(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 435 626**

(51) Int. CI.:

G06F 7/72 (2006.01)
H04L 9/28 (2006.01)
G06F 7/58 (2006.01)
G06F 17/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **15.06.2010 E 10738013 (1)**

(97) Fecha y número de publicación de la concesión europea: **02.10.2013 EP 2443787**

(54) Título: **Criptografía de una curva elíptica**

(30) Prioridad:

16.06.2009 FR 0954053

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.12.2013

(73) Titular/es:

MORPHO (100.0%)
27, Rue Leblanc
75015 Paris, FR

(72) Inventor/es:

ICART, THOMAS y
CORON, JEAN-SÉBASTIEN

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Criptografía de una curva elíptica

La presente invención concierne a la criptografía de mensajes basada en la utilización de puntos de una curva elíptica, y de modo más particular a una criptografía de este tipo de manera determinista.

A fin de aplicar un cálculo criptográfico a un mensaje, se ponen en práctica clásicamente algoritmos de inserción de valores arbitrarios en el seno de estructuras matemáticas. A tal efecto, las curvas elípticas son estructuras matemáticas que permiten a la vez facilitar la puesta en práctica de tales cálculos criptográficos y ahorrar espacio de memoria con respecto a la puesta en práctica de otros cálculos criptográficos.

Sin embargo, los algoritmos eficaces de inserción de valores arbitrarios que utilizan curvas elípticas son probabilistas. Por consiguiente, el tiempo de puesta en práctica de tales algoritmos no es constante, éste es función del mensaje que haya que codificar. Así, si un atacante determina diferentes tiempos de puesta en práctica del algoritmo aplicado, éste puede obtener informaciones sobre el mensaje codificado.

A fin de enmascarar el tiempo utilizado por un algoritmo de inserción probabilista, es posible prever añadir a este algoritmo etapas inútiles a fin de que su aplicación se extienda siempre en un período de tiempo de longitud idéntica, cualquiera que sea el mensaje tratado.

Un punto P de una curva elíptica está definido por su abscisa X y su ordenada Y, verificando X e Y la ecuación siguiente:

$$f(X) = Y^2 \quad (1)$$

donde f(X) es el polinomio $f(X) = X^3 + aX + b$

Se conoce una familia de polinomios, que verifican la igualdad de Skalba, que permiten determinar un punto de este tipo de una curva elíptica, tal como se define en el documento ‘Construction of Rational Points on Elliptic Curves over finite fields’ de Andrew Shallue y Christiaan van de Woestijne.

Polinomios $X_1(t)$, $X_2(t)$, $X_3(t)$ y U(t) verifican la igualdad de Skalba si estos verifican la ecuación siguiente:

$$f(X_1(t).f(X_2(t).fX_3(t)) = U^2(t) \quad (2)$$

donde f es la función que define la curva elíptica considerada y

donde t es un parámetro.

Polinomios que verifican la igualdad de Skalba pueden tomar dos parámetros u y t. En este caso, la igualdad de Skalba se escribe:

$$f(X_1(t,u).f(X_2(t,u).fX_3(t,u)) = U^2(t,u)$$

Se puede utilizar este tipo de ecuaciones con dos parámetros u y t. Sin embargo, en las aplicaciones consideradas, se puede prever ventajosamente fijar u, o también fijar t, a un valor cualquiera. Así, queda por elegir el valor de un solo parámetro.

Dados parámetros elegidos t y u, se anota por $X_1 = X_1(t,u)$, $X_2 = X_2(t,u)$, $X_3 = X_3(t,u)$, U = U(t,u) donde X_1, X_2, X_3 y U son elementos de F_q. Esta ecuación (2) significa que al menos uno de los valores $f(X_1)$, $f(X_2)$ y $f(X_3)$ corresponde a un término al cuadrado en el cuerpo finito F_q.

Después, una vez identificado el término al cuadrado en F_q, $f(X_i)$, se puede obtener a continuación un punto de la curva elíptica $P(X_i, \sqrt{f(X_i).})$

El cálculo de $\sqrt{f(X_i)}$ puede hacerse con la ayuda de un cálculo de exponenciación cuando la característica q del cuerpo Fq verifica:

$$q = 3 \bmod 4$$

En este caso, se conoce que:

$$\sqrt{f(X_i)} = f(X_i)^{(q+1)/4} \quad (3)$$

Así pues, para determinar un punto de la curva elíptica (1), conviene determinar qué valor de entre los tres valores $f(X_1)$, $f(X_2)$ y $f(X_3)$ corresponde a un término al cuadrado en el cuerpo finito F_q. A tal efecto, podría preverse controlar en primer lugar si el término $f(X_1)$ es un término al cuadrado en el cuerpo finito F_q, después, si este no es el caso,

aplicar este mismo control al término $f(X_2)$, y finalmente si éste sigue sin ser el caso controlar de manera similar el término $f(X_3)$. Sin embargo, procediendo así, la determinación de un punto en la curva elíptica no lleva siempre el mismo tiempo, puesto que esta determinación es efectuada más rápidamente si el primer término controlado es un término al cuadrado que si el tercer término es solamente un término al cuadrado.

Un potencial atacante podría sacar partido de esta diferencia de tiempo transcurrido para determinar un punto de la curva elíptica para violar el secreto ligado al parámetro que ha permitido generar este punto. Ahora bien, en el ámbito de la criptografía, estos parámetros deben permanecer secretos.

Estos parámetros pueden corresponder especialmente a contraseñas. Así, es importante que la determinación de estos puntos no facilite en sí misma informaciones que permitan violar el secreto del parámetro, y por ello, hay que evitar ataques basados en un análisis del tiempo transcurrido para determinar un punto de la curva.

Para paliar esta desventaja, sería posible controlar sistemáticamente los tres términos $f(X_i)$ yendo i de 1 a 3. Así, el tiempo para determinar un punto de la curva ya no sería función del punto determinado.

Pero, el hecho de controlar si un término de la ecuación (2) es un término al cuadrado en el cuerpo finito F_q es una operación compleja que especialmente pone en práctica una exponenciación que es laboriosa en tiempo de ejecución. En el caso en que se desee determinar un punto de la curva elíptica sobre la base de las igualdades de Skalba, efectuándose estas determinaciones a tiempo constante, se requieren cuatro operaciones de exponenciación en el caso anteriormente descrito, una exponenciación por control de cada uno de los términos de la ecuación (2) de Skalba y una exponenciación para calcular la raíz cuadrada, tal como se describe en la ecuación (3).

La presente invención pretende mejorar la situación.

Un primer aspecto de la presente invención propone un procedimiento de ejecución de un cálculo criptográfico en un componente electrónico, que comprende una etapa de obtención de un punto P(X,Y) a partir de al menos un parámetro t, en una curva elíptica que verifique la ecuación:

$$Y^2 = f(X), \text{ y}$$

a partir de polinomios $X_1(t)$, $X_2(t)$, $X_3(t)$ y $U(t)$ que verifiquen la igualdad de Skalba siguiente:

$$f(X_1(t)).f(X_2(t)).fX_3(t)) = U(t)^2$$

en el cuerpo finito F_q, cualquiera que sea el parámetro t, verificando q la ecuación $q = 3 \bmod 4$;

comprendiendo el citado procedimiento las etapas siguientes:

/1/ obtención de un valor del parámetro t;

/2/ determinación del punto P efectuando las subetapas siguientes:

/i/ cálculo de $X_1 = X_1(t)$, $X_2 = X_2(t)$, $X_3 = X_3(t)$ y $U = U(t)$

/ii/ si el término $f(X_1).f(X_2)$ es un término al cuadrado en el cuerpo finito F_q entones se prueba si el término $f(X_3)$ es un término al cuadrado en el cuerpo finito F_q y se calcula la raíz cuadrada del término $f(X_3)$, teniendo el punto P por abscisa X_3 y por ordenada la raíz cuadrada del término $f(X_3)$;

/iii/ si no, se prueba si el término $f(X_1)$ es un término al cuadrado en el cuerpo finito F_q y en este caso, se calcula la raíz cuadrada del término $f(X_1)$, teniendo el punto P por abscisa X_1 y por ordenada la raíz cuadrada del término $f(X_1)$;

/iv/ si no, se calcula la raíz cuadrada del término $f(X_2)$, tendiendo el punto P por abscisa X_2 y por ordenada la raíz cuadrada de término $f(X_2)$;

/3/ utilización del citado punto P en una aplicación criptográfica de cifrado o de hashing o de firma o de autenticación o de identificación.

