemento $j \in w(u)$ de un conjunto w(u) (en la etapa D4). La información de obtención calculada k_{uj} se almacena en los medios 4 de almacenamiento.

Tal como se ha descrito anteriormente, la información K_Y correspondiente al índice Y es generada e información correspondiente a un índice inferior es obtenida a partir de la información K_Y. Esto significa que, para un nodo padre A y un nodo padre B que tengan, los dos, un nodo hijo común C, se puede obtener información del nodo hijo común C a partir de información del nodo padre A, y se puede obtener información del nodo hijo común C a partir de información del nodo padre B.

Caso específico 2

A continuación se describirá un caso en el cual información de cada nodo sirve como clave en el cifrado basado predicados e información de un índice v^3, generado a partir de información de un índice v^1 coincide con información del índice v^3, generada a partir de información de un índice v^2 en términos de una clave en el cifrado basado en predicados. Los índices v^1, v^2, y v^3, descritos posteriormente, son ejemplos, y pueden aplicarse los mismos aspectos o los otros índices.

Se supone que el índice $v^1 = \{v_1, v_2, *, *)$, el índice $v^2 = \{*, *, v_3, v_4\}$, y el índice $v^3 = \{v_1, v_2, v_3, v_4\}$. A partir de la definición, $v^1 \geq v^3$ y $v^2 \geq v^3$, y el índice v^1, que actúa como nodo padre, y el índice v^2, que actúa como nodo padre, tienen el índice v^3 como nodo hijo común. En la siguiente descripción, v^i (i = 1, 2, 3) se puede indicar mediante v^i, y el elemento j-ésimo del índice v^i se puede indicar mediante v^ij.

Se supone que N se fija a 5 y $g_1 = g^a$, g_2, g_3, h_1, h_2, h_3, $h_4 \in G$ se hacen disponibles públicamente como claves públicas. A partir de estas claves públicas, se generan información K_{v^1} correspondiente al índice v^1 e información K_{v^2} correspondiente al índice v^2. Por medio del generador 1 de números aleatorios se generan números aleatorios r_{v^1} y r_{v^2}.

La información K_{v^1} (primera información principal k_{v^1}, segunda información principal g^{rv^1}, e información de obtención k_{v^13} y k_{v^14}) correspondiente al índice v^1 es tal como se describe a continuación.

$$k_{v^1} = g_2^{\,a}(g_3 h_1^{\,v1} h_2^{\,v2})^{rv^1}$$

$$g^{rv^1}$$

$$k_{v^13} = h_3^{\,rv^1}$$

$$k_{v^14} = h_4^{\,rv^1}$$

La información K_{v^2} (primera información principal k_{v^2}, segunda información de obtención principal g^{rv^2}, e información de obtención k_{v^21} y k_{v^22}) correspondiente al índice v^2 es tal como se describe a continuación.

$$k_{v^2} = g_2^{\,s}(g_3 h_3^{\,v3} h_4^{\,v4})^{rv^2}$$

$$g^{rv^2}$$

$$k_{v^21} = h_1^{\,rv^2}$$

$$k_{v^22} = h_2^{\,rv^2}$$

La primera información principal k_{v^3} correspondiente al índice v^3 se obtiene a partir de la información K_{v^1} correspondiente al índice v^1 según se describe a continuación.

$$k_{v^3} = k_{v^1}(k_{v^13}^{\,v3} k_{v^14}^{\,v4})(g_3 h_1^{\,v1} h_2^{\,v2} h_3^{\,v3} h_4^{\,v4})^{rv^3}$$

$$= g_2^{\,a}(g_3 h_1^{\,v1} h_2^{\,v2} h_3^{\,v3} h_4^{\,v4})^{r} \quad \cdots(C)$$

donde r_{v^3} es un número aleatorio generado por el generador 1 de números aleatorios, y $r = r_{v^1} + r_{v^3}$.

La primera información principal k_{v^3} correspondiente al índice v^3 se obtiene a partir de la información K_{v^2} correspondiente al índice v^2 según se describe a continuación.

$$k_{v^3} = k_{v^1}(k_{v^13}^{\,v3} k_{v^14}^{\,v4})(g_3 h_1^{\,v1} h_2^{\,v2} h_3^{\,v3} h_4^{\,v4})^{rv^3}$$

$$= g_2^{\,a}(g_3 h_1^{\,v1} h_2^{\,v2} h_3^{\,v3} h_4^{\,v4})^{r} \quad \cdots(D)$$

donde $r_{v\hat{}3'}$ es un número aleatorio y $r' = r_{v\hat{}2} + r_{v\hat{}3'}$.

