(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 357 290**

(51) Int. Cl.:
G06F 7/72 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07727183 .1**
(96) Fecha de presentación : **21.03.2007**
(97) Número de publicación de la solicitud: **1999571**
(97) Fecha de publicación de la solicitud: **10.12.2008**

(54) Título: **Procedimiento y dispositivo de reducción de un polinomio en un campo finito binario, en particular para una aplicación criptográfica.**

(30) Prioridad: **22.03.2006 DE 10 2006 013 989**

(45) Fecha de publicación de la mención BOPI:
25.04.2011

(45) Fecha de la publicación del folleto de la patente:
25.04.2011

(73) Titular/es: **IHP GmbH-Innovations for High Performance Microelectronics/Leibniz-Institut für Innovative Mikro**
Im Technologiepark 25
15236 Frankfurt/Oder, DE

(72) Inventor/es: **Langendörfer, Peter y**
Peter, Steffen

(74) Agente: **Isern Cuyas, María Luisa**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

Venta de fascículos: Oficina Española de Patentes y Marcas. Pº de la Castellana, 75 – 28071 Madrid

DESCRIPCIÓN

Procedimiento y dispositivo de reducción de un polinomio en un campo finito binario, en particular para una aplicación criptográfica.

La invención se refiere a un procedimiento y un dispositivo para reducir una primera palabra de datos binaria, que corresponde a un polinomio C(x) y que presenta una longitud máxima de 2n-1, a una segunda palabra de datos con una longitud máxima igual a m, que corresponde a un polinomio C"0(x) equivalente a C(x) en un campo finito binario cuyos elementos tienen una longitud máxima igual a m, siendo m menor o igual que n. La invención también se refiere a un procedimiento y un dispositivo criptográfico.

Los procedimientos criptográficos sirven para proteger datos frente a un acceso no autorizado. Los procedimientos criptográficos transforman los datos a proteger, en particular incluyendo un *código* secreto, en datos codificados. Los procedimientos criptográficos sirven también para descodificar los datos codificados incluyendo el código secreto para restablecer los datos a proteger.

Los procedimientos de codificación asimétricos como el RSA y la criptografía de curva elíptica (Elliptic Curve Cryptography, ECC) se utilizan para garantizar un intercambio seguro de códigos para procedimientos criptográficos y para calcular firmas digitales.

La criptografía de curva elíptica requiere una longitud de código claramente menor que el RSA con el mismo grado de seguridad. Además, para la criptografía de curva elíptica se pueden utilizar campos de Galois finitos binarios $GF(2^m)$, que gracias a sus propiedades algebraicas son muy adecuados para implementaciones de hardware. En este contexto, m indica la longitud de los elementos de cada campo de Galois correspondiente.

La operación más importante en la utilización de la criptografía de curva elíptica consiste en la multiplicación de grandes polinomios. Como es sabido, después de una multiplicación de polinomios en un campo finito, los posibles productos resultantes son más largos que el elemento más grande del campo finito utilizado como base. Por ello, después de una multiplicación de polinomios se ha de llevar a cabo una, así llamada, reducción. En esta reducción, el polinomio largo del producto resultante se convierte en un valor ("equivalente") dentro de los límites del campo. Esta operación es necesaria después de cada multiplicación de polinomios.

Dado que la multiplicación en la criptografía de curva elíptica constituye una operación principal, no sólo la operación de multiplicación es crítica para el rendimiento (performance) en el sentido de la rapidez de una implementación de ECC, sino también la operación de reducción.

La reducción corresponde a la división con resto (operación módulo) en campos finitos "normales". Esto se puede explicar mediante un sencillo ejemplo: el campo finito GF(7) consiste en los elementos {0,1,2,3,4,5,6}. Una multiplicación de 5*4 es igual a 20, que es mayor que el elemento más grande posible en el campo. En este caso se divide 20 por 7 y el resto de esta división, es decir, 6, es también el resultado de la multiplicación de 5*4 dentro del campo finito (GF(7)).

Los campos finitos binarios ($GF(2^m)$) no incluyen números, sino polinomios. Un elemento de estos campos es $A(x)=a_{m-1}*x^{m-1}+a_{m-2}*x^{m-2}+...+a_1*x+a_0$. Los coeficientes a_i son 0 o 1. Una propiedad importante de los campos consiste en que en la adición y sustracción de coeficientes se utiliza la operación XOR (O exclusiva). Por tanto, 1+1≡1-1≡1 XOR 1=0.