Gracias a estas disposiciones, se puede determinar un punto de una curva elíptica de manera adaptada a una utilización en el ámbito de la criptografía, puesto que, por una parte, esta determinación lleva el mismo tiempo cualquiera que sea el parámetro de entrada t y, por otra, ésta es eficaz porque se reduce el número de operaciones.

Esta determinación lleva un tiempo constante que no es dependiente del parámetro o de los parámetros de entrada. En efecto, aunque este procedimiento ofrece diferentes vías de tratamiento en función del término que corresponda a un término al cuadrado en la igualdad de Skalba, se efectúa el mismo número de operaciones del mismo tipo, cualquiera que sea el punto de la curva determinado. De manera más precisa, cualquiera que sea el punto de la curva determinado, se efectúa la lista de las operaciones siguientes:

- prueba de un término al cuadrado en F_q;
- determinación de una raíz cuadrada.

No es posible por tanto proceder a un ataque de tipo 'timing attack'.

Además, esta determinación es eficaz puesto que el número de las operaciones laboriosas puestas en práctica es limitado. En efecto, es posible controlar el hecho de que uno de entre los tres términos de la ecuación de Skalba (2) es un término al cuadrado en el cuerpo finito F_q poniendo en práctica como máximo dos operaciones de tipo exponenciación. De modo más preciso, conviene observar que, en un modo de realización de la presente invención, la prueba de un término al cuadrado corresponde a una exponenciación, que es la operación más laboriosa de poner en práctica en el presente contexto.

En la etapa /2/-/ii/, está previsto decidir si el término R_0:

$$R_0 = f(X_1).f(X_2)$$

es un término al cuadrado.

Esta etapa puede corresponder a una prueba de término al cuadrado, que ponga en práctica una exponenciación suplementaria, o también puede estar basada en un valor precalculado resultante de un cálculo previo en el caso en que un polinomio que verifique la igualdad de Skalba corresponda a un término que nunca puede ser un término al cuadrado. En este último caso, expuesto en secciones siguientes, la puesta en práctica de un procedimiento requiere ventajosamente una sola exponenciación. Pero en el peor de los casos, la puesta en práctica de un procedimiento de acuerdo con un modo de realización de la presente invención corresponde a dos exponenciaciones, una para la prueba de término al cuadrado aplicada a R_0, y otra exponenciación para la prueba de término al cuadrado aplicado a $f(X_3)$ o bien también a $f(X_1)$.

Durante la ejecución de tales cálculos de acuerdo con un modo de realización de la presente invención, el tiempo consumido para la puesta en práctica de las operaciones distintas a una exponenciación es despreciable frente al tiempo consumido por la puesta en práctica de una exponenciación. Ahora bien, gracias a las características de la presente invención, se puede pasar de cuatro exponenciaciones, como se describió anteriormente en un caso clásico, a dos exponenciaciones como máximo. Tal reducción del número de exponenciaciones es muy ventajosa.

En un modo de realización de la presente invención, en la etapa /2/-/ii/, se efectúan las etapas siguientes:

- cálculo de R_1 tal que:

$$R_1 = (f(X_1).f(X_2))^{\frac{q+1}{4}}$$

- si R_1^2 es igual a $f(X_1).f(X_2)$, entonces decidir que el término $f(X_1).f(X_2)$ es un término al cuadrado en el cuerpo F_q;

En la etapa /2/-/iii/, se prueba si el término $f(X_1)$ es un término al cuadrado en el cuerpo finito F_q según las etapas siguientes:

- cálculo de R_2' tal que

$$R_2' = f(X_1)^{(q-1)-\frac{q+1}{4}}$$

- cálculo de R_3' tal que:

$$R_3' = R_2'^2$$

- cálculo de R_4' tal que

$$R_4' = R_3'.f(X_1)$$

si R_4' no es igual a 1, en la etapa /2/-/iv/, se obtiene la raíz cuadrada de $f(X_2)$ según la ecuación siguiente:

$$\sqrt{f(X_2)} = R_1.R_2'$$

Este modo de realización es general y puede aplicarse fácilmente a cualquier familia de polinomios que verifiquen la igualdad de Skalba. Conviene observar que, de modo astuto, en el caso en que el término al cuadrado de la igualdad de Skalba (2) sea $f(X_2)$, es decir el último término que hay que controlar entre los tres términos de la

igualdad de Skalba, no se requiere efectuar una nueva exponenciación del tipo $f(X_1)^{q-1-\frac{q+1}{4}}$. En efecto, puede utilizarse ventajosamente el término R_2' a fin de obtener la raíz cuadrada del término $f(X_2)$. Se garantiza así que solo se pongan en práctica dos exponenciaciones como mucho en el transcurso de la ejecución de un procedimiento de acuerdo con un modo de realización de la presente invención.

En un modo de realización de la presente invención, los polinomios que verifican la ecuación de Skalba en X y en Y son expresados en coordenadas jacobianas en X', Y' y Z tales que

$$X' = X.Z^2,$$

$$Y' = Y.Z^3$$

y las operaciones de inversión son transformadas en operación de multiplicación.

La transformación en coordenadas jacobianas permite transformar las inversiones en multiplicaciones, cuando el término Z es correctamente elegido.

En un modo de realización de la presente invención, los polinomios que verifican la igualdad de Skalba son expresados en coordenadas jacobianas según las cuales el punto P(X, Y) se escribe P(X'.Y',Z) tales que:

$$X' = X.Z^2,$$

$$Y' = Y.Z^3$$

donde la función f se escribe $f_z(X')$ y verifica:

$$f_Z(X') = X'^3 + aX'Z^4 + bZ^6$$

verificando la curva elíptica la ecuación:

$$Y'^2 = f_Z(X')$$

y los polinomios que verifican la igualdad de Skalba expresados en coordenadas jacobianas son $X'_1(t)$, $X'_2(t)$, $X'_3(t)$, Z(t) y U'(t) y verifican la igualdad de Skalba en coordenadas jacobianas:

$$U'(t)^2 = f_{Z(t)}(X'_1(t)).f_{Z(t)}(X'_2(t)).f_{Z(t)}(X'_3(t))$$

Con Z(t) determinado de modo que las operaciones de inversión sean transformadas en operación de multiplicación.

Se trata aquí de la aplicación de una transformación en coordenadas jacobianas a los polinomios de Ulas que verifican la igualdad de Skalba, tales como los enunciados anteriormente. En este caso, se puede a la vez limitar el número de exponenciaciones a dos, y eliminar cualquier cálculo de inversión, al tiempo que se garantiza una puesta en práctica a tiempo constante de una determinación de un punto P de la curva elíptica.