La primera información principal $k_{v\hat{}3}$ obtenida a partir de la información $K_{v\hat{}1}$, mostrada en la Expresión (C), y la segunda información principal $g^{rv\hat{}3}$, y la primera información principal $k_{v\hat{}3}$ obtenida a partir de la información $K_{v\hat{}2}$, mostrada en la Expresión (D), y la segunda información principal $g^{rv\hat{}3'}$ no son iguales en cuanto a valor, pero son una clave con el mismo valor en el cifrado basado en predicados puesto que las relaciones de los exponentes de las claves públicas g_3, h_1, h_3 y h_4, son iguales.

Modificaciones y otros

En cada una de las realizaciones antes descritas, el aparato de generación de información incluye todos de entre el generador 2 de información principal, el generador 3 de información de obtención, la unidad 5 de obtención de información principal, y la unidad 6 de obtención de información de obtención, aunque es necesario que el aparato de generación de información posea por lo menos uno de ellos. Por ejemplo, el aparato de generación de información puede tener solamente el generador 2 de información principal y el generador 3 de información de obtención. Alternativamente, el aparato de generación de información puede tener solamente la unidad 5 de obtención de información principal y la unidad 6 de obtención de información de obtención, y puede usar la información K_v ya generada y almacenada en los medios 4 de almacenamiento para generar la información K_u.

Cada operación definida en el cuerpo finito F_q se puede sustituir por una operación definida en un anillo finito Z_q de orden q. Un ejemplo de sustitución de cada operación definida en el cuerpo finito F_q por una operación definida en el anillo finito Z_q es un método en el que se permite una q diferente a un número primo o su potencia.

Cada uno de los aparatos de generación de información antes descritos se puede implementar por medio de un ordenador. En ese caso, los detalles de procesado de las funciones que debería proporcionar el aparato se describen en un programa. Cuando un ordenador ejecuta el programa, las funciones de procesado del aparato se implementan en el ordenador.

El programa de generación de información que contiene los detalles de procesado se puede grabar en un soporte de grabación legible por ordenador. El aparato de generación de información se configura cuando un ordenador ejecuta el programa. Por lo menos una parte de los detalles de procesado se puede implementar mediante hardware.

La presente invención no se limita a las realizaciones antes descritas. Son posibles cualesquiera modificaciones dentro del alcance de la presente invención.

REIVINDICACIONES

1. Aparato de generación de información que comprende:

un generador (1) de números aleatorios adaptado para generar un número aleatorio $\sigma_Y \in Z_q$ y un número aleatorio $\sigma_{Yj} \in Z_q$ correspondiente a cada elemento $j \in w(Y)$ de un conjunto w(Y);
un generador (2) de información principal adaptado para usar el número aleatorio generado σ_Y con el fin de calcular información principal k_Y que cumple $k_Y = \sigma_Y \Sigma_{i \in \{1, ..., N-1\} \setminus w(Y)} Y_i b_i^* + b_N^*$; y
un generador (3) de información de obtención adaptado para usar el número aleatorio generado σ_{Yj} con el fin de calcular información de obtención k_{Yj} que cumple $k_{Yj} = \sigma_{Yj} \Sigma_{i \in \{1, ..., N-1\} \setminus w(Y)} Y_i b_i^* + b_j^*$ para cada elemento $j \in w(Y)$ del conjunto w(Y);
donde e es una función bilineal, no degenerada, que da salida a un elemento de un grupo cíclico G_T como respuesta a entradas de N elementos γ_L (L = 1, ..., N) ($N \geq 2$) de un grupo cíclico G_1 y N elementos γ_L^* (L = 1, ..., N) de un grupo cíclico G_2; $b_i \in G_1^N$ (i = 1, ..., N) es un vector base N-dimensional que tiene N elementos del grupo cíclico G_1 como elementos; $b_j^* \in G_2^N$ (j = 1, ..., N) es un vector base N-dimensional que tiene N elementos del grupo cíclico G_2 como elementos; un valor de función correspondiente a la función e obtenido cuando cada elemento del vector base $b_i \in G_1^N$ (i = 1, ..., N) y cada elemento del vector base $b_j^* \in G_2^N$ (j = 1, ..., N) se ponen en la función bilineal e está representado por $g_T^{\tau \cdot \delta(i,j)} \in G_T$, usando una función delta de Kronecker en la cual $\delta(i, j) = 1_F$ cuando i = j y $\delta(i, j) = 0_F$ cuando $i \neq j$; 0_F es un elemento unitario aditivo de un cuerpo finito F_q; 1_F es un elemento unitario multiplicativo del cuerpo finito F_q; τ es un elemento del cuerpo finito F_q, diferente de 0_F; y F_q es idéntico a Z_q, g_T es un generador del grupo cíclico G_T, q es un número primo, los grupos G_1, G_2, y G_T son de orden q; y
* indica un carácter indeterminado, un índice Y es $Y = (Y_1, ..., Y_{N-1}) \in I = (F_q \cup \{*\})^{N-1}$, el conjunto w(Y) se corresponde con el índice Y, y $w(Y) = \{i | Y_i = *\}$,
en donde el generador de números aleatorios está adaptado además para generar un número aleatorio $\sigma_u \in Z_q$,
comprendiendo el aparato de generación de información:

