(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 696 530**

(51) Int. CI.:

G06F 7/72 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.06.2016 E 16176068 (1)**

(97) Fecha y número de publicación de la concesión europea: **15.08.2018 EP 3121710**

(54) Título: **Procedimiento de cálculo, dispositivo de cálculo y producto de software de cálculo para dominio de Montgomery**

(30) Prioridad:

22.07.2015 IL 24010015

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.01.2019

(73) Titular/es:

WINBOND ELECTRONICS CORP. (100.0%)
No. 8 Keya 1st Rd., Daya District, Central Taiwan Science Park,
Taichung City, Taiwan., TW

(72) Inventor/es:

KALUZHNY, URI

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento de cálculo, dispositivo de cálculo y producto de software de cálculo para dominio de Montgomery

Antecedentes de la invención

1. Campo de la invención

La presente invención se refiere, en general, a circuitos y procedimientos de cálculo, y en particular a cálculos modulares eficaces.

2. Descripción de la técnica relacionada

En la criptografía de curva elíptica (ECC), las operaciones aritméticas se realizan sobre los puntos de una curva elíptica elegida. Estos puntos pueden representarse en la forma canónica convencional como pares de números (x, y) que cumplen una ecuación específica. En la mayoría de los casos, esta ecuación puede escribirse en la forma corta de Weierstrass como $y^2 = x^3 + A * x + B$, en la que A y B son constantes que definen la curva elíptica. Los números A, B, x e y se toman de un campo finito fijo, tal como el campo de los números enteros con módulo M, en la que M es un número primo grande, y las operaciones en los números se realizan sobre este campo.

En general, los algoritmos de ECC implican dos operaciones que se realizan a través de los puntos de una curva elíptica elegida:

$$\text{Suma de punto: } (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

$$\text{Duplicación de punto: } 2(x_1, y_1) = (x_3, y_3)$$

La definición directa de estas operaciones implica la división modular, que es una operación pesada y que requiere mucho tiempo.

Por lo tanto, es una práctica común representar los puntos de la curva elíptica en las coordenadas alternativas que permiten las operaciones de suma de punto y duplicación de punto a realizar como una secuencia de sumas y multiplicaciones modulares. Las coordenadas jacobianas se usan ampliamente para este fin, en el que cada punto (x, y) en la curva elíptica está representado por tres números (*X, Y, Z*), elegidos de tal manera que las coordenadas elípticas originales x e y puedan expresarse como cocientes de potencias de las coordenadas alternativas X, Y y Z: x = XZ 2, y = YZ 3

$$x = \frac{X}{Z^2}, \qquad y = \frac{Y}{Z^3}$$

Otras representaciones que pueden usarse de una manera similar para aumentar la eficacia de cálculo sobre curvas elípticas incluyen coordenadas proyectivas (en las que x = X/Z e y = Y/Z); coordenadas W12 (x = X/Z, y = Y/Z^2); coordenadas XYZZ (x = X/ZZ, y = Y/ZZZ, y $ZZ^3 = ZZZ^2$); y coordenadas XZ (x = X/Z). Las representaciones de este tipo se mencionan en la presente descripción y en las reivindicaciones como “representaciones basadas en cociente”, ya que cada una de las coordenadas elípticas x e y se representa como un cociente de ciertas potencias de las coordenadas alternativas. Se puede encontrar más información sobre tales representaciones y su uso en cálculos de curvas elípticas en el sitio web hyperelliptic.org.

Incluso en las coordenadas Jacobianas, sin embargo, los cálculos de curvas elípticas consumen mucho tiempo. El procedimiento clásico para calcular un producto modular implica en primer lugar multiplicar los operandos como números enteros no modulares y a continuación tomar el módulo del resultado, denominado como “reducción modular”. La reducción modular en sí misma supone cálculos costosos, equivalentes a una división larga. La duplicación de puntos y la adición de puntos implican muchas operaciones de este tipo.

