(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 440 286**

(51) Int. CI.:

G06F 7/72 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.07.2010 E 10168455 (3)**

(97) Fecha y número de publicación de la concesión europea: **18.09.2013 EP 2275925**

(54) Título: **Procedimiento de procesamiento criptográfico de datos y dispositivo asociado**

(30) Prioridad:

06.07.2009 FR 0954666

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.01.2014

(73) Titular/es:

OBERTHUR TECHNOLOGIES (100.0%)
420 rue d'Estienne d'Orves
92700 Colombes, FR

(72) Inventor/es:

GIRAUD, CHRISTOPHE y
VERNEUIL, VINCENT

(74) Agente/Representante:

PÉREZ BARQUÍN, Eliana

DESCRIPCIÓN

Procedimiento de procesamiento criptográfico de datos y dispositivo asociado

La invención se refiere a un procedimiento de procesamiento, preferentemente criptográfico, de datos, por ejemplo aplicado dentro de una entidad electrónica, y a un dispositivo asociado (por ejemplo esta entidad electrónica).

En el ámbito del procesamiento de datos (pudiendo estos datos representar por ejemplo un mensaje que se ha de intercambiar o una clave criptográfica de cifrado de un mensaje de este tipo), se utilizan las propiedades de las curvas elípticas en los cuerpos acabados durante los cálculos criptográficos implicados por el procesamiento de los datos, por ejemplo para firma de un mensaje o intercambio de claves entre interlocutores.

Para poner en práctica estos procesamientos, de manera general en una entidad electrónica, se utiliza una representación particular de los puntos de la curva elíptica mediante por ejemplo una pluralidad de elementos de un cuerpo de Galois (que forma las coordenadas de punto), tal como por ejemplo la representación proyectiva jacobiana (representación por un triplete de puntos del cuerpo de Galois F_p) o una representación proyectiva jacobiana modificada (mediante cuatro elementos o coordenadas del cuerpos de Galois F_p), como se describe por ejemplo en el artículo "Efficient elliptic curve exponentiation using mixed coordinate" de H. Cohen, T. Ono, y A. Miyaji, en K. Ohta y P. Dinggyi, editors, Advances in Cryptology - ASIACRYPT '98, volumen 1514 de Lecture Notes in Computer Science, páginas 51-65. Springer, 1998.

Las operaciones en la curva elíptica se refieren entonces en efecto a operaciones en el cuerpo de Galois F_p.

De este modo por ejemplo una adición o una duplicación en la curva elíptica (operaciones que permiten por composición realizar la multiplicación por un escalar en la curva elíptica como se describe por ejemplo en el artículo mencionado anteriormente) se realizan por la aplicación de operaciones en el cuerpo de Galois F_p en las coordenadas del o de los puntos en cuestión (debiendo estas operaciones en el cuerpo de Galois dar como resultado típicamente adiciones, sustracciones, multiplicaciones y elevaciones a una potencia 2, 3 o 4).

Para protegerse de los ataques por canal auxiliar (en inglés "*Side Channel Attacks*"), tales como la observación del consumo energético de la entidad electrónica para intentar determinar las operaciones que se aplican, se ha propuesto la realización de las operaciones mencionadas anteriormente en el cuerpo de Galois entre un conjunto más amplio de operaciones, de las cuales algunas son por consiguiente ficticias, de manera que la serie de los tipos de operaciones sucesivas forma una repetición periódica de un número de tipos predeterminado, y esto, cualquiera que sea la operación en la curva elíptica en cuestión. Esta técnica se describe de manera general en la solicitud de patente FR 2 838 210 y en su aplicación a las curvas elípticas en el artículo "Low-cost Solutions for Preventing Simple Side-Channel Analysis: Side-Channel Atomicity" de B. Chevallier-Mames, M. Ciet, y M. Joye, IEEE Transactions on Computers, 53(6) : 760-768, 2004 (véase también "Aspects of Fast and Secure Arithmetics for Elliptic Curve Cryptography" de M. Ciet, tesis de doctorado, Universidad católica de Lovaina, junio 2003).