una unidad (4) de almacenamiento adaptada para almacenar información principal k_v correspondiente a un índice v e información de obtención k_{vj} correspondiente al índice v; y
una unidad (5) de obtención de información principal adaptada para usar la información principal k_v e información de obtención k_{vi}, que se leen, las dos, de la unidad de almacenamiento, y el número aleatorio generado σ_u para calcular información principal k_u correspondiente a un índice u, que cumple $k_u = \sigma_u \Sigma_{i \in w(v) \setminus w(u)} u_i k_{vi} + k_v$:

donde * indica un carácter indeterminado; el índice v es $v = (v_1, ..., v_{N-1}) \in I = (F_q \cup \{*\})^{N-1}$; w(v) es un conjunto correspondiente al índice v y $w(v) = \{i | v_i = *\}$; el índice u es $u = (u_1, ..., u_{N-1}) \in I = (F_q \cup \{*\})^{N-1}$; w(u) es un conjunto correspondiente al índice u y $w(u) = \{i | u_i = *\}$; $w(u) \subset w(v)$; y $v_i = u_i$ ($i \in \{1, ..., N-1\} \setminus w(v)$); y
donde cada una de la información principal k_Y, la información principal k_v y la información principal k_u está adaptada para ser usada como información de claves en el cifrado basado en predicados.

2. Aparato de generación de información según la reivindicación 1, en el que el generador (1) de números aleatorios genera además un número aleatorio $\sigma_{uj} \in Z_q$, correspondiente a cada elemento $j \in w(u)$ del conjunto w(u);
comprendiendo además el aparato de generación de información:

una unidad (6) de obtención de información de obtención, adaptada para usar la información de obtención k_{vj} leída de la unidad de almacenamiento y el número aleatorio generado σ_{uj} con el fin de calcular información de obtención k_{uj} correspondiente al índice u, que cumple $k_{uj} = \sigma_{uj} \Sigma_{i \in w(v) \setminus w(u)} u_i k_{vi} + k_{vj}$, para cada elemento $j \in w(u)$ del conjunto w(u).

3. Aparato de generación de información que comprende:

una unidad (4) de almacenamiento adaptada para almacenar información principal k_v correspondiente a un índice v, actuando la información principal k_v como información principal k_Y o información principal obtenida a partir de la información principal k_Y e información de obtención k_{Yj}, e información de obtención k_{vj} correspondiente al índice v, actuando la información de obtención k_{vj} como información de obtención k_{Yj} o información de obtención obtenida a partir de la información de obtención k_{Yj};
un generador (1) de números aleatorios adaptado para generar un número aleatorio $\sigma_u \in Z_q$; y
una unidad (5) de obtención de información principal adaptada para usar la información principal k_v e información de obtención k_{vi}, que se leen, las dos, de la unidad de almacenamiento, y el número aleatorio