La longitud máxima de un elemento del campo $GF(2^m)$ es m. La multiplicación de dos elementos (A(x)*B(x)) da como resultado un polinomio el doble de largo $C(x)=A(x)*B(x)=c_{m-2}*x^{2m-2}+...+c_0$. Por tanto, el resultado tiene una longitud de 2m-1.

El polinomio C(x) se puede descomponer en $C(x)= C1(x)*x^m+C0(x)$. C0(x) tiene la longitud correspondiente a la longitud máxima de los polinomios del campo. C1(x) es la parte que sobresale de la longitud máxima del campo y que se ha de integrar en C0 mediante el proceso de reducción.

Esta reducción puede resolverse mediante una división de polinomios completa, lo que requiere mucho tiempo. Un procedimiento de este tipo corresponde exactamente a la división módulo arriba explicada en el ejemplo de GF(7).

Existen posibilidades alternativas para realizar esta reducción más rápidamente. Un método usado con frecuencia consiste en la reducción multiplicativa. Si se multiplica C1(x) por un polinomio de reducción R(x) y el producto obtenido se le resta a C(x), el resultado es menor que el polinomio inicial, pero equivalente dentro del campo usado como base. Es aplicable: C(x)≡C(x)-C1(x)*R(x). Si se repite esta operación se obtienen campos cada vez más pequeños, pero equivalentes dentro del campo utilizado como base. La reducción termina cuando C1(x) llega a la longitud cero.

Si se conoce la longitud del campo y el polinomio de reducción R(x), se puede realizar muy eficientemente un cableado directo de la lógica de reducción. Esto se da a conocer p. ej. en la publicación de Saqib, N. A., Rodriguez-Henriquez, F., y Diaz-Perez, A., "A parallel architecture for fast computation of elliptic curve scalar multiplication

over GF(2m)", 18th International Parallel & Distributed Processing Symposium (IPDPS), Santa Fe, New Mexico, 26-30 de abril de 2004.

Sin embargo, la desventaja del sistema dado a conocer en dicha publicación consiste precisamente en que requiere el conocimiento de la longitud del campo y del polinomio de reducción R(x). Por ello se intenta encontrar un método con una eficiencia similar que posibilite estas operaciones para campos de duración variable con polinomios de reducción variables en hardware.

Una posibilidad ya dada a conocer en el documento de Eberle, H., Gura, N., y Chang-Shantz, S., "A cryptograhpic processor for arbitrary elliptic curves over GF(2m)", IEEE 14th International Conference on Application-specific Systems, Architectures and Processors (ASAP), 24-26 de junio, 2003, pags. 444-454, consiste en usar un multiplicador completo para el paso de reducción C(x)-C1(x)*R(x). Sin embargo, una multiplicación completa adicional en este punto es muy negativa para la rapidez de la implementación de ECC.

Por el documento US2003/0208518 A1 (Figura 32 de dicho documento) se conoce la realización de un paso de cálculo $C'(x)=C1(x)*(M-x^m)+x^{n-m}+C0(x)$ en la reducción multiplicativa de polinomios con orientación centrada, hasta que desaparece la parte sobresaliente del polinomio resultante. En este contexto, M designa un polinomio irreducible. El procedimiento incluye el paso consistente en almacenar el polinomio de reducción sin el término x^m desplazado hacia la izquierda n-m posiciones y rellenar las posiciones marginales a la izquierda y la derecha con el valor cero. Para una implementación de 233 bits (m=233) con $M=x^{233}+x^{74}+1$ en un hardware de 256 bits (n=256), resulta $(M-x^m)*x^{n-m}= (x^{74}+1)* x^{256-233}=x^{97}+x^{23}$. Este polinomio reutilizable para todo el proceso de reducción se multiplica por la parte sobresaliente C1(x) y se añade a C0(x) (XOR), hasta que C1(x) es igual a cero. Por consiguiente, se requieren repetidas multiplicaciones completas de polinomios. A continuación, el polinomio reducido equivalente así calculado se desplaza hacia la izquierda mediante una multiplicación por x^m.