En este artículo, se propone de este modo aplicar la repetición de un bloque elemental (denominado bloque atómico) formado por la sucesión de una multiplicación, una adición, una oposición y una nueva adición (siendo consideradas todas estas operaciones en el cuerpo de Galois F_p). Como ya se ha indicado, cualquiera que sea la operación (duplicación o adición) realizada en la curva elíptica, esta operación se aplica prácticamente a la entidad electrónica por la repetición de bloques elementales del mismo tipo (10 bloques en el caso de la duplicación y16 bloques en el caso de la adición), variando sin embargo los datos manipulados de un bloque elemental a otro.

La aplicación sistemática de multiplicaciones por la entidad electrónica (con la ayuda por ejemplo de una instrucción de multiplicación dentro de un microprocesador de la entidad electrónica), en los casos en que los dos operandos son distintos como en el que los dos operandos son idénticos, permite en este contexto utilizar con frecuencia operaciones del mismos tipo (en este caso multiplicaciones) y participan por lo tanto en la posibilidad de definir el bloque elemental que ha de repetirse.

En este contexto, la invención propone un procedimiento de procesamiento criptográfico de datos aplicado en una entidad electrónica, en el que se determina, a partir de un primer punto en una curva elíptica representado mediante al menos tres primeros elementos de un cuerpo de Galois, un segundo punto en la curva elíptica representada mediante al menos tres segundos elementos del cuerpo de Galois, siendo obtenido cada uno de los segundos elementos a partir de los primeros elementos mediante un primer conjunto de operaciones que comprenden multiplicaciones y adiciones, en el que se aplica un segundo conjunto de operaciones sucesivas que tienen cada una un tipo, la serie de los tipos de operaciones sucesivas del segundo conjunto que forma una repetición periódica de una pluralidad de tipos de operación que incluyen al menos una multiplicación y una adición en el cuerpo de Galois, comprendiendo el segundo conjunto de operaciones el primer conjunto de operaciones, caracterizado porque la pluralidad de tipos de operación comprende una puesta al cuadrado en el cuerpo de Galois.

El uso de una operación de puesta al cuadrado, cuya aplicación es más rápida que una multiplicación (especialmente para un microprocesador de una entidad electrónica), permite reducir el tiempo de aplicación de las

operaciones en la curva elíptica, sin que por ello se comprometa la posibilidad de efectuar estas operaciones por la repetición de bloques elementales a tipos de operación predefinidos, contrariamente a lo que podía parecer deseable como se ha indicado anteriormente.

Dichos tres primeros elementos son por ejemplo coordenadas proyectivas jacobianas del premier punto y dichos tres segundos elementos por ejemplo coordenadas proyectivas jacobianas del segundo punto.

Según una realización considerada más adelante en la descripción, el segundo punto es el producto escalar del primer punto por un número entero; este producto escalar puede formar parte de un algoritmo criptográfico de firma (por ejemplo según el protocolo ECDSA) o de intercambio de claves criptográficas (por ejemplo según el protocolo ECDH).

Tal producto escalar es por ejemplo aplicado mediante adiciones en coordenadas proyectivas jacobianas y de duplicaciones en coordenadas proyectivas jacobianas modificadas, lo que limita el número de multiplicaciones que han de efectuarse.

En una variante, el segundo punto puede ser una suma del primer punto y de un tercer punto de la curva elíptica.

La curva elíptica puede en la práctica tener por ecuación proyectiva jacobiana de Weierstrass $Y^2 = X^3 + aXZ^4 + bZ^6$, en la que a y b son elementos del cuerpo de Galois y $4a^3 + 27b^2$ no es el elemento nulo.

Según una realización considerable, la entidad electrónica puede ser un microprocesador, en cuyo caso cada una de dichas operaciones corresponde a una instrucción del microprocesador. En una variante, la entidad electrónica puede ser una placa de microcircuito que integra un procesador capaz de ejecutar instrucciones que corresponden a dichas operaciones.