En un modo de realización, los polinomios que verifican la igualdad de Skalba son tales que es posible fijar el valor de $X_3(t)$ para cualquier t posible, tal que $f(X_3(t))$ no sea nunca un término al cuadrado en F_q,

en el cual, en la etapa /2/-/ii/, el término $f(X_1).f(X_2)$ no es un término al cuadrado en el cuerpo finito F_q,

en el cual, en la etapa /2/-/iii/, se prueba si el término $f(X_1)$ es un término al cuadrado en el cuerpo finito F_q según las etapas siguientes:

- cálculo de R_2' tal que

$$R'_2 = f(X_1)^{(q-1)-\frac{q+1}{4}}$$

- cálculo de R_3' tal que:

$$R'_3 = R'^2_2$$

- cálculo de R_4' tal que

$$R'_4 = R'_3.f(X_1)$$

en el cual, si R_4' no es igual a 1, en la etapa /2/-/iv/, se obtiene la raíz cuadrada de $f(X_2)$ según la ecuación siguiente:

$$\sqrt{f(X_2} = R_1.R_2^{'}$$

donde $R_1 = (f(X_1).f(X_2))^{\frac{q+1}{4}}$

en el cual R_1 es obtenido previamente según la ecuación siguiente:

$$R_1 = (f(X).f(X_2))^{\frac{q+1}{4}} = U.f(u)^{(q-1)-\frac{q+1}{4}}$$

Así, en un caso particular, es posible limitar todavía el número de exponenciaciones que hay que efectuar utilizando una familia particular de polinomios, tales que sea posible fijar el valor $X_3(t)$ para cualquier t posible, tal que $f(X_3(t))$ no sea nunca un término al cuadrado en F_q. Puede utilizarse aquí ventajosamente la familia de polinomios de Ulas tales como los descritos en el documento 'Rational points on certain hyperelliptic curves over finite fields' de Macie Ulas, de fecha 11 de junio de 2007.

Para una familia de polinomios de este tipo que verifiquen la igualdad de Skalba, puede escribirse:

$$X_1(t,u) = -\frac{b}{a}\left(1 + \frac{1}{t^4 f(u) + t^2 f(u)}\right)$$

$$X_2(t,u) = t^2 f(u) X_1(t,u)$$

$$X_3(t,u) = u$$

$$U(t,u) = t^3 f(u)^4 f(X_1(t,u))$$

donde $f(u) = u^3 + au + b$, donde a y b son elementos de F_q tal que su producto no sea nulo.

Es posible utilizar ventajosamente estos polinomios determinando un valor del parámetro u fijado tal que $f(X_3)=f(u)$ no sea un término al cuadrado en F_q.

Entonces, en la etapa /2/-/ii/, el término $f(X_1).f(X_2)$ no es un término al cuadrado en el cuerpo finito F_q, después, en la etapa /1/-/iii/, se prueba si el término $f(X_1)$ es un término al cuadrado en el cuerpo finito F_q según las etapas siguientes:

- cálculo de R_2' tal que

$$R_2^{'} = f(X_1)^{(q-1)-\frac{q+1}{4}}$$

- cálculo de R_3' tal que:

$$R_3^{'} = R_2^{'2}$$

- cálculo de R_4' tal que

$$R_4^{'} = R_{3.}^{'} f(X_1)$$

después, si R_4' no es igual a 1, en la etapa /1/-/iv/, se obtiene la raíz cuadrada de $f(X_2)$ según la ecuación siguiente:

$$\sqrt{f(X_2} = R_1.R_2^{'}$$

donde $R_1 = (f(X_1).f(X_2))^{\frac{q+1}{4}}$

ventajosamente, R_1 puede ser obtenido previamente según la ecuación siguiente:

$$R_1 = (f(X).f(X_2))^{\frac{q+1}{4}} = U.f(u)^{(q-1)-\frac{q+1}{4}}$$

En particular, el término $f(u)^{(q-1)-\frac{q+1}{4}}$ puede ser calculado de antemano. Esto es posible porque f(u) es calculado igualmente de antemano. En este caso particular de polinomios que verifiquen la igualdad de Skalba, es por tanto posible no tener que efectuar la exponenciación relativa al cálculo de $(f(X_1(t)).f(X_2(t)))^{\frac{q+1}{4}}$ en el transcurso de la puesta en práctica del procedimiento, sino justo la multiplicación $U(t).f(u))^{(q-1)-\frac{q+1}{4}}$. Así la puesta en práctica de un procedimiento de este tipo corresponde a una sola exponenciación, la del cálculo $R_2^{'} = f(X_1)^{(q-1)-\frac{q+1}{4}}$.

En este contexto, estos polinomios particulares son expresados en coordenadas jacobianas según las cuales el punto P(X,Y) se escribe P(X',Y',Z) tales que

$$X' = X.Z^2,$$

$$Y' = Y.Z^3$$

donde la función f se escribe fz(X') y verifica:

$$f_Z(X') = X'^3 + aX'Z^4 + bZ^6$$

verificando la curva elíptica la ecuación:

$$Y'^2 = f_Z(X')$$

donde los polinomios que verifican la igualdad de Skalba expresados en coordenadas jacobianas son $X'_1(t)$, $X'_2(t)$, Z(t) y U'(t) y verifican la igualdad de Skalba en coordenadas jacobianas:

$$U'(t)^2 = f_{Z(t)}(X'_1(t)).f_{Z(t)}(X'_2(t)).f_{Z(t)}(X'_3(t))$$

y donde Z(t) es determinada de modo que las operaciones de inversión sean transformadas en operación de multiplicación.

En la etapa /1/, el valor del parámetro t puede ser obtenido en función de una contraseña o un identificador. Puede, así, preverse tomar como parámetro la contraseña directamente o también una derivada de la contraseña.

En un modo de realización de la presente invención, la aplicación criptográfica es una aplicación de autenticación o de identificación por una entidad de control, y

en la etapa /1/, se realizan las etapas siguientes:

/a/ generación de un valor aleatorio;

/b/ obtención de un valor cifrado, cifrando el citado valor aleatorio sobre una base de una función de cifrado que utiliza una clave de cifrado determinada a partir de una contraseña o identificador correspondiente al parámetro; y

/c/ transmisión del valor cifrado a la entidad de control.

Procediendo así, la entidad de control está en condiciones de obtener el valor aleatorio en función del valor cifrado recibido a partir de la contraseña. Después, ésta recupera el valor del parámetro t aplicando una función adaptada.

Un segundo aspecto de la presente invención propone un dispositivo electrónico que comprenda medios adaptados para la puesta en práctica de un procedimiento de ejecución de un cálculo criptográfico de acuerdo con el primer aspecto de la presente invención.

Otros aspectos, objetivos y ventajas de la invención se pondrán de manifiesto con la lectura de la descripción de uno de los modos de realización.

La invención se comprenderá mejor igualmente con la ayuda de las figuras siguientes:

- la figura 1 ilustra las principales etapas de un procedimiento de ejecución de un cálculo criptográfico de acuerdo con un modo de realización de la presente invención;
- la figura 2 ilustra un procedimiento de ejecución de un cálculo criptográfico en detalle de acuerdo con un modo de realización de la presente invención;

- la figura 3 ilustra un procedimiento de ejecución de un cálculo criptográfico en detalle de acuerdo con un modo de realización de la presente invención en el caso particular de los polinomios de Ulas.

La figura 1 ilustra las principales etapas de un procedimiento de ejecución de un cálculo de acuerdo con un modo de realización de la presente invención.

Estas principales etapas están adaptadas para la determinación de un punto de una curva elíptica con el objetivo de utilizar este punto en el seno de una aplicación criptográfica. Un cálculo criptográfico de este tipo puede ser ejecutado en un componente electrónico de manera segura, es decir sin que la determinación de este punto dé ninguna información sobre el punto determinado.