En una variante descrita en el documento US2003/0208518 A1 (Figura 33) está previsto utilizar un polinomio parcialmente reducido en lugar del polinomio original para el cálculo de operaciones de multiplicación puntual, para a continuación llevar a cabo la reducción correspondientemente al procedimiento arriba descrito. De este modo, con una implementación se pueden realizar operaciones en los campos $GF(2^m)$ con valores m diferentes.

En el documento US2003/0182340 A1 se da a conocer un dispositivo de cálculo de valor residual a través de un campo de Galois, que funciona a un ritmo lento y que es especialmente adecuado para un cálculo de valor residual que puede ser utilizado en un procedimiento criptográfico en el que se emplean curvas elípticas. Para ello se propone una disposición de diferentes funciones lógicas y un esquema del funcionamiento de esta disposición. En este caso se multiplican dos expresiones a través de un campo de Galois GF (2^m) por un polinomio irreducible como módulo. Para ello, una de las dos expresiones se lleva a un sumador a través de una puerta Y cuando el bit de control correspondiente de la segunda expresión es 1. En caso contrario se lleva al sumador una expresión consistente exclusivamente en valores 0. El sumador está realizado en forma de elementos EXOR (O exclusiva), ya que en los campos GF (2^m) no es necesaria una aritmética de arrastre. Dependiendo del bit de mayor valor de la salida del sumador, la expresión módulo se resta de la salida del sumador, pudiendo presentar el sustractor en el campo GF (2^m) utilizado una configuración idéntica a la del sumador. De este modo se calcula un valor residual temporal, que se lleva de nuevo al sumador a través de un circuito de desplazamiento. Mediante este procedimiento se evita la suma de múltiplos del módulo, que de todos modos no contribuyen al valor residual. Mediante la repetición correspondiente del proceso arriba descrito se calculan el valor residual y el cociente del producto de las dos expresiones iniciales módulo del polinomio irreducible indicado.

Sin embargo, una desventaja del procedimiento descrito en dicho documento consiste en la necesidad de realizar reiteradas multiplicaciones completas de polinomios para la reducción. Para la reducción se requieren numerosos ciclos de reloj.

Por consiguiente, el problema técnico que sirve de base a la presente invención consiste en proponer un procedimiento y un dispositivo para la reducción de un producto de polinomios, que posibiliten la realización de una reducción en muy pocos ciclos de reloj en campos de distinta longitud y con polinomios de reducción diferentes.

La invención se refleja en tres aspectos. Dos aspectos se refieren a un procedimiento y un tercer aspecto se refiere a un dispositivo.

De acuerdo con un primer aspecto de la invención se propone un procedimiento para reducir una primera palabra de datos, que corresponde a un polinomio C(x) y que presenta una longitud máxima de 2n-1, a una segunda palabra de datos con una longitud máxima igual a m. La segunda palabra de datos corresponde a un polinomio C"0(x) equivalente a C(x) en un campo finito binario $GF(2^m)$ cuyos elementos tienen una longitud máxima igual a m, siendo m menor o igual que n. El procedimiento incluye los siguientes pasos:

- preparación de un polinomio de reducción R(x) consistente en un trinomio o un pentanomio;
- partición de la primera palabra de datos en una primera subpalabra de datos binaria C0 y una segunda subpalabra de datos binaria C1 cuyos polinomios correspondientes, C0(x) y C1(x), satisfacen la ecuación $C(x)=C1(x)*x^m+C0(x)$, y toma de la segunda subpalabra de datos para formar un primer término de sumandos;

- desplazamiento a la derecha de la segunda subpalabra de datos para formar un segundo término de sumandos, y repetición del paso de desplazamiento a la derecha para formar otros términos de sumandos hasta que cada término que no desaparezca del polinomio de reducción, que no sea el término x^m, tenga asignado un término de sumandos, siendo la anchura de paso de cada desplazamiento a la derecha igual a la diferencia entre m y el orden de un término correspondiente que no desaparece del polinomio de reducción;

- adición de los términos de sumandos formados a la primera subpalabra de datos para formar una palabra de datos de suma;

- si la palabra de datos de suma así determinada tiene una longitud mayor que m, aplicación de los pasos de procedimiento a partir del paso de partición a la palabra de datos de sumandos formada, hasta que la palabra de datos de suma así determinada tenga una longitud máxima igual a m y por consiguiente constituya la segunda palabra de datos.