Por esta razón, los cálculos criptográficos a menudo usan un procedimiento más eficiente, conocido como multiplicación modular de Montgomery (o simplemente la multiplicación de Montgomery). Para realizar la multiplicación de Montgomery, los operandos se convierten a una forma especial de Montgomery usando un algoritmo conocido como reducción de Montgomery. La multiplicación de los operandos en la forma de Montgomery evita la necesidad de una reducción modular tal como se requiere en la aritmética convencional. Los algoritmos de reducción y multiplicación de Montgomery se describen, por ejemplo, por Menezes y col., en el Handbook of Applied Cryptography (1996), sección 14.3.2, páginas 600-603, que se incorpora en el presente documento como referencia.

Para resumir brevemente, dados dos grandes números enteros *A* y *B*, en lugar de calcular *A* * *B*, la multiplicación de Montgomery produce *A* ʘ *B* = A * B * R^{-1} % *M*, en la que *R* es una constante que depende de la longitud del módulo *M*. (El símbolo “%” se usa en la presente descripción y en las figuras para indicar “módulo”). Con este fin, los

operandos de entrada se preprocesan en primer lugar (denominados como conversión de operandos al dominio de Montgomery o a la forma de Montgomery), de tal manera que cada entrada X se convierta en *X'= X * R% M*. Los operandos en forma de Montgomery se multiplican entre sí de la siguiente manera:

$$A' \odot B' = \mathrm{A} * \mathrm{R} * \mathrm{B} * R * R^{-1} \ \% M = (A * B)' \ \% M.$$

Una cadena de cálculos puede realizarse de esta manera en el dominio de Montgomery. El resultado final *Res*' se convierte de nuevo en una forma entera usando la multiplicación de Montgomery en 1: *Res'* Θ 1 = *Res * R * R*$^{-1}$ % *M* = *Res*.

Sumario de la invención

Las realizaciones de la presente invención que se describen a continuación en el presente documento proporcionan procedimientos y aparatos que son útiles en la simplificación y mejora de la eficacia de la operación en el dominio de Montgomery.

Por lo tanto, se proporciona, de acuerdo con una realización de la invención, un procedimiento para calcular, que incluye recibir, en un circuito multiplicador de Montgomery, un par de coordenadas (x, y) de entrada que especifican un punto de una curva elíptica en una forma canónica. El par de coordenadas de entrada se convierte en una representación basada en cociente que incluye tres coordenadas alternativas (X', Y', Z') en una forma de Montgomery realizando unas primeras multiplicaciones de Montgomery de las coordenadas de entrada por unos factores de conversión seleccionados. Una o más operaciones de curva elíptica se realizan aplicando unas segundas multiplicaciones de Montgomery a las coordenadas alternativas en la forma de Montgomery.

En una realización desvelada, las coordenadas alternativas incluyen unas coordenadas jacobianas.

Normalmente, realizar las primeras multiplicaciones de Montgomery incluye aplicar una multiplicación de Montgomery por 1 en calcular al menos una de las coordenadas alternativas. En una realización desvelada, realizar las primeras multiplicaciones de Montgomery incluye seleccionar los factores de conversión ω, α y β, en el que α y β son potencias de ω, y calcular las coordenadas alternativas como productos de Montgomery de α y β con las coordenadas de entrada, de tal manera que X' = α Θ x, Y'= (β Θ y) Θ 1, y Z' = ω, en el que el símbolo "Θ" significa multiplicación de Montgomery. En una realización, ω es un número entero aleatorio, $\alpha = \omega^2$ y $\beta = \omega^3$.

En una realización desvelada, realizar la una o más operaciones de curva elíptica incluye calcular un resultado expresado en la representación basada en cociente en la forma de Montgomery, y aplicar al menos una de las segundas multiplicaciones de Montgomery devolviendo el resultado a la forma canónica.

También se proporciona, de acuerdo con una realización de la invención, un dispositivo de cálculo, que incluye unas entradas configuradas para recibir un par de coordenadas (x, y) de entrada que especifican un punto en una curva elíptica en una forma canónica. Un circuito multiplicador de Montgomery está configurado para convertir el par de coordenadas de entrada en una representación basada en cociente que incluye tres coordenadas alternativas (X', Y', Z') en una forma de Montgomery realizando las primeras multiplicaciones de Montgomery de las coordenadas de entrada mediante unos factores de conversión seleccionados, y para realizar una o más operaciones de curva elíptica aplicando las segundas multiplicaciones de Montgomery a las coordenadas alternativas en la forma de Montgomery.