Este cálculo comprende, en un cuerpo finito F_q donde q es igual a 3 mod 4, una etapa de obtención de un punto P(X,Y) de una curva elíptica que verifica la ecuación:

$$Y^2 = f(X)$$

Un punto P(X,Y) tiene su abscisa X que corresponde a uno de entre $X_1(t)$, $X_2(t)$ y $X_3(t)$, para un valor de t obtenido, tales que:

$$f(X_1)(t).f(X_2(t).f(X_3)(t) = U^2(t) \quad (2)$$

Donde $X_1(t)$, $X_2(t)$, $X_3(t)$ y U(t) son polinomios que verifican la ecuación de Skalba en el cuerpo finito F_q.

De modo más preciso, los polinomios que verifican la igualdad de Skalba, tales como los definidos en el documento 'Rational points on certain hyperelliptic curves over finite fields' de Maciej Ulas, de fecha 11 de junio de 2007 son función de dos parámetros u y t. En el contexto de la presente invención, uno de los parámetros puede ser ventajosamente fijado y por consiguiente los polinomios que verifican la ecuación de Skalba son entonces función de un solo parámetro t.

A fin de determinar un punto de la curva, se busca determinar, dados los parámetros de entrada u y t, aquéllos de los valores $X_1 = X_1(t, u)$, $X_2 = X_2(t,u)$, $X_3 = X_3(t,u)$ que correspondan a un término al cuadrado en el cuerpo finito F_q. A tal efecto, está previsto ventajosamente aplicar dos tratamientos diferentes en función del hecho de que el término $f(X_1).f(X_2)$ sea o no un término al cuadrado en el cuerpo finito F_q.

En una etapa inicial 100, se tiene en cuenta el parámetro t y se calcula:

$$X_i = X_i(t) \text{ para i comprendido entre 1 y 3}$$

y

$$U = U(t)$$

En una etapa 11, se decide si este producto $f(X_1).f(X_2)$ es un término al cuadrado. Esta decisión puede estar basada en cálculos previos o también en un control en el transcurso de la puesta en práctica del procedimiento. Si el término $f(X_1).f(X_2)$ es un término al cuadrado entonces el término $f(X_3)$ es igualmente un término al cuadrado. Se prevé en este caso calcular la raíz cuadrada del término $f(X_3)$, en una etapa 12. En una etapa 16, el punto P así determinado tiene por abscisa X_3 y por ordenada Y_3 que verifica la ecuación siguiente:

$$Y_3 = \sqrt{f(X_3)}$$

Conviene observar que si el término producto $f(X_1).f(X_2)$ es un término al cuadrado, se deduce que el término $f(X_3)$ es igualmente un término al cuadrado. Sin embargo, a fin de conservar una determinación de punto de la curva elíptica a tiempo constante, se prevé poner en práctica una prueba 10 con el fin de controlar si el término $f(X_3)$ es efectivamente un término al cuadrado. Esta prueba 10 permite garantizar la puesta en práctica del procedimiento de acuerdo con un modo de realización de la presente invención a tiempo constante.

En el otro caso, es decir cuando el término $f(X_1).f(X_2)$ no es un término al cuadrado, entonces se puede deducir que $f(X_1)$, o bien $f(X_2)$ es un término al cuadrado. Así pues, puede preverse controlar en primer lugar si el término $f(X_1)$ es un término al cuadrado en una etapa 13. Si la prueba es positiva, se calcula a continuación su raíz cuadrada en una etapa 14 para obtener la abscisa del punto P:

$$Y_1 = \sqrt{f(X_1}$$

En una etapa 17, se obtiene entonces el punto P que tiene por ordenada X1 y por abscisa Y1.

Si la prueba en la etapa 13 es negativa, se puede deducir entonces que el término $f(X_2)$ es un término al cuadrado. Por consiguiente, se obtiene en una etapa 15 la abscisa Y_2 de un punto P de la curva elíptica según la ecuación:

$$Y_2 = \sqrt{f(X_2)}$$

Así, en una etapa 18 puede facilitarse un punto $P(X_2,Y_2)$ de la curva.

Conviene observar que llegar a las etapas 16, 17 o también 18 de obtención de un punto de la curva elíptica de acuerdo con un modo de realización de la presente invención requiere operaciones similares. Así, cualesquiera que sean los parámetros de entrada t y u, no es posible hacer un ataque sobre la base del tiempo transcurrido.

El punto $P(X_i,Y_i)$, para una i comprendida entre 1 y 3, puede utilizarse después ventajosamente en una aplicación criptográfica de cifrado o de hashing o de firma o de autenticación o de identificación, puesto que su determinación no ha facilitado ningún elemento susceptible de violar su secreto.

En el cuerpo Fq, correspondiendo q a 3 mod 4, es posible controlar si un término es un término al cuadrado de diferentes maneras. Las pruebas de término al cuadrado tales como las pruebas 10 y 13 de la figura 1 pueden ser realizadas como sigue.

En un modo de realización de la presente invención, cuando se busca determinar si un término A es un término al cuadrado en F_q, se pueden efectuar las etapas siguientes:

$$W_1 = \frac{1}{A^{\frac{q+1}{4}}} = A^{(q-1)-\frac{q+1}{4}} \quad \text{(i)}$$

$$W_2 = W_1^2 \quad \text{(ii)}$$

$$W_3 = W_2.A \quad \text{(iii)}$$

En concreto, si el término A es un término al cuadrado, entonces:

- W_1 corresponde a la inversa de la raíz cuadrada de A, o sea $1/\sqrt{A}$, porque una exponenciación a (q-1) corresponde a una inversión y una exponenciación a (q+1)/4 corresponde a una raíz cuadrada en el cuerpo finito F_q;
- W_2 corresponde a la inversa de A; y
- W_3 corresponde al valor 1.

Así, cuando W_3 es igual al valor 1, se concluye que el término A es un término al cuadrado en el cuerpo finito F_q. Si A no es un término al cuadrado, entonces W_3 no es igual a 1.

La figura 2 ilustra la puesta en práctica de un procedimiento de ejecución de un cálculo de acuerdo con un modo de realización de la presente invención.

En un modo de realización de la presente invención, en una etapa 201, se efectúa la multiplicación siguiente:

$R_0 = f(X_1).f(X_2)$

Después, se controla si este término R_0 es un término al cuadrado aplicando las etapas (iv) y (v). Así, en una etapa 202, se calcula:

$R_1 = R_0^{(q+1)/4}$

Después, en la etapa 203, se determina si se verifica la ecuación siguiente:

$R_1^2 = R_0$

Se decide si el término R_0, igual a $f(X_1.f(X_2)$, es o no un término al cuadrado. En el caso en que el término R_0 sea un término al cuadrado, se pone en práctica una prueba que pretende determinar si el término $f(X_3)$ es un término al cuadrado. El resultado de esta última prueba es conocido previamente puesto que si R_0 es un término al cuadrado entonces esta prueba es positiva. Sin embargo, con el objetivo de garantizar un tiempo constante, conviene ponerle en práctica según las etapas (i) a (iii).

Así, en una etapa 204 se efectúa el cálculo siguiente:

$R_2 = f(X_3)^{(q-1-(q-1)/4)}$

Aquí, R_2 corresponde al cálculo de la inversa de la raíz cuadrada de $f(X_3)$, en el caso en que $f(X_3)$ sea un término al cuadrado.

Después, en una etapa 205, se calcula la ecuación siguiente:

$$R_3 = R_2^2$$

En este caso, R_3 corresponde a la inversa de $f(X_3)$.

Después, en una etapa 206, se multiplica R_3 por el término $f(X_3)$ para obtener un término R_4. Como se sabe que $f(X_3)$ es un término al cuadrado, se sabe igualmente que el término R_4 es igual a 1. Estas etapas 205 y 206 son puestas en práctica a fin de garantizar la determinación de un punto P de la curva elíptica a tiempo constante.