generado σ_u con el fin de calcular información principal k_u correspondiente a un índice u, que cumple $k_u = \sigma_u \Sigma_{i \in w(v) \setminus w(u)} u_i k_{vi} + k_v$;
donde e es una función bilineal, no degenerada, que da salida a un elemento de un grupo cíclico G_T como respuesta a entradas de N elementos γ_L (L = 1, ..., N) (N ≥ 2) de un grupo cíclico G_1 y N elementos γ_L* (L = 1, ..., N) de un grupo cíclico G_2; $b_i \in G_1^N$ (i = 1, ..., N) es un vector base N-dimensional que tiene N elementos del grupo cíclico G_1 como elementos; $b_j^* \in G_2^N$ (j = 1, ..., N) es un vector base N-dimensional que tiene N elementos del grupo cíclico G_2 como elementos; un valor de función correspondiente a la función e obtenido cuando cada elemento del vector base $b_i \in G_1^N$ (i = 1, ..., N) y cada elemento del vector base $b_j^* \in G_2^N$ (j = 1, ..., N) se ponen en la función bilineal e está representado por $g_T^{\tau \cdot \delta(i,j)} \in G_T$, usando una función delta de Kronecker en la cual $\delta(i, j) = 1_F$ cuando i = j y $\delta(i, j) = 0_F$ cuando $i \neq j$; 0_F es un elemento unitario aditivo de un cuerpo finito F_q; 1_F es un elemento unitario multiplicativo del cuerpo finito F_q; τ es un elemento del cuerpo finito F_q, diferente de 0_F; y F_q es idéntico a Z_q, g_T es un generador del grupo cíclico G_T, q es un número primo, los grupos G_1, G_2, y G_T son de orden q;
* indica un carácter indeterminado; un índice Y es $Y = (Y_1, ..., Y_{N-1}) \in I = (F_q \cup \{*\})^{N-1}$; un conjunto w(Y) correspondiente al índice Y es $w(Y) = \{i | Y_i = *\}$; $\sigma_Y \in Z_q$ es un número aleatorio; $\sigma_{Yi} \in Z_q$ es un número aleatorio correspondiente a cada elemento $j \in w(Y)$ del conjunto w(Y); la información principal k_Y se corresponde con el índice Y y cumple $k_Y = \sigma_Y \Sigma_{i \in \{1,..., N-1\} \setminus w(Y)} Y_i b_i^* + b_N^*$; y la información de obtención k_{Yj} se corresponde con el índice Y y cumple $k_{Yj} = \sigma_{Yj} \Sigma_{i \in \{1, ..., N-1\} \setminus w(Y)} Y_i b_i^* + b_j^*$;
* indica un carácter indeterminado; el índice v es $v = (v_1, ..., v_{N-1}) \in I = (F_q \cup \{*\})^{N-1}$; el índice u es $u = (u_1, ..., u_{N-1}) \in I = (F_q \cup \{*\})^{N-1}$; w(v) es un conjunto correspondiente al índice v y $w(v) = \{i | v_i = *\}$; w(u) es un conjunto correspondiente al índice u y $w(u) = \{i | u_i = *\}$; $w(u) \subset w(v)$; y $v_i = u_i$ ($i \in \{1, ..., N-1\} \setminus w(v)$); y
donde cada una de la información principal k_Y, la información principal k_v y la información principal k_u está adaptada para ser usada como información de claves en el cifrado basado en predicados.

4. Aparato de generación de información según la reivindicación 3, en el que el generador (1) de números aleatorios genera además un número aleatorio $\sigma_{uj} \in Z_q$, correspondiente a cada elemento $j \in w(u)$ del conjunto w(u);
comprendiendo además el aparato de generación de información:
una unidad (6) de obtención de información de obtención, adaptada para usar la información de obtención k_{vj} leída de la unidad de almacenamiento y el número aleatorio generado σ_{uj} con el fin de calcular información de obtención k_{uj} que cumple $k_{uj} = \sigma_{uj} \Sigma_{i \in w(v) \setminus w(u)} u_i k_{vi} + k_{vj}$, para cada elemento $j \in w(u)$ del conjunto w(u).