Se proporciona adicionalmente, de acuerdo con una realización de la invención, un producto de software informático, que incluye un medio legible por ordenador no transitorio en el que se almacenan instrucciones de programa, instrucciones que, cuando se leen por un procesador programable, hacen que el procesador reciba un par de coordenadas (x, y) de entrada que especifican un punto en una curva elíptica en una forma canónica. Las instrucciones hacen que el procesador convierta el par de coordenadas de entrada en una representación basada en cociente que comprende tres coordenadas alternativas (X', Y', Z') en una forma de Montgomery realizando las primeras multiplicaciones de Montgomery de las coordenadas de entrada mediante unos factores de conversión seleccionados, y para realizar una o más operaciones de curva elíptica aplicando las segundas multiplicaciones de Montgomery a las coordenadas alternativas en la forma de Montgomery.

Breve descripción de los dibujos

La presente invención se entenderá más completamente a partir de la siguiente descripción detallada de las realizaciones de la misma, tomada junto con los dibujos en los que:

La figura 1 es un diagrama de bloques que ilustra esquemáticamente unos elementos de circuito en un dispositivo criptográfico, de acuerdo con una realización de la invención; y
La figura 2 es un diagrama de flujo que ilustra esquemáticamente un procedimiento para realizar cálculos de curva elíptica, de acuerdo con una realización de la invención.

Descripción de las realizaciones

A pesar de la complejidad de cálculo de las operaciones de curva elíptica puede reducirse convirtiendo las coordenadas en una representación jacobiana (u otra representación basada en cociente) en el dominio de Montgomery, esta conversión en sí misma implica una serie de etapas de cálculo que consumen tiempo. Además, por razones de seguridad, puede desearse aleatorizar las coordenadas, por ejemplo, multiplicándolas por un factor constante, añadiendo otra etapa de cálculo.

Las realizaciones de la presente invención que se describen en el presente documento reducen la complejidad de cálculo de los cálculos de curva elíptica aún más simplificando las etapas de conversión de coordenadas. En las realizaciones desveladas, un par de coordenadas (x, y) de entrada, que especifican un punto en una curva elíptica en forma canónica, se convierten en una representación (X', Y', Z') basada en cociente alternativa en forma de Montgomery mediante las multiplicaciones de Montgomery de las coordenadas de entrada por los factores de conversión seleccionados. Una o dos multiplicaciones de Montgomery de cada una de las coordenadas de entrada son, en general, suficientes para generar cada una de X' e Y', mientras que Z' se genera mediante un cálculo aritmético simple.

El mismo circuito de multiplicación de Montgomery que realiza la conversión de coordenadas puede entonces usarse para realizar las operaciones de curva elíptica aplicando más multiplicaciones de Montgomery a las coordenadas alternativas obtenidas de este modo. La última de estas multiplicaciones de Montgomery puede usarse para devolver el resultado de estas operaciones de la representación basada en cociente en forma de Montgomery a la forma canónica.

En las realizaciones desveladas, las multiplicaciones de Montgomery que se usan en la conversión de las coordenadas (x, y) de entrada en las coordenadas alternativas (X', Y', Z') incluyen al menos una multiplicación de Montgomery por 1. Como se ha observado anteriormente, la multiplicación de Montgomery de un valor por 1 significa, en términos aritméticos ordinarios, una multiplicación por R^{-1} mod M, que introduce de este modo un factor de R^{-1} en las coordenadas basadas en cociente. Como ejemplo específico, el multiplicador de Montgomery puede usar unos factores de números enteros seleccionados ω, α y β, en el que α y β son potencias de ω, para realizar la conversión calculando los productos de Montgomery de α y β con las coordenadas de entrada, de tal manera que $X' = \alpha \Theta x$, $Y' = (\beta \Theta y) \Theta 1$, y $Z' = \omega$. Para la conversión a coordenadas jacobianas, los factores α y β se calculan como $\alpha = \omega^2$ y $\beta = \omega^3$. Con fines de aleatorización coordinada, ω puede ser un valor aleatorio o pseudoaleatorio.