El procedimiento según la invención para reducir una primera palabra de datos posibilita una realización especialmente rápida en pocos ciclos de reloj en una implementación de hardware. En un ejemplo de realización preferente, que se describe más abajo, la reducción tiene lugar incluso en un único ciclo de reloj.

El procedimiento según la invención incluye diferentes medidas que conducen a dicha aceleración de la operación de reducción en comparación con procedimientos conocidos.

De acuerdo con la invención, en primer lugar se prepara un polinomio de reducción R(x) consistente en un trinomio o un pentanomio. Los trinomios son polinomios con tres términos ocupados. Los pentanomios son polinomios con cinco términos ocupados. Con esta medida, el procedimiento según la invención aprovecha las propiedades de los campos finitos binarios utilizados en la práctica en la criptografía de curva elíptica, ya que éstos son recomendados por gremios de normalización, como p. ej. el National Institut of Standards and Technology (NIST) americano.

Dado que además la segunda posición ocupada más alta de los polinomios de reducción recomendados es por regla general menor que m/2, una reducción completa se puede concluir después de dos multiplicaciones sucesivas.

Además, en el procedimiento según la invención se realizan pasos de multiplicación mediante operaciones de desplazamiento flexibles. Esto conduce a una simplificación esencial de los pasos de multiplicación necesarios y al mismo tiempo a una implementación de hardware flexible que permite reducir productos de palabras de datos con longitudes diferentes (pero iguales en un producto correspondiente).

El procedimiento de reducción según la invención se puede describir matemáticamente de la siguiente manera: partiendo de un polinomio con la forma

$$C(x)=C1(x)*x^m-C0(x) \quad (1)$$

en una primera iteración de la operación de reducción se calcula la siguiente diferencia:

$$C'(x)=C(x)-C1(x)*R(x) \quad (2)$$

A continuación se explica cómo se calcula esta diferencia de forma especialmente sencilla según la invención. La ecuación (2) también se puede representar como

$$C'(x)=C1(x)*x^m+C0(x)-(C1(x)*x^m+C1(x)*x^m/x^{S3}+C1(x)*x^m/x^{S2}+C1(x)*x^m/x^{S1}+C1(x)*x^m/x^{S0}) \quad (3)$$

La ecuación (3) es equivalente a

$$C'(x)=C0(x)-(C1(x)*x^m/x^{S3}+C1(x)*x^m/x^{S2}+C1(x)*x^m/x^{S1}+C1(x)*x^m/x^{S0}) \quad (4)$$

Las divisiones por los términos x^{S3}, x^{S2}, x^{S1}, x^{S0} corresponden a operaciones de desplazamiento a la derecha con una anchura de paso correspondiente al orden de los términos x^{S3}, x^{S2}, x^{S1} y x^{S0} que no desaparecen del polinomio de reducción.

En muchos casos, después de esta primera utilización del polinomio de reducción todavía no se ha logrado una reducción completa. Por ello se lleva a cabo un siguiente paso de iteración basado en una representación del resultado intermedio C'(x) de la siguiente forma:

$$C'(x)=C1'(x)*x^m+C0'(x) \quad (5)$$

La longitud máxima del resultado intermedio C1'(x) es m-s3-1. La nueva utilización del polinomio de reducción tiene lugar de acuerdo con la ecuación

$$C''(x)=C'(x)-C1'(x)*R(x)=C1''(x)*x^m+C0''(x) \quad (6)$$

Si m<2*s3, el orden del término C1''(x) es cero. Por tanto, en este caso la reducción sólo requiere dos iteraciones.

El paso de partición de la primera palabra de datos incluido en el procedimiento según la invención no implica necesariamente una descomposición física de la primera palabra de datos en dos subpalabras de datos independientes, ni siquiera su almacenamiento por separado en memorias o registros. Para la partición sólo es esencial que las subpalabras de datos se utilicen por separado en el curso posterior del procedimiento. Para ello, en una implementación de hardware ventajosa, puede bastar un cableado independiente de las posiciones de bit de las subpalabras de datos en un registro que contiene la primera palabra de datos completa, con implementaciones de operación posconectadas en cada caso.