Así pues, en una etapa 207, se prueba si el término R_4 corresponde a 1. En el caso presente, esta prueba es siempre positiva, puesto que se deduce de la prueba 203.

A continuación, en una etapa 208, se efectúa el cálculo siguiente:

$$R_5 = R_2.f(X_3)$$

En este caso, se obtiene un punto P de la curva que tiene por abscisa X_3 y por ordenada la raíz cuadrada de $f(X_3)$, es decir el valor R_5.

En el caso en que en la etapa 11 se decida que el término $f(X_1).f(X_2)$ no es un término al cuadrado, entonces el término $f(X_1)$, o bien el término $f(X_2)$ es un término al cuadrado.

En lo que sigue, se trata de determinar cuál de estos dos términos $f(X_1)$ y $f(X_2)$ corresponde a un término al cuadrado.

A tal efecto, se efectúan operaciones similares a las descritas anteriormente, con la diferencia de que, en este caso, el término $f(X_1)$ puede no ser un término al cuadrado.

En la etapa 211, se calcula la ecuación siguiente:

$$R'_2 = f(X_1)^{q-1-(q+1)/4}$$

En el caso en que $f(X_1)$ sea un término al cuadrado, entonces R'_2 corresponde al valor de la inversa de la raíz cuadrada de $f(X_1)$ como se describe en la etapa (i). Después, en una etapa 212, este último término se eleva al cuadrado:

$$R'_3 = R'^2_2$$

para obtener la inversa de $f(X_1)$ en el caso en que $f(X_1)$ fuera un término al cuadrado.

Así, multiplicando R_3' por el término $f(X_1)$, se obtiene R_4' en una etapa 213 que vale 1 si el término $f(X_1)$ es efectivamente un término al cuadrado. En este caso, la prueba efectuada en una etapa 214 en el transcurso de la cual se compara el término R_4' con el valor 1 es positiva.

Después, en una etapa 215, se efectúa el cálculo siguiente:

$$R'_5 = R'_2.\ f(X_1)$$

El término R'_5 corresponde entonces a $f(X_1)$.

Se obtiene un punto P de la curva con su abscisa X_1, y su ordenada R'_5.

En el caso en que la prueba 214 sea negativa, el término $f(X_1)$ no es un término al cuadrado. Entonces, se deduce que el término al cuadrado de la ecuación de Skalba (2) es el término $f(X_2)$. En este caso, en una etapa 216, se efectúa el cálculo siguiente:

$$R''_5 = R_1.R'_2$$

Conviene observar que la ecuación anterior permite obtener ventajosamente la raíz cuadrada de $f(X_2)$ sin por ello efectuar una operación de exponenciación como la efectuada en la etapa 204 o también en la etapa 211. En efecto, se trata en este caso de efectuar de modo astuto una multiplicación en lugar de una exponenciación.

Se obtiene entonces R_5" que corresponde al término $f(X_2)$, facilitado en una etapa 216. Se ha determinado así un punto P de la curva elíptica que tiene por abscisa X_2 y por ordenada R_5".

En el modo de realización descrito anteriormente refiriéndose a la figura 2, cualquiera que sea la determinación del punto P, es decir que esta determinación esté basada en el valor X_1 o X_2 o también en X_3, se ponen en práctica cálculos similares garantizando así una determinación de punto de la curva elíptica a tiempo constante.

De manera más precisa, se ponen en práctica dos operaciones de exponenciación, una exponenciación en la etapa 202 y otra exponenciación en la etapa 204 o 211 según el resultado de la prueba 203. Así, ya no se requiere efectuar cuatro exponenciaciones para determinar a tiempo constante un punto en una curva en el contexto de los polinomios de Skalba.

En un modo de realización de la presente invención, es posible elegir polinomios que verifiquen la igualdad de Skalba de tal modo que el polinomio $f(X_3(t))$ no pueda corresponder nunca a un término al cuadrado cualquiera que sea el valor de t. En este caso, la ecuación de Skalba:

$$f(X_1(t)).f(X_2(t)).f(X_3(t)) = U^2(t) \quad (2)$$

puede escribirse en la forma:

$$(f(X_i(t)).f(X_2(t)).f(X_3(t))^{\frac{q+1}{4}} = (U(t)^2)^{\frac{q+1}{4}} = U(t)$$

y después, todavía en la forma:

$$(f(X_i(t)).f(X_2(t)))^{\frac{q+1}{4}} = \frac{U(t)}{f(X_3(t))^{\frac{q+1}{4}}}$$

y también:

$$(f(X_i(t)).f(X_2(t)))^{\frac{q+1}{4}} = (U(t).f(X_3(t))^{q-1-\frac{q+1}{4}} \quad (4)$$

Todas estas ecuaciones son solamente válidas si se realiza la condición q = 3 mod 4. Ahora bien, si el término $(f(X_3(t))^{q-1-\frac{q+1}{4}}$ de esta última ecuación corresponde a un valor fijo, se está en condiciones de calcular eficazmente el valor del término $R_1 = (f(X_i).f(X_2))^{\frac{q+1}{4}}$ gracias a la multiplicación $U.(f(X_3(t))^{q-1-\frac{q+1}{4}}$. En este caso, se puede determinar un punto de la curva elíptica poniendo en práctica solamente una operación de exponenciación, la que corresponde a la etapa 204 de la prueba 10, o la que corresponde a la etapa 211 de la prueba 13, según el caso.

Estas condiciones pueden ser satisfechas utilizando por ejemplo un conjunto de polinomios que verifiquen la ecuación de Skalba tales como los descritos en el documento 'Rational points on certain hyperelliptic curves over finite fields' de Macie Ulas, de fecha 11 de junio de 2007. En este documento, se describen los polinomios que verifican la ecuación de Skalba (2):

$$X_i(t,u) = -\frac{b}{a}\left(1 + \frac{1}{t^4 f(u) + t^2 f(u)}\right)$$

$$X_2(t,u) = t^2 f(u) X_1(t,u)$$

$$X_3(t,u) = u$$

$$U(t,u) = t^3 f(u)^4 f(X_1(t,u))$$

donde $f(u) = u^3 + au + b$

donde a y b son elementos de F_q tal que su producto no sea nulo.

Así, determinando un valor de u que sea fijado y que no corresponda a un término al cuadrado en F_q entonces el valor de R_1 es un valor fijado que puede ser precalculado según la ecuación (4), para cualquier determinación de punto P de acuerdo con un modo de realización de la presente invención.

La figura 3 ilustra un procedimiento de ejecución de un cálculo criptográfico en detalle de acuerdo con un modo de realización de la presente invención en el caso particular de los polinomios de Ulas, para un polinomio $X_3(t,u)$ fijado de acuerdo con un modo de realización de la presente invención. En este caso, solamente pueden ser puestas en práctica las etapas 211 a 216. Si se realiza la etapa 216, entonces el valor R_1 puede ser recuperado de una zona de memoria porque éste ha sido calculado previamente.

Debido a esto, se puede reducir todavía el número de exponenciaciones requerido para determinar un punto de la curva, a una sola exponenciación, la que corresponde a la prueba 10 o a la prueba 13.

En un modo de realización de la presente invención, se prevé utilizar ventajosamente las coordenadas jacobianas. Una transformación en coordenadas jacobianas de este tipo permite transformar las operaciones de inversión en operaciones de multiplicación que son más rápidas y más fáciles de poner en práctica. Conviene observar que tal modo de realización puede ser aplicado no a todas las curvas de tipo Skalba, incluso en el caso particular de las curvas de Ulas.