La invención propone asimismo una entidad electrónica de procesamiento criptográfico de datos que comprende medios de procesamiento capaces de determinar, a partir de un primer punto en una curva elíptica representado mediante al menos tres primeros elementos de un cuerpo de Galois, un segundo punto en la curva elíptica representado mediante al menos tres segundos elementos del cuerpo de Galois, siendo obtenido cada uno de los segundos elementos a partir de los primeros elementos mediante un primer conjunto de operaciones que comprende multiplicaciones y adiciones, siendo los medios de procesamiento capaces de aplicar un segundo conjunto de operaciones sucesivas, teniendo cada una un tipo, formando la serie de los tipos de las operaciones sucesivas del segundo conjunto una repetición periódica de una pluralidad de tipos de operación que incluyen al menos una multiplicación y una adición en el cuerpo de Galois, comprendiendo el segundo conjunto de operaciones el primer conjunto de operaciones, caracterizado porque la pluralidad de tipos de operación comprende una puesta al cuadrado en el cuerpo de Galois.

Otras características y ventajas de la invención aparecerán a la luz de la siguiente descripción.

El procedimiento de procesamiento de datos (por ejemplo de mensaje o de clave criptográfica) descrito a continuación se aplica en una entidad electrónica, por ejemplo una entidad electrónica, tal como una placa de microcircuito, que comprende un microprocesador, en cuyo caso el procedimiento se aplica ejecutando instrucciones dentro del microprocesador y se realizan las operaciones efectuadas sobre los datos procesados por tales instrucciones. En una variante, la entidad electrónica podría realizarse en lógica cableada, tal como es el caso para un coprocesador criptográfico.

En la presente realización, se considera una curva elíptica ε de ecuación afín:

$$y^2 = x^3 + ax + b$$

y por lo tanto de ecuación proyectiva jacobiana de Weierstraβ, la ecuación:

$$Y^2 = X^3 + aXZ^4 + bZ^6,$$

en la que $a, b \in F_p$ et $4a^3 + 27b^2 \neq 0$.

Se recuerda que un punto P de coordenadas afines *(x, y) tiene por* coordenadas proyectivas jacobianas homogéneas $(X : Y : Z)=(x : y : 1)$.

Recíprocamente, un punto de coordenadas proyectivas jacobianas *(X : Y : Z)* tiene por coordenadas afines *(x, y)= (X/Z, Y/(Z²))*.

Salvo que se haga una mención expresa, se utilizan a continuación las coordenadas proyectivas jacobianas.

El opuesto de un punto *(X : Y: Z)* es *(X : -Y: Z)* y el punto al infinito se representa por (*1* : 1 : 0).

La suma de $P = (X_1 : Y_1 : Z_1)$ y $Q = (X_2 : Y_2 : Z_2)$, en la que $P,Q \neq O$ y $P \neq \pm Q$, es el punto $P+Q=(X_3 : Y_3 : Z_3)$ tal como:

$$\begin{cases} X_3 = F^2 - E^3 - 2AE^2 \\ Y_3 = F(AE^2 - X_3) - CE^3 \\ Z_3 = Z_1 Z_2 E \end{cases} \quad \text{con} \quad \begin{aligned} A &= X_1 Z_2^{\,2} \\ B &= X_2 Z_1^{\,2} \\ C &= Y_1 Z_2^{\,3} \\ D &= Y_2 Z_1^{\,3} \\ E &= B - A \\ F &= D - C \end{aligned}$$

El doble de un punto $P = (X_1 : Y_1 : Z_1)$ es el punto $2P = (X_3 : Y_3 : Z_3)$ tal como:

$$\begin{cases} X_3 = B^2 - 2A \\ Y_3 = B(A - X_3) - 8Y_1^4 \\ Z_3 = 2Y_1 Z_1 \end{cases} \quad \text{con} \quad \begin{aligned} A &= 4X_1 Y_1^{\,2} \\ B &= 3X_1^{\,2} + aZ_1^{\,4} \end{aligned}$$

Para reducir el número de operaciones (de multiplicación) necesarias para la determinación del doble de un punto, se utiliza la representación proyectiva jacobiana modificada, como se ha explicado por ejemplo en el artículo "*Efficient elliptic curve exponentiation using mixed coordinate*" ya mencionado. Un punto P de coordenadas proyectivas jacobianas *(X : Y : Z)* tiene por coordenadas proyectivas jacobianas modificadas $(X : Y : Z: aZ^4)$.