Por el concepto "longitud de una palabra de datos de sumandos formada" se ha de entender la posición de valor máximo cuyo valor es diferente de cero. Por consiguiente, si una palabra de datos de sumandos tiene una longitud mayor que m, significa que en posiciones > m hay valores diferentes de cero.

El paso incluido en el procedimiento según la invención consistente en el desplazamiento a la derecha de la segunda subpalabra de datos para formar un segundo término de sumandos, y en la repetición del paso de desplazamiento a la derecha para formar otros términos de sumandos, se ha de entender de tal modo que el segundo término de sumandos se utiliza desplazado a la derecha en el resultado en comparación con la segunda subpalabra de datos C(1) en su posición original en la primera palabra de datos (C0+C1). Esto se puede lograr no sólo mediante un desplazamiento real a la derecha, sino también por ejemplo tomando primero la segunda subpalabra de datos alineada a la derecha y desplazándola después hacia la izquierda con una anchura de paso a adaptar correspondientemente en cada caso. No obstante, el resultado evidentemente es el mismo.

De acuerdo con un segundo aspecto de la invención se propone un procedimiento para reducir una primera palabra de datos, que corresponde a un polinomio C(x) y que presenta una longitud máxima de 2n-1, a una segunda palabra de datos con una longitud máxima igual a m, que corresponde a un polinomio C"0(x) equivalente a C(x) en un campo finito binario GF(2^m) cuyos elementos tienen una longitud máxima igual a m, siendo m menor o igual que n, que incluye los siguientes pasos:

- preparación de un polinomio de reducción R(x) consistente en un trinomio o un pentanomio;
- partición de la primera palabra de datos en una primera subpalabra de datos binaria C0 y una segunda subpalabra de datos binaria C1 cuyos polinomios correspondientes, C0(x) y C1(x), satisfacen la ecuación $C(x)= C1(x)*x^m+C0(x)$, y toma de la segunda subpalabra de datos para formar un primer término de sumandos;
- desplazamiento a la derecha de la segunda subpalabra de datos para formar un segundo término de sumandos, y repetición del paso de desplazamiento a la derecha para formar otros términos de sumandos hasta que cada término que no desaparezca del polinomio de reducción, que no sea el término x^m, tenga asignado un término de sumandos, siendo la anchura de paso de cada desplazamiento a la derecha igual a la diferencia entre m y el orden de un término correspondiente que no desaparece del polinomio de reducción;
- adición de los términos de sumandos formados, a excepción del primer término de sumandos, a la primera subpalabra de datos (en adelante, también llamada primer paso de adición);
- si la palabra de datos de suma así determinada tiene una longitud mayor que m, aplicación de los pasos de procedimiento a partir del paso de partición a la palabra de datos de sumandos formada, hasta que la palabra de datos de suma así determinada tenga una longitud máxima igual a m;
- adición del primer término de sumandos y, en el caso mencionado de una aplicación de los pasos de procedimiento a partir del paso de partición a la palabra de datos de sumandos formada, de cada segunda subpalabra de datos adicional determinada entre tanto, a la palabra de datos de suma determinada en último lugar para formar la segunda palabra de datos (en adelante, también llamada segundo paso de adición).

El procedimiento del segundo aspecto de la invención se diferencia del procedimiento del primer aspecto de la invención en que los primeros términos de sumandos correspondientes, es decir, las segundas subpalabras de datos correspondientes, no se suman a la palabra de datos de sumandos determinada en último lugar hasta el final, después de la realización de todas las iteraciones necesarias para la reducción, para formar la segunda palabra de datos completamente reducida.

La ventaja adicional del procedimiento del segundo aspecto de la invención consiste en que posibilita implementaciones de hardware todavía más compactas, ya que, en un dispositivo de reducción según la invención, una unidad de desplazamiento prevista en el mismo sólo ha de realizar un máximo de tres operaciones de desplazamiento a la derecha para la realización de este procedimiento. De este modo se ahorra superficie de chip.

El procedimiento de este aspecto de la invención se basa en el conocimiento de que todos los polinomios irreducibles tienen la siguiente estructura:

$$R(x)=x^m+...+1 \quad (7)$$

Por consiguiente, los términos x^m y 1 forman parte de cada polinomio de reducción R(x). Dado que el orden más bajo del polinomio de reducción siempre es cero ($x^0 = 1$), y que s0 corresponde a la diferencia entre m y cero, s0 siempre es equivalente a m. Por ello, para este término realmente no se requiere ningún desplazamiento a la derecha y la adición necesaria se puede realizar a continuación de las iteraciones.