La ecuación de una curva elíptica:

$$X^3 + aX + b = Y^2$$

puede escribirse en coordenadas jacobianas:

$$X'^3 + aX'Z^4 + bZ^6 = Y'^2$$

Se observa que las coordenadas de un punto (X,Y) pueden escribirse en coordenadas jacobianas (X',Y',Z') tales que:

$$X' = X.Z^2 \text{ , e}$$

$$Y' = Y.Z^3$$

Así pues, conviene determinar un polinomio Z(t,u) de tal modo que las coordenadas jacobianas X', Y' y Z puedan escribirse sin inversión.

En las secciones siguientes, se aplica esta transformación en coordenadas jacobianas a un caso particular, el de las curvas Ulas tal como se describió anteriormente.

En este contexto, se elimina cualquier operación de inversión tomando:

$$Z(t,u) = a(t^4 f(u)^2 + t^2 f(u))$$

en el cual u está fijado.

En efecto, los polinomios de Ulas pueden escribirse entonces en coordenadas jacobianas en la forma siguiente:

$$X'_1(t,u) = -bZ(t,u)(t^4 f(u)^2 + t^2 f(u) + 1)$$

$$X'_2(t,u) = t^2 f(u) X'_1(t,u)$$

$$X'_3(t,u) = u$$

Así pues, conviene observar que en coordenadas jacobianas ya no hay inversión. Pudiendo ser esta operación tan laboriosa como una exponenciación, estas coordenadas permiten una mejora significativa del tiempo de cálculo.

Después, para obtener la coordenada Y' jacobiana, conviene calcular U'(t,u), el equivalente de U(t,u) en coordenadas jacobianas.

En este contexto, se tiene en coordenadas clásicas:

$$U(t,u)^2 = f(X_1(t,u)).f(X_2(t,u)).f(X_3(t,u))$$

Se puede escribir entonces en coordenadas jacobianas:

$$U(t,u)^2 = f(X'_1(t,u)/Z(t,u)^2).f(X'_2(t,u)/Z(t,u)^2).f(X'_3(t,u)/Z(t,u)^2)$$

Escribiendo

$$f_{Z(t)}(X') = X'^3 + aX'Z(t)^4 + bZ(t)^6 = Z^6.f(\frac{X}{Z^2})$$

se obtiene la ecuación siguiente:

$$Z^{18}(t,u).U(t,u)^2 = (Z(t,u)^9.U(t,u)^2 = f_{Z(t,u)}(X'_1(t,u)).f_{Z(t,u)}(X'_2(t,u)).f_{Z(t,u)}(X_3(t,u))$$

Después:

$$U'(t,u) = Z(t,u)^9 . U(t,u))$$

donde U'(t,u) es la expresión en coordenadas jacobianas de U(t,u).

En el caso en que se considere que U(t,u) verifique la ecuación:

$$U(t,u) = t^3 f(u)^2 . f(X_2(t,u))$$

se puede escribir entonces:

$$U(t,u) = t^3 f(u)^2 . f_{Z(t,u)}(X'_2(t,u)) . Z(t,u)^3$$

La igualdad de Skalba en coordenadas jacobianas pasa a ser:

$$U(t,u)^2 = f_{Z(t,u)}(X'_1(t,u)) . f_{Z(t,u)}(X'_2(t,u)) . f_{Z(t,u)}(X'_3(t,u))$$

Sin embargo, como en el caso de los polinomios de Ulas es posible imponer que $X'_3(t,u)$ sea tal que $f_{Z(t,u)} X'_3(t,u)$ no sea nunca un cuadrado. En este caso, se tiene:

$$U''(t,u) = t^3 f(u)^2 . f_{Z(t,u)}(X'_2(t,u))$$

y la igualdad de Skalba correspondiente es:

$$U''(t,u)^2 = f_{Z(t,u)}(X'_1(t,u)) . f_{Z(t,u)}(X'_2(t,u)) . f(X'_3(t,u))$$

La presente invención puede ser puesta en práctica ventajosamente en cualquier tipo de cálculo criptográfico que utilice curvas elípticas. Ésta puede ser especialmente ventajosa en el seno de protocolos de autenticación por contraseña, como PACE (de 'Password Authenticated Connection Establishment' en inglés). En este caso, ésta permite una mejora del rendimiento de los cálculos, al tiempo que no permite ningún ataque ligado al tiempo de ejecución del cálculo criptográfico.

La presente invención puede ser aplicada ventajosamente en el contexto de los protocolos que respetan la vida privada, tales como los que se utilizan para el control de documentos de identidad electrónicos, como los pasaportes electrónicos.

REIVINDICACIONES

1. Procedimiento de ejecución de un cálculo criptográfico en un componente electrónico que comprende una etapa de obtención de un punto P(X,Y) a partir de al menos un parámetro t, en una curva elíptica que verifica la ecuación:

$Y^2 = f(X)$, y

a partir de polinomios $X_1(t)$, $X_2(t)$, $X_3(t)$ y $U(t)$ que verifican la igualdad de Skalba siguiente:

$f(X_1(t)).f(X_2(t)).f(X_3(t)) = U(t)^2$

en el cuerpo finito F_q, cualquiera que sea el parámetro t, verificando q la ecuación $q = 3 \bmod 4$;

comprendiendo el citado procedimiento las etapas siguientes:

/1/ obtención de un valor del parámetro t;

/2/ determinación del punto P efectuando las subetapas siguientes:

/i/ cálculo de $X_1 = X_1(t)$, $X_2 = X_2(t)$, $X_3 = X_3(t)$ y $U = U(t)$

/ii/ si el término $f(X_1).f(X_2)$ es un término al cuadrado en el cuerpo finito F_q se prueba entones si el término $f(X_3)$ es un término al cuadrado en el cuerpo finito F_q y se calcula la raíz cuadrada del término $f(X_3)$, teniendo el punto P por abscisa X_3 y por ordenada la raíz cuadrada del término $f(X_3)$;

/iii/ si no, se prueba si el término $f(X_1)$ es un término al cuadrado en el cuerpo finito F_q y en este caso, se calcula la raíz cuadrada del término $f(X_1)$, teniendo el punto P por abscisa X_1 y por ordenada la raíz cuadrada del término $f(X_1)$;

/iv) si no, se calcula la raíz cuadrada del término $f(X_2)$, tendiendo el punto P por abscisa X_2 y por ordenada la raíz cuadrada de término $f(X_2)$;

/3/ utilización del citado punto P en una aplicación criptográfica de cifrado o de hashing o de firma o de autenticación o de identificación.

2. Procedimiento de ejecución de un cálculo criptográfico de acuerdo con la reivindicación 1, en el cual en la etapa /2/-/ii/ se efectúan las etapas siguientes:

- cálculo de R_1 tal que:

$$R_1 = (f(X_1).f(X_2))^{\frac{q+1}{4}}$$

- si R_1^2 es igual a $f(X_1).f(X_2)$, entonces decidir que el término $f(X_1).f(X_2)$ es un término al cuadrado en el cuerpo F_q;

en el cual, en la etapa /2/-/iii/, se prueba si el término $f(X_1)$ es un término al cuadrado en el cuerpo finito F_q según las etapas siguientes:

- cálculo de R_2' tal que

$$R_2' = f(X_1)^{(q-1)-\frac{q+1}{4}}$$

- cálculo de R_3' tal que:

$$R_3' = R_2'^2$$

- cálculo de R_4' tal que

$$R_4' = R_3'.f(X_1)$$

en el cual, si R_4' no es igual a 1, en la etapa /2/-/iv/, se obtiene la raíz cuadrada de $f(X_2)$ según la ecuación siguiente:

$$\sqrt{f(X_2)} = R_1.R_2'$$

3. Procedimiento de ejecución de un cálculo criptográfico de acuerdo con las reivindicaciones 1 o 2, en el cual los polinomios que verifican la igualdad de Skalba son expresados en coordenadas jacobianas según las cuales el punto P(X,Y) se escribe P(X',Y',Z) tales que

$$X' = X.Z^2 ,$$

$$Y' = Y.Z^3$$

donde la función f se escribe $F_Z(X')$ y verifica:

$$f_Z(X') = X'^3 + a \cdot X' \cdot Z^4 + b \cdot Z^6$$

verificando la curva elíptica la ecuación:

$$Y'^2 = f_Z(X')$$

en el cual los polinomios que verifican la igualdad de Skalba expresados en coordenadas jacobianas son $X'_1(t)$, $X'_2(t)$, $X'_3(t)$, Z(t) y U'(t) y verifican la igualdad de Skalba en coordenadas jacobianas:

$$U'(t)^2 = f_{Z(t)}(X'_1(t)).f_{Z(t)}(X'_2(t)).f_{Z(t)}(X'_3(t))$$

y en el cual Z(t) es determinada de modo que las operaciones de inversión sean transformadas en operación de multiplicación.