En esta representación, el doble de un punto $P = (X_1 : Y_1 : Z_1 : W_1)$ es el punto $2P = (X_3 : Y_3 : Z_3 : W_3)$ tal como:

$$\begin{cases} X_3 = A^2 - 2C \\ Y_3 = A(C - X_3) - 8B \\ Z_3 = 2Y_1 Z_1 \\ W_3 = 16BW_1 \end{cases} \quad \text{con} \quad \begin{aligned} A &= 3X_1^{\,2} + W_1 \\ B &= Y_1^4 \\ C &= 2((X_1 + Y_1^{\,2})^2 - X_1^{\,2} - B) \end{aligned}$$

Se propone aquí aplicar la adición en coordenadas proyectivas jacobianas $(X_3 : Y_3 : Z_3) \leftarrow (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$ definida anteriormente mediante las siguientes operaciones:

$$A.\begin{bmatrix} T_1 \leftarrow Z_2^2 \\ \varnothing \\ \varnothing \\ T_2 \leftarrow Y_1 . Z_2 \\ \varnothing \\ Y_1 \leftarrow Y_2 . Z_1 \\ \varnothing \\ T_3 \leftarrow T_1 . T_2 \\ \varnothing \\ \varnothing \\ T_4 \leftarrow Z_1^2 \\ \varnothing \\ T_2 \leftarrow Y_1 . T_4 \\ \varnothing \\ T_3 \leftarrow -T_3 \\ T_2 \leftarrow T_2 + T_3 \\ Y_1 \leftarrow T_1 . X_1 \\ \varnothing \\ \varnothing \\ \varnothing \\ X_1 \leftarrow X_2 . T_4 \\ Y_1 \leftarrow -Y_1 \\ X_1 \leftarrow X_1 + Y_1 \end{bmatrix} \quad B.\begin{bmatrix} T_1 \leftarrow X_1^2 \\ \varnothing \\ Y_1 \leftarrow -Y_1 \\ T_4 \leftarrow Y_1 . T_1 \\ \varnothing \\ Y_1 \leftarrow T_1 . X_1 \\ \varnothing \\ T_1 \leftarrow Z_1 . X_1 \\ \varnothing \\ \varnothing \\ X_1 \leftarrow T_2^2 \\ X_1 \leftarrow -X_1 \\ Z_1 \leftarrow T_1 . Z_2 \\ T_1 \leftarrow T_4 + T_4 \\ \varnothing \\ X_1 \leftarrow X_1 + T_1 \\ T_1 \leftarrow Y_1 . T_3 \\ X_1 \leftarrow Y_1 + X_1 \\ T_1 \leftarrow -T_1 \\ T_4 \leftarrow T_4 + X_1 \\ T_3 \leftarrow T_4 . T_2 \\ X_1 \leftarrow -X_1 \\ Y_1 \leftarrow T_3 + T_1 \end{bmatrix}$$

$$X_3 \leftarrow X_1, Y_3 \leftarrow Y_1, Z_3 \leftarrow Z_1 .$$

La duplicación en coordenadas jacobianas modificadas ($X : Y : Z : W$) ← 2 * ($X : Y : Z : W$) definida anteriormente es por su parte aplicada mediante las siguientes operaciones:

$$C.\begin{cases} T_1 \leftarrow X^2 \\ T_2 \leftarrow Y + Y \\ \varnothing \\ Z \leftarrow T_2.Z \\ T_4 \leftarrow T_1 + T_1 \\ T_3 \leftarrow T_2.Y \\ Y \leftarrow T_3 + T_3 \\ T_2 \leftarrow Y.T_3 \\ T_1 \leftarrow T_4 + T_1 \\ T_1 \leftarrow T_1 + W \\ T_3 \leftarrow T_1^2 \\ \varnothing \\ T_4 \leftarrow Y.X \\ X \leftarrow W + W \\ T_4 \leftarrow -T_4 \\ T_3 \leftarrow T_3 + T_4 \\ W \leftarrow T_2.X \\ X \leftarrow T_3 + T_4 \\ T_2 \leftarrow -T_2 \\ Y \leftarrow T_4 + X \\ T_4 \leftarrow Y.T_1 \\ T_4 \leftarrow -T_4 \\ Y \leftarrow T_4 + T_2 \end{cases}$$

Los símbolos Ø representan operaciones ficticias que no manipulan los datos mencionados anteriormente, sino que trabajan con otros registros (o memorias) dedicadas a la aplicación de estas operaciones ficticias Ø.