5. Método de generación de información, que comprende:

una etapa de generación de números aleatorios en la que se genera, en un generador de números aleatorios, un número aleatorio $\sigma_Y \in Z_q$ y un número aleatorio $\sigma_{Yj} \in Z_q$ correspondiente a cada elemento $j \in w(Y)$ de un conjunto w(Y);
una etapa de generación de información principal en la que se usa, en un generador de información principal, el número aleatorio generado σ_Y con el fin de calcular información principal k_Y que cumple $k_Y = \sigma_Y \Sigma_{i \in \{1, ..., N-1\} \setminus w(Y)} Y_i b_i^* + b_N^*$; y
una etapa de generación de información de obtención en la que se usa, en un generador de información de obtención, el número aleatorio generado σ_{Yj} con el fin de calcular información de obtención k_{Yj} que cumple $k_{Yj} = \sigma_{Yj} \Sigma_{i \in \{1, ..., N-1\} \setminus w(Y)} Y_i b_i^* + b_j^*$ para cada elemento $j \in w(Y)$ del conjunto w(Y);
donde e es una función bilineal, no degenerada, que da salida a un elemento de un grupo cíclico G_T como respuesta a entradas de N elementos γ_L (L = 1, ..., N) (N ≥ 2) de un grupo cíclico G_1 y N elementos γ_L* (L = 1, ..., N) de un grupo cíclico G_2; $b_i \in G_1^N$ (i = 1, ..., N) es un vector base N-dimensional que tiene N elementos del grupo cíclico G_1 como elementos; $b_j^* \in G_2^N$ (j = 1, ..., N) es un vector base N-dimensional que tiene N elementos del grupo cíclico G_2 como elementos; un valor de función correspondiente a la función e obtenido cuando cada elemento del vector base $b_i \in G_1^N$ (i = 1, ..., N) y cada elemento del vector base $b_j^* \in G_2^N$ (j = 1, ..., N) se ponen en la función bilineal e está representado por $g_T^{\tau \cdot \delta(i,j)} \in G_T$, usando una función delta de Kronecker en la cual $\delta(i, j) = 1_F$ cuando i = j y $\delta(i, j) = 0_F$ cuando $i \neq j$; 0_F es un elemento unitario aditivo de un cuerpo finito F_q; 1_F es un elemento unitario multiplicativo del cuerpo finito F_q; τ es un elemento del cuerpo finito F_q, diferente de 0_F; y F_q es idéntico a Z_q, g_T es un generador del grupo cíclico G_T, q es un número primo, los grupos G_1, G_2, y G_T son de orden q; y
* indica un carácter indeterminado, un índice Y es $Y = (Y_1, ..., Y_{N-1}) \in I = (F_q \cup \{*\})^{N-1}$, y el conjunto w(Y) se corresponde con el índice Y, y $w(Y) = \{i | Y_i = *\}$,
en donde la etapa de generación de números aleatorios genera además un número aleatorio $\sigma_u \in Z_q$,
comprendiendo además el método de generación de información,
una etapa de obtención de información principal en la que, usando una información principal k_v y una información de obtención k_{vi}, que se leen, las dos, de una unidad de almacenamiento, y el número aleatorio generado σ_u, se calcula información principal k_u correspondiente a un índice u, que cumple $k_u = \sigma_u \Sigma_{i \in w(v) \setminus w(u)} u_i k_{vi} + k_v$, estando adaptada la unidad de almacenamiento para almacenar la información principal k_v correspondiente a un índice v y la información de obtención k_{vj} correspondiente al índice v,

donde * indica un carácter indeterminado; el índice v es $v = (v_1, ..., v_{N-1}) \in I = (F_q \cup \{*\})^{N-1}$; w(v) es un conjunto correspondiente al índice v y $w(v) = \{i|v_i = *\}$; el índice u es $u = (u_1, ..., u_{N-1}) \in I = (F_q \cup \{*\})^{N-1}$; w(u) es un conjunto correspondiente al índice u y $w(u) = \{i|u_i = *\}$; $w(u) \subset w(v)$; y $v_i = u_i$ ($i \in \{1, ..., N-1\} \setminus w(v)$); y
donde cada una de la información principal k_Y, la información principal k_v y la información principal k_u se usa como información de claves en el cifrado basado en predicados.

6. Programa de generación de información que consigue que un ordenador funcione como cada unidad del aparato de generación de información según una de las reivindicaciones 1 a 4.

7. Soporte de grabación legible por ordenador que tiene almacenado en el mismo el programa de generación de información según la reivindicación 6.