4. Procedimiento de ejecución de un cálculo criptográfico de acuerdo con las reivindicaciones 1 o 2, en el cual los polinomios que verifican la igualdad de Skalba son tales que es posible fijar el valor de $X_3(t)$ para cualquier t posible, tal que $f(X_3(t))$ no sea nunca un término al cuadrado en F_q,

y en el cual, en la etapa /2/-/ii/, el término $f(X_1).f(X_2)$ no es un término al cuadrado en el cuerpo finito F_q,

en el cual, en la etapa /2/-/iii/, se prueba si el término $f(X_1)$ es un término al cuadrado en el cuerpo finito F_q según las etapas siguientes:

- cálculo de R_2' tal que

$$R_2' = f(X_1)^{(q-1)-\frac{q+1}{4}}$$

- cálculo de R_3' tal que:

$$R_3' = R_2'^2$$

- cálculo de R_4' tal que

$$R_4' = R_3'.f(X_1)$$

después, si R_4' no es igual a 1, en la etapa /2/-/iv/, se obtiene la raíz cuadrada de $f(X_2)$ según la ecuación siguiente:

$$\sqrt{f(X_2)} = R_1.R_2'$$

donde $R_1 = (f(X_1).f(X_2))^{\frac{q+1}{4}}$

en el cual R_1 es obtenido previamente según la ecuación siguiente:

$$R_1 = (f(X).f(X_2))^{\frac{q+1}{4}} = U.f(u)^{(q-1)-\frac{q+1}{4}}$$

5. Procedimiento de ejecución de un cálculo criptográfico de acuerdo con la reivindicación 4, en el cual los polinomios que verifican la igualdad de Skalba son expresados en coordenadas jacobianas según las cuales el punto P(X,Y) se escribe P(X',Y',Z) tales que

$$X' = X.Z^2 ,$$

$$Y' = Y.Z^3$$

donde la función f se escribe $F_Z(X')$ y verifica:

$$f_Z(X') = X'^3 + a \cdot X' \cdot Z^4 + b \cdot Z^6$$

verificando la curva elíptica la ecuación:

$$Y'^2 = f_Z(X')$$

en el cual los polinomios que verifican la igualdad de Skalba expresados en coordenadas jacobianas son $X'_1(t)$, $X'_2(t)$, Z(t) y U'(t) y verifican la igualdad de Skalba en coordenadas jacobianas:

$$U'(t)^2 = f_{Z(t)}(X'_1(t)).f_{Z(t)}(X'_2(t)).f(X_3(t))$$

y en el cual Z(t) es determinado de modo que las operaciones de inversión sean transformadas en operación de multiplicación.

6. Procedimiento de ejecución de un cálculo criptográfico de acuerdo con una cualquiera de las reivindicaciones precedentes, en el cual, en la etapa /1/, el valor del parámetro t es obtenido en función de una contraseña o un identificador.

7. Procedimiento de ejecución de un cálculo criptográfico de acuerdo con una cualquiera de las reivindicaciones 1 a 5, en el cual la aplicación criptográfica es una aplicación de autenticación o de identificación por una entidad de control, y

en el cual, en la etapa /1/, se realizan las etapas siguientes:

/a/ generación de un valor aleatorio;

/b/ obtención de un valor cifrado, cifrando el citado valor aleatorio sobre una base de una función de cifrado que utiliza una clave de cifrado determinada a partir de una contraseña o identificador correspondiente al parámetro; y

/c/ transmisión del valor cifrado a la entidad de control.

8. Dispositivo electrónico que comprende medios adaptados para la puesta en práctica de un procedimiento de ejecución de un cálculo criptográfico de acuerdo con una cualquiera de las reivindicaciones 1 a 7.

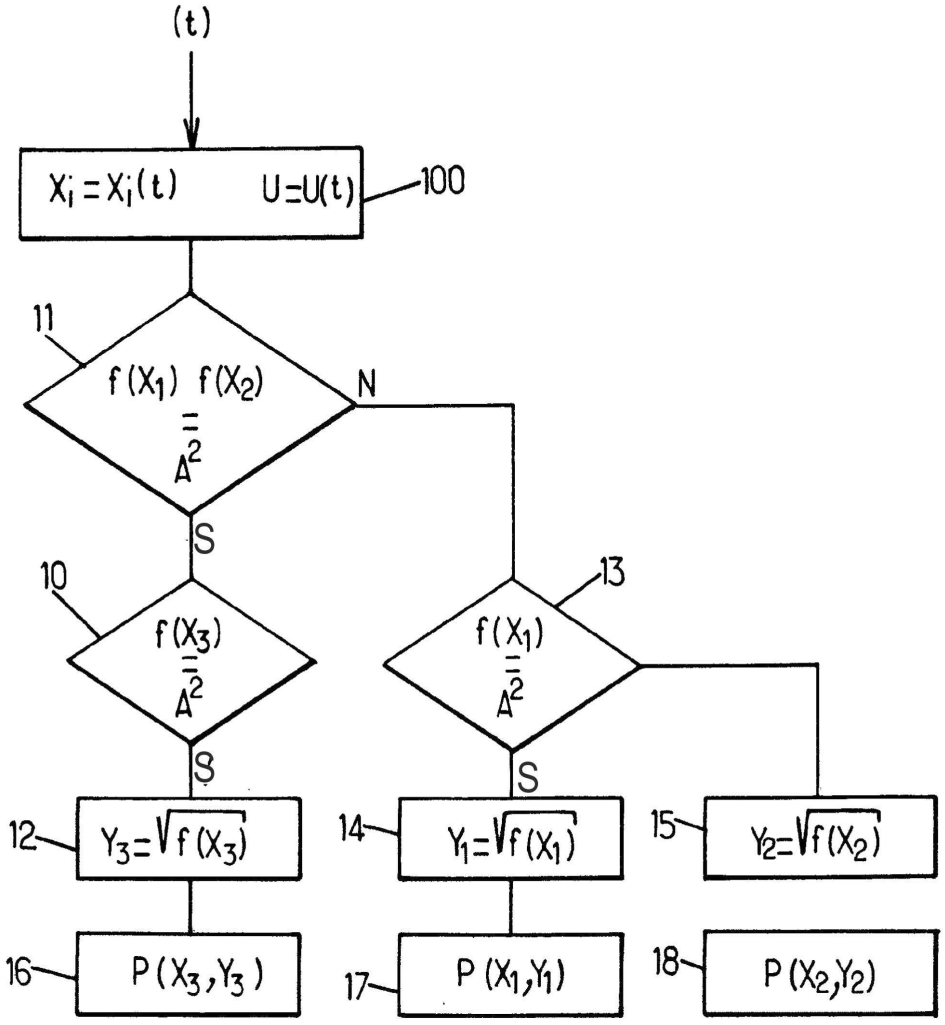
(t)
Xi = Xi(t)
U=U(t)
100
11
f(X1) f(X2)
A2
N
S
10
f(X3)
A2
13
f(X1)
A2
S
S
12
Y3=√f(X3)
14
Y1=√f(X1)
15
Y2=√f(X2)
16
P(X3,Y3)
17
P(X1,Y1)
18
P(X2,Y2)

FIG.1.