Aunque las realizaciones descritas a continuación en el presente documento se refieren específicamente, en aras de la concreción y la claridad, a la representación de puntos de curva elíptica en las coordenadas jacobianas, los principios de estas realizaciones pueden extenderse de una manera directa a otras representaciones basadas en cociente, tales como, por ejemplo, las coordenadas proyectivas, las coordenadas W12, las coordenadas XYZZ o las coordenadas XZ. Se considera que todas estas implementaciones alternativas están dentro del ámbito de la presente invención.

La figura 1 es un diagrama de bloques que ilustra esquemáticamente los elementos de circuito en un dispositivo criptográfico, de acuerdo con una realización de la invención. Los elementos de circuito mostrados en la figura se implementan normalmente como circuitos lógicos de hardware en un dispositivo de circuito integrado (CI), pero como alternativa pueden implementarse como módulos en software en un procesador programable adecuado. Los circuitos ilustrados realizan cálculos de curva elíptica y funciones de multiplicación de Montgomery que pueden integrarse en el dispositivo criptográfico en una amplia variedad de configuraciones y aplicaciones diferentes, para realizar operaciones relacionadas, por ejemplo, con el cifrado, el descifrado y/o la autenticación. Solo los elementos del dispositivo 20 que son directamente relevantes para los cálculos de curva elíptica y para la multiplicación de Montgomery se muestran en la figura, y la integración de estos elementos con otros componentes del dispositivo 20 será evidente para los expertos en la materia.

El dispositivo 20 comprende una unidad 22 de cálculo elíptico, que tiene un par de entradas 24, 26 de operandos para recibir los operandos elípticos, y una entrada 40 de módulo, que recibe el valor del módulo M que se va a usar en los cálculos. La unidad 22 comprende un multiplicador 30 de Montgomery, que recibe los operandos A y B de Montgomery desde las entradas 36 y 38 internas y calcula su producto de Montgomery $A \Theta B = A * B * R^{-1} \% M$. El multiplicador 30 emite el resultado del cálculo a una salida 28, cuyos contenidos pueden entregarse a otros componentes del dispositivo 20 o retroalimentarse a una o ambas entradas 36, 38 para cálculos posteriores, tales como múltiples multiplicaciones sucesivas que se usan en los cálculos de curva elíptica.

El multiplicador 30 comprende unos circuitos aritméticos, que incluyen al menos un circuito 32 sumador y al menos un circuito 34 multiplicador, con interconexiones adecuadas para realizar los cálculos iterativos que están involucrados en la multiplicación de Montgomery de números grandes. El sumador y el multiplicador normalmente operan en bloques de un tamaño predefinido, tal como treinta y dos bits. Las entradas 24, 26, 36, 38 y 40 y la salida 28 son normalmente números enteros de longitud m = n * tamaño de bloque, o específicamente m = 32n bits en el presente ejemplo, tal como 128 bits. Las entradas y salidas pueden implementarse convenientemente como localizaciones en una matriz de memoria.

Para los fines de la conversión eficiente de los operandos elípticos en las entradas 24 y 26 en la forma de Montgomery basada en cociente aleatorizada, la unidad 22 de cálculo comprende un generador 42 de números aleatorios, que emite un valor ω entero aleatorio o pseudoaleatorio para su uso en cada una de tales conversiones. (El término "aleatorio", como se usa en la presente descripción y en las reivindicaciones, debería entenderse como que incluye también números "pseudoaleatorios", a menos que el contexto indique lo contrario). El valor ω puede ser de cualquier longitud deseada, pero es conveniente que su longitud sea igual al tamaño de bloque del multiplicador 30 de Montgomery, es decir, treinta y dos bits en el presente ejemplo. Para la conversión a la representación jacobiana, el multiplicador 30 hace uso de los valores $\alpha = \omega^2$ y $\beta = \omega^3$, que se generan mediante una multiplicación aritmética (no modular), realizada o bien por el circuito 34 multiplicador o por un multiplicador dedicado asociado con el generador 42 de números aleatorios.

La figura 2 es un diagrama de flujo que ilustra esquemáticamente un procedimiento para realizar unos cálculos de curva elíptica, de acuerdo con una realización de la invención. Este procedimiento se describe a continuación en el presente documento, en aras de la claridad y la conveniencia, haciendo referencia a los elementos del dispositivo 20 que se muestran en la figura 1. Como alternativa, el procedimiento puede realizarse, mutatis mutandis, en otras configuraciones de hardware o en software, como se ha observado anteriormente. Se considera que todas estas implementaciones alternativas están dentro del ámbito de la presente invención.