Tras ventajas de este procedimiento se desprenden de la siguiente descripción de ejemplos de realización, que también se refieren al procedimiento de acuerdo con el primer aspecto de la invención. Los ejemplos de realización se pueden combinar entre sí siempre que no se indique expresamente que se trata de ejemplos de realización alternativos entre sí.

De acuerdo con un ejemplo de realización preferente del procedimiento según la invención, en el que la primera palabra de datos tiene una longitud menor que 2n-1, antes de la operación de desplazamiento a la derecha se lleva a cabo un primer paso de justificación adicional. El primer paso de justificación incluye un desplazamiento a la izquierda de la primera palabra de datos con una anchura de paso de relleno, y una adición de una cantidad de ceros correspondiente a la anchura de paso de relleno a ambos lados de la primera palabra de datos. El desplazamiento a la izquierda y la adición de los ceros se realizan de tal modo que la longitud de la primera palabra de datos así modificada es igual a 2n-1 y que, en la primera palabra de datos modificada, aquellos términos del polinomio C(x) correspondiente a la primera palabra de datos que tienen un orden mayor que m están dispuestos en las mismas posiciones de bit que ocuparían si la primera palabra de datos ya hubiera tenido desde un principio la longitud 2n-1.

De este modo, en una única implementación de hardware también se pueden reducir palabras de datos más pequeñas. Por consiguiente, se aumenta la flexibilidad de una implementación de hardware.

Preferentemente, en esta realización del procedimiento se lleva a cabo un segundo paso de justificación, que en el procedimiento de acuerdo con el primer aspecto de la invención se realiza en particular después de la adición de los términos de sumandos formados a la primera subpalabra de datos para formar la palabra de datos de sumandos en el último paso de iteración. En el procedimiento de acuerdo con el segundo aspecto de la invención, el segundo paso de justificación se lleva a cabo en particular antes del segundo paso de adición.

En una forma de realización especialmente preferente del procedimiento según la invención, el polinomio irreducible se representa exclusivamente mediante las potencias de los términos que no desaparecen del polinomio de reducción y que no son el término x^m. Esto significa que el polinomio de reducción no se almacena con la longitud completa de una palabra de datos, sino únicamente en la forma (s1, s2, s3). De este modo, el procedimiento se simplifica y se acelera adicionalmente. El parámetro adicional de la longitud máxima conocida m de palabras de datos del campo finito binario, que se requiere para conocer de forma inequívoca el polinomio irreducible, se puede almacenar junto con los parámetros (s1, s2, s3), aunque esto no es necesario porque también está presente en otro lugar.

Un tercer aspecto de la presente invención se refiere a un procedimiento criptográfico asimétrico utilizable en un dispositivo criptográfico electrónico. El procedimiento incluye una reducción de una primera palabra de datos, que corresponde a un polinomio C(x) y que presenta una longitud máxima de 2n-1, a una segunda palabra de datos con una longitud máxima igual a m, que corresponde a un polinomio C"0(x) equivalente a C(x) en un campo finito binario $GF(2^m)$ cuyos elementos tienen una longitud máxima igual a m, siendo m menor o igual que n, de acuerdo con un procedimiento según el primer o el segundo aspecto de la invención, o de acuerdo con una de las formas de realización del procedimiento según el primer o el segundo aspecto de la invención descritas en el marco de esta solicitud.

En este contexto, por el concepto “procedimiento criptográfico” se entiende un procedimiento para codificar o descodificar un mensaje representado en particular en forma de una palabra de datos. Por el concepto “mensaje” se entiende también por ejemplo una parte de una corriente de datos, que adopta la forma de una palabra de datos.

Una forma de realización del procedimiento criptográfico del tercer aspecto de la invención constituye un procedimiento de criptografía de curva elíptica que incluye, antes de la reducción, la multiplicación de dos palabras de datos factor correspondientes a polinomios factor A(x) y B(x) para obtener la primera palabra de datos que corresponde a un polinomio C(x) y que presenta una longitud máxima de 2n-1.