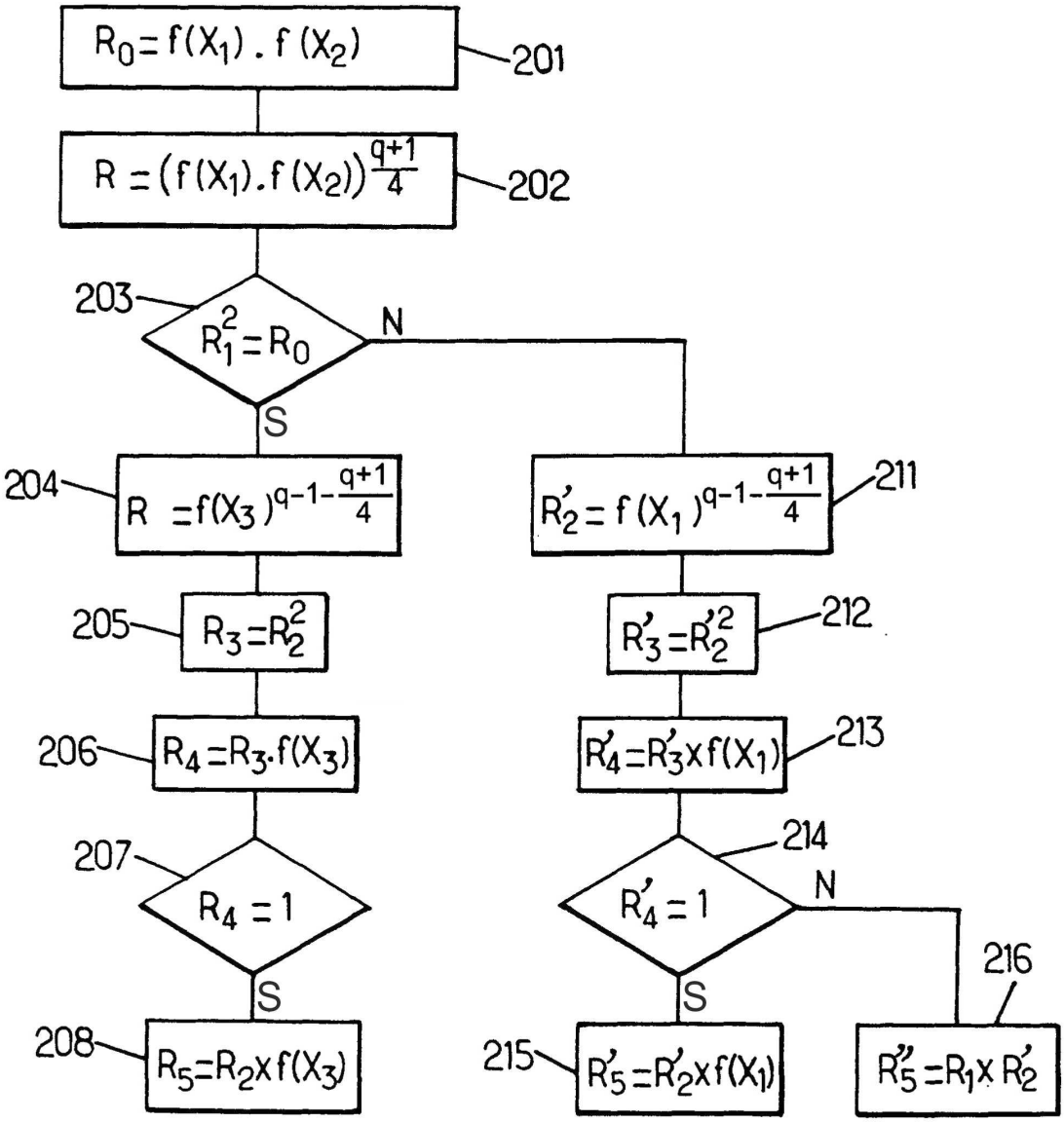
$R_0 = f(X_1) \cdot f(X_2)$
201
$R = (f(X_1) \cdot f(X_2))^{\frac{q+1}{4}}$
202
203
$R_1^2 = R_0$
N
S
204
$R = f(X_3)^{q-1-\frac{q+1}{4}}$
205
$R_3 = R_2^2$
206
$R_4 = R_3 \cdot f(X_3)$
207
$R_4 = 1$
S
208
$R_5 = R_2 \times f(X_3)$
211
$R'_2 = f(X_1)^{q-1-\frac{q+1}{4}}$
212
$R'_3 = R'^2_2$
213
$R'_4 = R'_3 \times f(X_1)$
214
$R'_4 = 1$
N
S
215
$R'_5 = R'_2 \times f(X_1)$
216
$R''_5 = R_1 \times R'_2$

FIG.2.

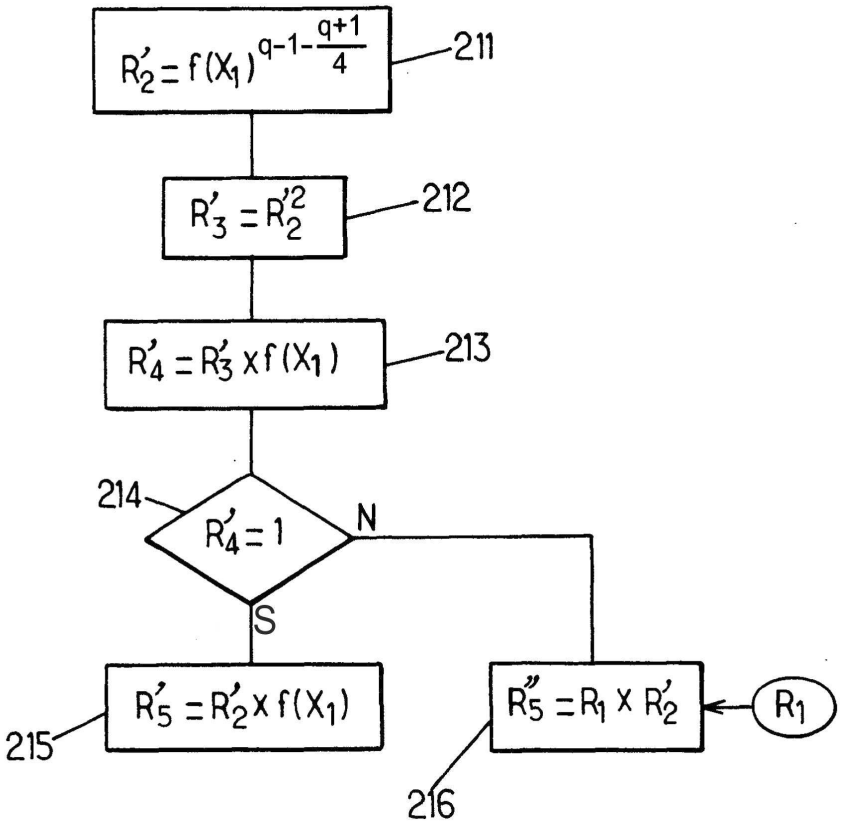
$R'_2 = f(X_1)^{q-1-\frac{q+1}{4}}$
211
$R'_3 = R'^2_2$
212
$R'_4 = R'_3 \times f(X_1)$
213
214
$R'_4 = 1$
N
S
$R'_5 = R'_2 \times f(X_1)$
215
$R''_5 = R_1 \times R'_2$
216
R_1

FIG.3.