Las operaciones ficticias 0 de este modo pueden ser elegidas para que la serie de los tipos de operaciones (o patrón de atomicidad) sea idéntica para las series de operaciones A, B y C. Por ejemplo, al ser la segunda operación de la serie C una adición, las segundas operaciones (ficticias) de las series A y B son adiciones.

Se recuerda que el símbolo ← representa la sustitución del dato (en general del registro) que precede al símbolo ← por el resultado de la operación indicada después del símbolo ←.

Las operaciones de adición y de duplicación descritas anteriormente son por ejemplo aplicadas dentro de la entidad electrónica para la realización de un producto escalar en la curva elíptica, es decir el producto de un número entero d por un punto P de la curva elíptica ε.

El producto escalar por un número entero puede en efecto referirse siempre a duplicaciones y adiciones debido a la descomposición del número entero en base 2, como en el marco del algoritmo habitualmente utilizado denominado *"double and add"* o en el marco de algoritmos más evolucionados, como por ejemplo en el artículo *"Efficient elliptic curve exponentiation using mixed coordinate"* mencionado anteriormente o en el artículo " Fast point multiplication non elliptic curves without precomputation" de M. Joye en 2nd International Workshop on the Arithmetic of Finite Fields (WAIFI 2008), 07 2008.

El producto escalar se utiliza por ejemplo cuando la entidad electrónica debe efectuar una firma utilizando el protocolo ECDSA ("*Elliptic Curve Digital Signature Algorithm",* utilizado en diferentes normas) que necesita el cálculo del producto escalar k.P, siendo k un número aleatorio, o bien cuando la entidad electrónica permite efectuar un intercambio de clave entre dos interlocutores mediante el protocolo ECDH (por "*Elliptic Curve Diffie-Hellman*") que necesita el cálculo del producto escalar d_A.P (siendo d_A un número entero elegido por el primer interlocutor, debiendo el producto escalar entonces ser enviado al segundo interlocutor), o el cálculo del producto escalar $d_A.(d_B.P)$ (siendo el punto d_B.P el punto recibido del segundo interlocutor por el primer interlocutor), siendo la clave secreta compartida determinada entonces a partir de la coordenada afín x del punto $d_A.(d_B.P)$.

La determinación del producto escalar se realiza de este modo por la aplicación sucesiva de operaciones de tipo A y B por una parte y C por otra parte, sucesión que depende del operando entero (respectivamente d, k et d_A en los ejemplos anteriores). Sin embargo, debido a que la serie de los tipos de las operaciones de cada una de las series de operaciones A, B, C es idéntica y que los tipos de operación aplicados para realizar un producto escalar (compuesto por operaciones de tipos A, B y C) forman por lo tanto una repetición periódica de una pluralidad de tipos de operación, no será posible que un atacante exterior que observa la entidad electrónica determine en qué orden se realizan las series de operaciones A, B, C y el atacante no tendrá acceso al operando entero.

Asimismo, cada una de las series A, B, C utiliza dos operaciones de puesta al cuadrado, previamente aplicadas por multiplicaciones, y se obtiene de este modo una ganancia en tiempo de cálculo del orden de algunos porcientos.

Se observa que, respecto a la solución descrita en el artículo "*Low cost solutions for preventing simple side channel analysis: side-channel atomicity*" mencionado anteriormente, las series de operaciones A, B, C anteriores se obtienen agrupando ocho bloques atómicos, tales como se ha propuesto en el artículo (formando cada grupo de ocho bloques un "*patrón de atomicidad*"), modificando dos de estos bloques atómicos por la sustitución de una multiplicación por una puesta al cuadrado (de ahí una primera ganancia en tiempo de cálculo), a continuación por la supresión de algunas operaciones del patrón de atomicidad que no se utilizan en ningún caso (de ahí una segunda ganancia en tiempo de cálculo). La agrupación de bloques atómicos es especialmente posible debido a que el número de bloques atómicos necesarios para la adición en coordenadas proyectivas jacobianas y el número de bloques atómicos necesarios para la duplicación en coordenadas proyectivas jacobianas modificadas tienen un menor múltiplo común estrictamente superior a 1.