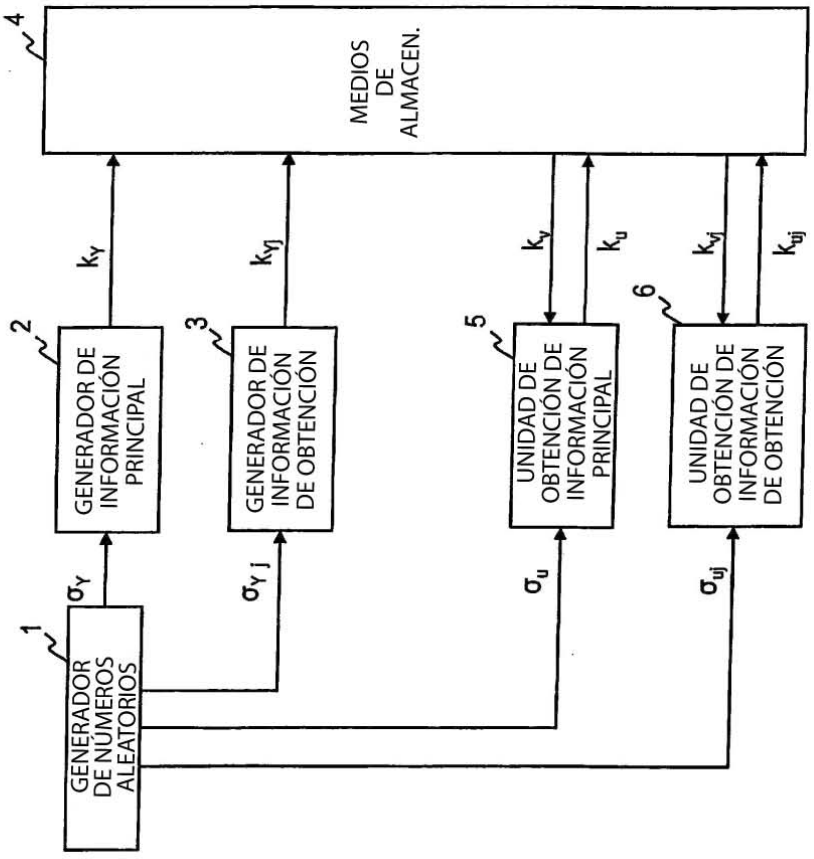

4
MEDIOS DE ALMACEN.
2
GENERADOR DE INFORMACIÓN PRINCIPAL
3
GENERADOR DE INFORMACIÓN DE OBTENCIÓN
5
UNIDAD DE OBTENCIÓN DE INFORMACIÓN PRINCIPAL
6
UNIDAD DE OBTENCIÓN DE INFORMACIÓN DE OBTENCIÓN
1
GENERADOR DE NÚMEROS ALEATORIOS
k_γ
$k_{\gamma j}$
k_u
k_{uj}
σ_γ
$\sigma_{\gamma j}$
σ_u
σ_{uj}

FIG.1

FIG.2

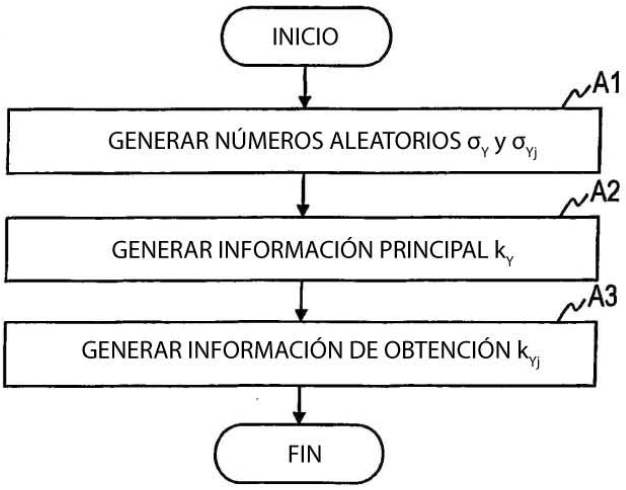

INICIO
A1
GENERAR NÚMEROS ALEATORIOS σ_Y y σ_{Yj}
A2
GENERAR INFORMACIÓN PRINCIPAL k_Y
A3
GENERAR INFORMACIÓN DE OBTENCIÓN k_{Yj}
FIN