El procedimiento se inicia cuando la unidad 22 de cálculo elíptico recibe uno o más nuevos operandos en la entrada(s) 24 y/o 26, en una etapa 50 de entrada. Como se ha explicado anteriormente, las entradas comprenden las coordenadas (x, y) que especifican un punto en una curva elíptica en forma canónica. Para convertir las entradas en coordenadas jacobianas (X', Y', Z') en la forma de Montgomery, la unidad 22 solicita un valor ω aleatorio del generador 42 de números aleatorios, y calcula los parámetros aleatorios $\alpha = \omega^2$ y $\beta = \omega^3$, en una etapa 52 de generación de parámetros. Los parámetros α y β se introducen en la entrada 36 del multiplicador 30 de Montgomery, mientras que las coordenadas x e y de entrada elípticas se introducen en la entrada 38. El multiplicador 30 realiza las multiplicaciones de Montgomery de estos valores con el fin de calcular las coordenadas jacobianas, en una etapa 54 de conversión de coordenadas.

Como se ha señalado anteriormente, el multiplicador 30 de Montgomery calcula las coordenadas jacobianas en la etapa 54 de acuerdo con las siguientes fórmulas:

$$X' = \alpha \odot x, \qquad Y' = (\beta \odot y) \odot 1, \qquad Z' = \omega.$$

La validez de estas fórmulas se muestra por la siguiente derivación:

- $X' = \omega^2 * x * R^{-1} \% M = (\omega * R^{-1})^2 * x * R \% M,$
  - $X = (\omega * R^{-1})^2 * x,$
- $Y' = (\omega^3 * y * R^{-1}) * 1 * R^{-1} \% M = (\omega * R^{-1})^3 * y * R \% M,$
  - $Y = (\omega * R^{-1})^3 * y,$
- $Z' = (\omega * R^{-1}) * R \% M,$
  - $Z = (\omega * R^{-1}),$

,

Las coordenadas convertidas en forma (X, Y, Z) normal, como se proporciona por la derivación anterior, satisface de este modo la definición formal de conversión jacobiana: $x = X * Z^{-2} \% M;\ y = Y * Z^{-3} \% M.$

Los valores X', Y' y Z' de coordenadas convertidos se introducen de nuevo desde la salida 28 a las entradas 36 y 38 para su uso en operaciones posteriores por el multiplicador 30 de Montgomery, en un etapa 56 de cálculo elíptico. Normalmente, múltiples multiplicaciones de este tipo, así como sumas modulares, se usan con el fin de completar cada operación de suma de puntos o de duplicación de puntos que se solicita a la unidad 22 de cálculo elíptico.

Tras la conclusión del cálculo elíptico en la forma de Montgomery jacobiana, el resultado se introduce de nuevo desde la salida 28 a una de las entradas 36 y 38. El multiplicador 30 realiza la multiplicación de Montgomery de los resultados por 1 (en el dominio de Montgomery) para convertirlos de nuevo a las coordenadas (X, Y, Z) jacobianas normales, seguido de una división modular: $x = X * Z^{-2} \% M,\ y = Y * Z^{-3} \% M$, con el fin de convertir de nuevo el resultado final a la forma canónica para la salida de la unidad 22, en una etapa 58 de conversión de resultados.

Como se ha observado anteriormente, en una realización alternativa de la presente invención, las etapas y las operaciones descritas anteriormente se realizan por un procesador programable adecuado bajo el control de unas instrucciones de programa de software. El software puede descargarse al procesador en forma electrónica, por

ejemplo, a través de una red. Adicional o alternativamente, el software puede almacenarse en medios legibles por ordenador no transitorios, tangibles tales como unos medios de memoria ópticos, magnéticos o electrónicos.