En una variante, se habría podido formar un patrón de atomicidad a partir de cuatro bloques atómicos, tales como se han descrito en el artículo, y modificar solo el primer bloque atómico de cada patrón de atomicidad (sustitución en este bloque de la multiplicación por una puesta al cuadrado).

El patrón de atomicidad obtenido según esta variante se ha de repetir dos veces para una duplicación y cuatro veces para una adición, con las mismas ventajas en tiempo de cálculo que se han descrito anteriormente.

Los ejemplos que preceden solo son modos posibles de aplicación de la invención que no se limita a los mismos.

REIVINDICACIONES

1. Procedimiento de procesamiento criptográfico de datos aplicado dentro de una entidad electrónica, en el que se determina, a partir de un primer punto en una curva elíptica representado mediante al menos tres primeros elementos de un cuerpo de Galois, un segundo punto en la curva elíptica representado mediante al menos tres segundos elementos del cuerpo de Galois, siendo obtenido cada uno de los segundos elementos a partir de los primeros elementos mediante un primer conjunto de operaciones que comprende multiplicaciones y adiciones, en el que se aplica un segundo conjunto de operaciones sucesivas que tienen cada una un tipo, formando la serie de los tipos de las operaciones sucesivas del segundo conjunto una repetición periódica de una pluralidad de tipos de operación que incluye al menos una multiplicación y una adición en el cuerpo de Galois, comprendiendo el segundo conjunto de operaciones el primer conjunto de operaciones, **caracterizado porque** la pluralidad de tipos de operación comprende una puesta al cuadrado en el cuerpo de Galois.

2. Procedimiento según la reivindicación 1, en el que dichos tres primeros elementos son coordenadas proyectivas jacobianas del primer punto.

3. Procedimiento según la reivindicación 1 o 2, en el que dichos tres segundos elementos son coordenadas proyectivas jacobianas del segundo punto.

4. Procedimiento según una de las reivindicaciones1 a 3, en el que el segundo punto es el producto escalar del primer punto por un número entero.

5. Procedimiento según la reivindicación 4, en el que el producto escalar se aplica mediante adiciones en coordenadas proyectivas jacobianas y duplicaciones en coordenadas proyectivas jacobianas modificadas.

6. Procedimiento según una de las reivindicaciones1 a 3, en el que el segundo punto es la suma del primer punto y de un tercer punto de la curva elíptica.

7. Procedimiento según una de las reivindicaciones1 a 6, en el que la curva elíptica tiene por ecuación proyectiva jacobiana de Weierstrass $y^2 = X^3 + aXZ^4 + bZ^6$, en la que a y b son elementos del cuerpo de Galois y $4a^3 + 27b^2$ no es el elemento nulo.

8. Procedimiento según una de las reivindicaciones1 a 7, en el que la entidad electrónica es un microprocesador y en el que cada una de dichas operaciones corresponde a una instrucción del microprocesador.

9. Entidad electrónica de procesamiento criptográfico de datos que comprende medios de procesamiento capaces de determinar, a partir de un primer punto en una curva elíptica representado mediante al menos tres primeros elementos de un cuerpo de Galois, un segundo punto en la curva elíptica representado mediante al menos tres segundos elementos del cuerpo de Galois, siendo obtenido cada uno de los segundos elementos a partir de los primeros elementos mediante un primer conjunto de operaciones que comprende multiplicaciones y adiciones, siendo los medios de procesamiento capaces de aplicar un segundo conjunto de operaciones sucesivas que tienen cada una un tipo, formando la serie de los tipos de las operaciones sucesivas del segundo conjunto una repetición periódica de una pluralidad de tipos de operación que incluyen al menos una multiplicación y una adición en el cuerpo de Galois, comprendiendo el segundo conjunto de operaciones el primer conjunto de operaciones,
caracterizado porque la pluralidad de tipos de operación comprende una puesta al cuadrado en el cuerpo de Galois.