FIG.3

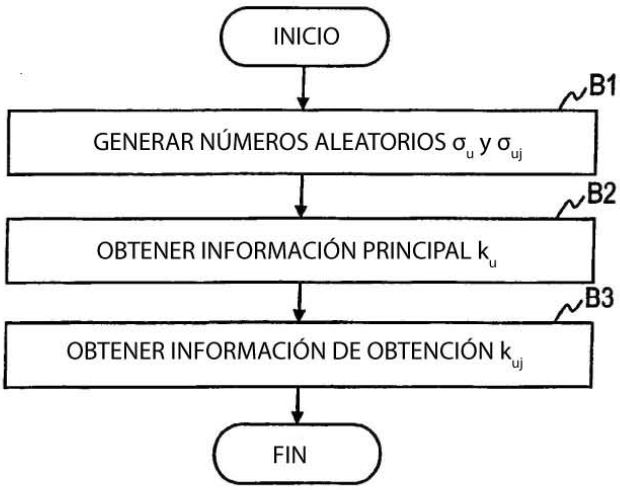

INICIO
B1
GENERAR NÚMEROS ALEATORIOS σ_u y σ_{uj}
B2
OBTENER INFORMACIÓN PRINCIPAL k_u
B3
OBTENER INFORMACIÓN DE OBTENCIÓN k_{uj}
FIN