REIVINDICACIONES

1. Un procedimiento (50, 52, 54, 56, 58) de cálculo, que comprende:

recibir, en un circuito multiplicador de Montgomery, un par de coordenadas (x, y) de entrada que especifican un punto en una curva elíptica en una forma (50) canónica;
convertir el par de coordenadas de entrada en una representación basada en cociente que comprende tres coordenadas alternativas (X', Y', Z') en una forma de Montgomery realizando unas primeras multiplicaciones ⊚ de Montgomery, que comprenden una multiplicación de Montgomery por 1 (52, 54), de las coordenadas de entrada por los factores (52, 54) de conversión seleccionados ω, α y β, en el que α y β son potencias de ω (52), para calcular las coordenadas alternativas como productos de Montgomery de α y β con las coordenadas de entrada, de tal manera que $X' = \alpha \Theta x$, $Y' = (\beta \Theta y) \Theta 1$, y $Z' = \omega$ (54); y
realizar una o más operaciones de curva elíptica aplicando las segundas multiplicaciones ⊚ de Montgomery a las coordenadas alternativas en la forma (56, 58) de Montgomery.

2. El procedimiento de acuerdo con la reivindicación 1, en el que las coordenadas alternativas comprenden unas coordenadas (54) jacobianas.

3. El procedimiento de acuerdo con la reivindicación 1, en el que realizar la una o más operaciones (56, 58) de curva elíptica comprende calcular un resultado expresado en la representación basada en cociente en la forma (56) de Montgomery y aplicar al menos una de las segundas multiplicaciones de Montgomery al devolver el resultado a la forma (58) canónica.

4. Un dispositivo (20) de cálculo, que comprende:

unas entradas (24, 26, 40) configuradas para recibir un par de coordenadas (x, y) de entrada que especifican un punto en una curva elíptica en una forma (50) canónica; y
un circuito (22) multiplicador de Montgomery, que está configurado para convertir el par de coordenadas de entrada en una representación basada en cociente que comprende tres coordenadas (X', Y', Z') alternativas en una forma de Montgomery realizando unas primeras multiplicaciones ⊚ de Montgomery, que comprenden una multiplicación de Montgomery por 1 (52, 54), de las coordenadas de entrada por los factores (52, 54) de conversión seleccionados ω, α y β, en el que α y β son potencias de ω (52), para calcular las coordenadas alternativas como productos de Montgomery de α y β con las coordenadas de entrada, de tal manera que $X' = \alpha \Theta x$, $Y' = (\beta \Theta y) \Theta 1$, y $Z' = \omega$ (54), y para realizar una o más operaciones de curva elíptica aplicando las segundas multiplicaciones ⊚ de Montgomery a las coordenadas alternativas en la forma (56, 58) de Montgomery.

5. El dispositivo de acuerdo con la reivindicación 4, en el que las coordenadas alternativas comprenden unas coordenadas (54) jacobianas.

6. El dispositivo de acuerdo con la reivindicación 4, en el que el circuito (22) multiplicador de Montgomery está configurado para realizar la una o más operaciones (56, 58) de curva elíptica calculando un resultado expresado en la representación basada en cociente en la forma (56) de Montgomery, y aplicando al menos una de las segundas multiplicaciones de Montgomery para devolver el resultado a la forma (58) canónica.

7. Un producto de software informático, que comprende un medio legible por ordenador no transitorio en el que se almacenan las instrucciones de programa, instrucciones que, cuando se leen por un procesador (20) programable, hacen que el procesador reciba un par de coordenadas (x, y) de entrada que especifican un punto en una curva elíptica en una forma (50) canónica, para convertir el par de coordenadas de entrada en una representación basada en cociente que comprende tres coordenadas (X', Y', Z') alternativas en una forma de Montgomery realizando unas primeras multiplicaciones ⊚ de Montgomery de las coordenadas de entrada por los factores (52, 54) de conversión seleccionados ω, α y β, en el que α y β son potencias de ω (52), para calcular las coordenadas alternativas como productos de Montgomery de α y β con las coordenadas de entrada, de tal manera que $X' = \alpha \Theta x$, $Y' = (\beta \Theta y) \Theta 1$, y $Z' = \omega$ (54), y para realizar una o más operaciones de curva elíptica aplicando las segundas multiplicaciones ⊚ de Montgomery a las coordenadas alternativas en la forma (56, 58) de Montgomery.

8. El producto de acuerdo con la reivindicación 7, en el que ω es un número entero aleatorio, $\alpha = \omega^2$ y $\beta = \omega^3$ (52).