FIG.4

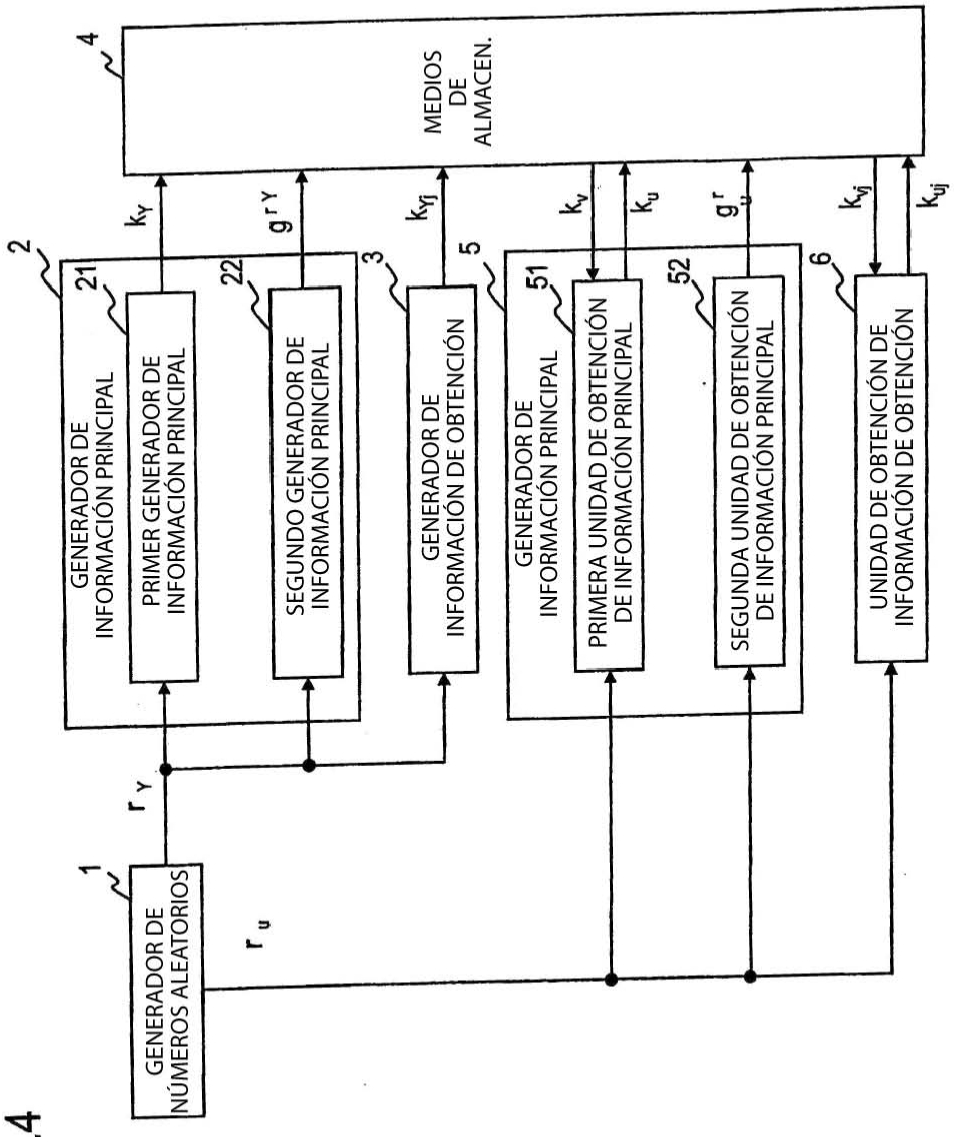

4
MEDIOS DE ALMACEN.
2
GENERADOR DE INFORMACIÓN PRINCIPAL
21
PRIMER GENERADOR DE INFORMACIÓN PRINCIPAL
22
SEGUNDO GENERADOR DE INFORMACIÓN PRINCIPAL
3
GENERADOR DE INFORMACIÓN DE OBTENCIÓN
5
GENERADOR DE INFORMACIÓN PRINCIPAL
51
PRIMERA UNIDAD DE OBTENCIÓN DE INFORMACIÓN PRINCIPAL
52
SEGUNDA UNIDAD DE OBTENCIÓN DE INFORMACIÓN PRINCIPAL
6
UNIDAD DE OBTENCIÓN DE INFORMACIÓN DE OBTENCIÓN
1
GENERADOR DE NÚMEROS ALEATORIOS
k_Y
g^{rY}
k_{Yj}
k_v
k_u
g^r_u
k_{uj}
k_{ij}
r_Y
r_u

FIG.5

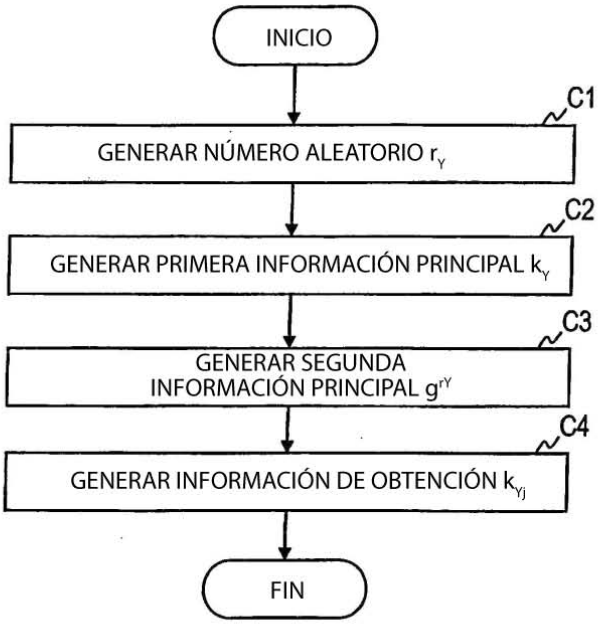
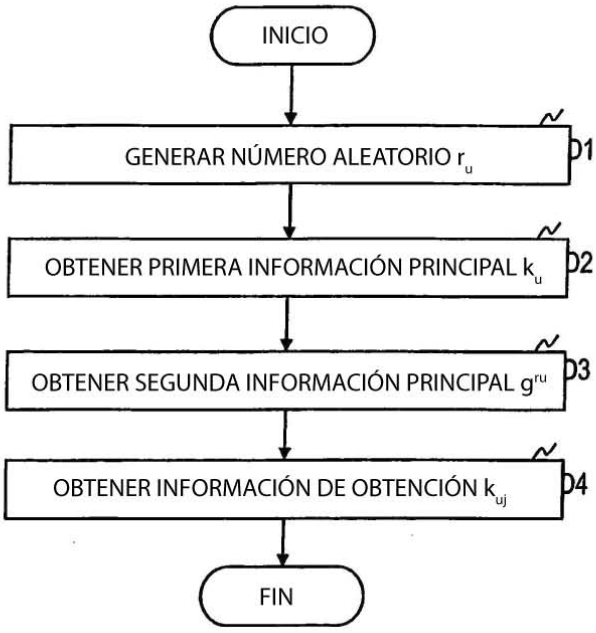

INICIO
C1
GENERAR NÚMERO ALEATORIO r_Y
C2
GENERAR PRIMERA INFORMACIÓN PRINCIPAL k_Y
C3
GENERAR SEGUNDA INFORMACIÓN PRINCIPAL g^{rY}
C4
GENERAR INFORMACIÓN DE OBTENCIÓN k_{Yj}
FIN

FIG.6


INICIO
GENERAR NÚMERO ALEATORIO r_u
D1
OBTENER PRIMERA INFORMACIÓN PRINCIPAL k_u
D2
OBTENER SEGUNDA INFORMACIÓN PRINCIPAL g^{ru}
D3
OBTENER INFORMACIÓN DE OBTENCIÓN k_{uj}
D4
FIN