9. El producto de acuerdo con la reivindicación 7, en el que las instrucciones hacen que el procesador realice la una o más operaciones (56, 58) de curva elíptica calculando un resultado expresado en la representación basada en cociente en la forma (56) de Montgomery, y aplicando al menos una de las segundas multiplicaciones de Montgomery para devolver el resultado a la forma (58) canónica.

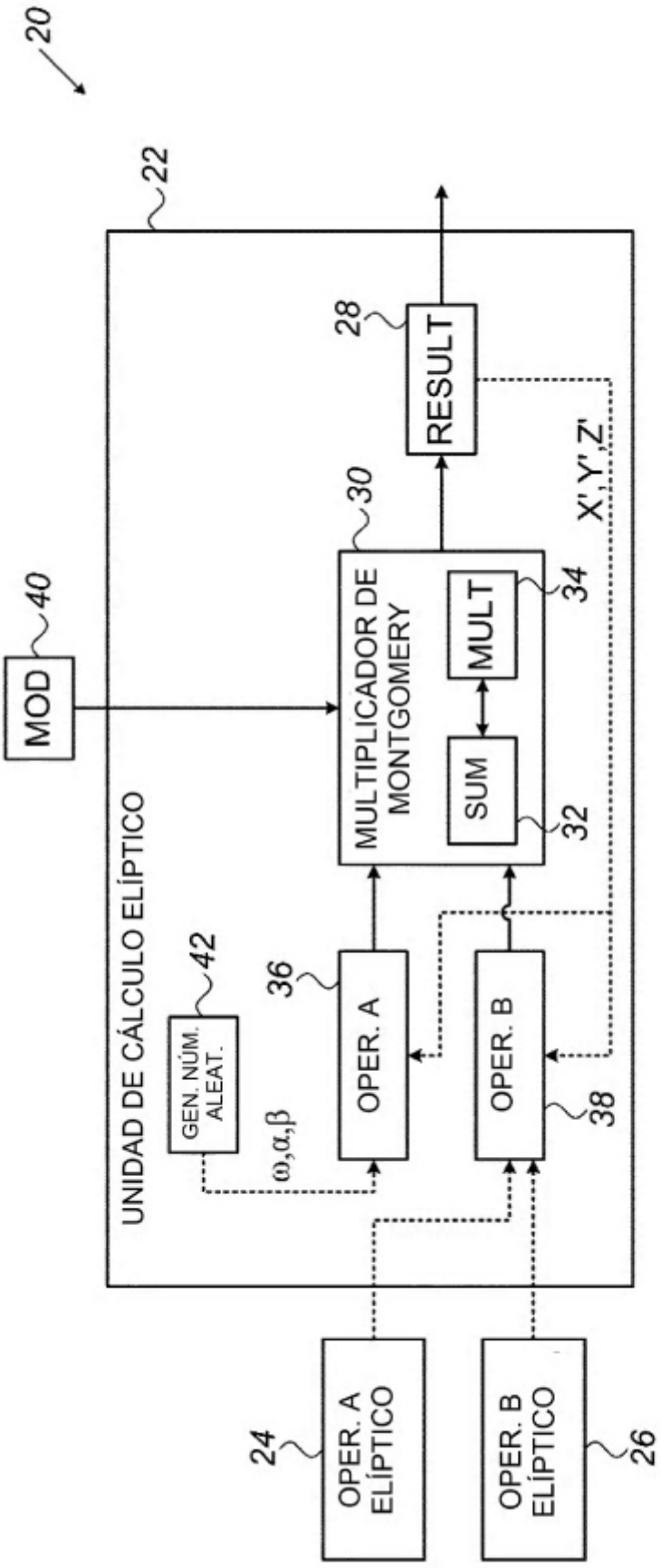
20
22
UNIDAD DE CÁLCULO ELÍPTICO
MOD
40
MULTIPLICADOR DE MONTGOMERY
30
SUM
32
MULT
34
RESULT
28
X',Y',Z'
GEN. NÚM. ALEAT.
42
ω,α,β
OPER. A
36
OPER. B
38
OPER. A ELÍPTICO
24
OPER. B ELÍPTICO
26

FIG. 1

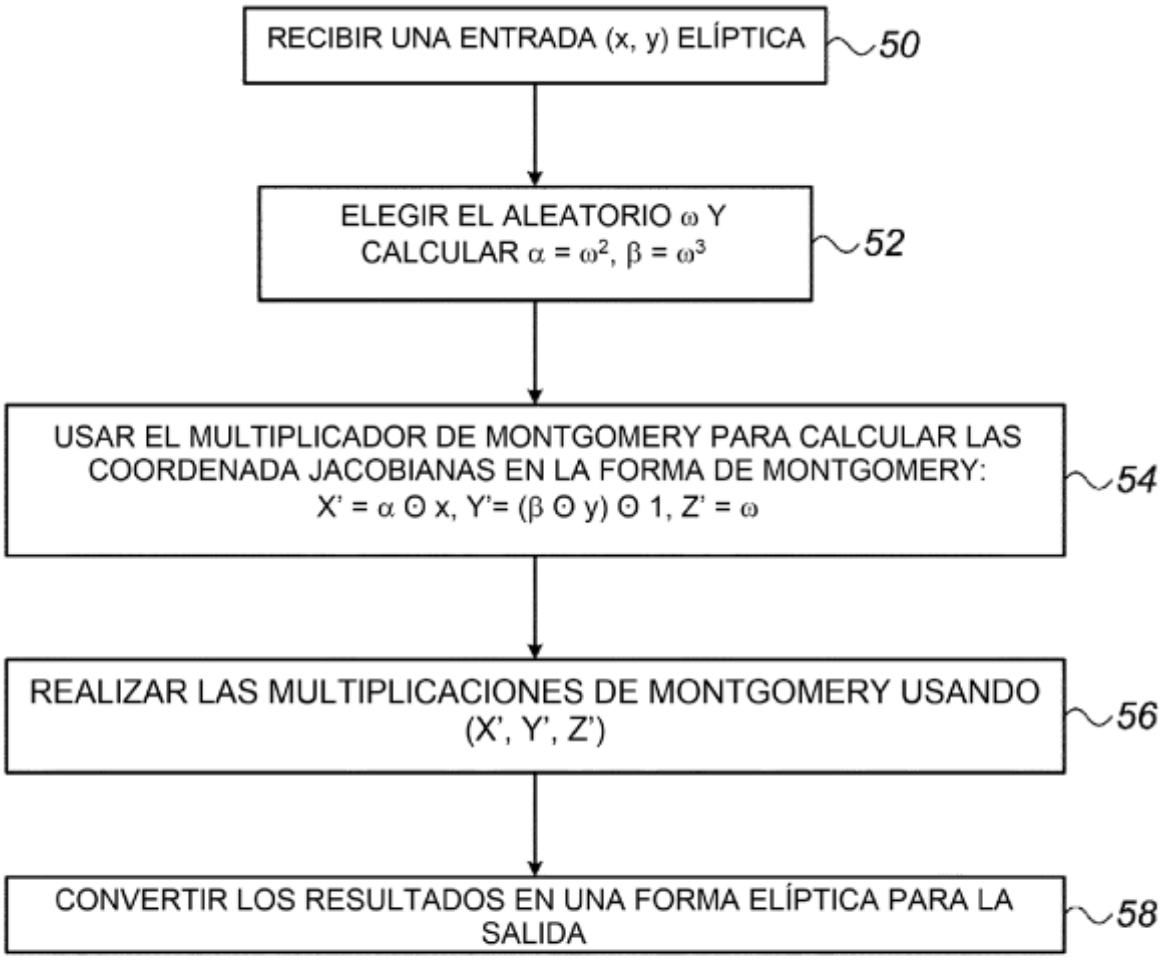
RECIBIR UNA ENTRADA (x, y) ELÍPTICA
50
ELEGIR EL ALEATORIO ω Y CALCULAR α = ω², β = ω³
52
USAR EL MULTIPLICADOR DE MONTGOMERY PARA CALCULAR LAS COORDENADA JACOBIANAS EN LA FORMA DE MONTGOMERY: X' = α Θ x, Y'= (β Θ y) Θ 1, Z' = ω
54
REALIZAR LAS MULTIPLICACIONES DE MONTGOMERY USANDO (X', Y', Z')
56
CONVERTIR LOS RESULTADOS EN UNA FORMA ELÍPTICA PARA LA SALIDA
58

FIG. 2