Un cuarto aspecto de la invención se refiere a un procedimiento para calcular una firma digital. El procedimiento incluye un procedimiento de criptografía de curva elíptica con un procedimiento de reducción según el primer o el segundo aspecto de la invención, o de acuerdo con una de las formas de realización del procedimiento según el primer o el segundo aspecto de la invención descritas en el marco de esta solicitud.

Un quinto aspecto de la invención se refiere a un dispositivo para reducir una primera palabra de datos, que corresponde a un polinomio C(x) y que presenta una longitud máxima de 2n-1, a una segunda palabra de datos con una longitud máxima igual a m, que corresponde a un polinomio C"0(x) equivalente a C(x) en un campo finito binario $GF(2^m)$ cuyos elementos tienen una longitud máxima igual a m, siendo m menor o igual que n, que incluye:

- una memoria que contiene una representación de al menos un polinomio de reducción R(x) consistente en un trinomio o un pentanomio;

- una unidad de selección configurada para tomar una subpalabra de datos binaria de la primera palabra de datos, cuyo polinomio correspondiente C1(x) satisface la ecuación $C(x)=C1(x)*x^m+C0(x)$ y que constituye un primer término de sumandos;

- una unidad de desplazamiento que está conectada con la unidad de selección y configurada para desplazar la subpalabra de datos a la derecha con una anchura de paso predeterminada en cada caso con el fin formar un segundo término de sumandos o términos de sumandos adicionales, y para emitir los términos de sumandos formados;

- una unidad de adición que está conectada con la unidad de desplazamiento y configurada para añadir a la primera palabra de datos un término de sumandos correspondiente y también los sumandos emitidos por la unidad de desplazamiento; y

- una unidad de control configurada para

  - determinar la anchura de paso de un desplazamiento a la derecha correspondiente a realizar por la unidad de desplazamiento con el fin de formar un término de sumandos como la diferencia entre m y el orden de un término correspondiente que no desaparece del polinomio de reducción;

  - dar instrucciones a la unidad de desplazamiento para que repita la realización del paso de desplazamiento a la derecha con el fin de formar otros términos de sumandos con una anchura de paso determinada de nuevo en cada caso, hasta que cada término que no desaparezca de un polinomio de reducción predeterminado en cada caso, y que no sea el término x^m, tenga asignado un término de sumandos;

  - en caso necesario, activar de nuevo la unidad de cálculo, la unidad de desplazamiento y la unidad de adición, hasta que una palabra de datos de suma determinada presente una longitud máxima igual a m y, en consecuencia, constituya la segunda palabra de datos.

El dispositivo de reducción según la invención, que también se designa como dispositivo reductor con el mismo significado, posibilita una reducción rápida de palabras de datos. Además satisface las condiciones para ofrecer una gran flexibilidad que posibilita la reducción de palabras de datos con longitudes diferentes en ejemplos de realización preferentes.

En comparación con dispositivos conocidos, esto se logra con una estructura especialmente sencilla que no requiere ningún tipo de unidad de multiplicación decidida. Mediante el control correspondiente de la unidad de desplazamiento flexible, que desplaza a la derecha una subpalabra de datos seleccionada con una anchura de paso predeterminada en cada caso, en cooperación con una unidad de adición se puede realizar una reducción multiplicativa a través de únicamente unas pocas operaciones sencillas de desplazamiento y adición. El hecho de que la unidad de control esté configurada para activar de nuevo en caso necesario la unidad de cálculo, la unidad de desplazamiento y la unidad de adición hasta que una palabra de datos de suma determinada tenga una longitud máxima igual a m, y en consecuencia constituya la segunda palabra de datos, no implica necesariamente un paso de comprobación en el que se determine la longitud de una palabra de datos parcialmente reducida. Más bien, en una implementación preferente no se lleva a cabo ningún control de la longitud. En este contexto se aprovecha la circunstancia de que un polinomio de reducción adecuadamente elegido asegura que la reducción está completa después de 2 iteraciones.

A continuación se describen ejemplos de realización del dispositivo según la invención. Éstos se pueden combinar entre sí siempre que no se describan expresamente como ejemplos de realización alternativos.

En un ejemplo de realización preferente del dispositivo reductor, la unidad de control está configurada para, en caso de una repetición de los pasos de procedimiento a partir del paso consistente en la determinación de una subpalabra de datos binaria, dar instrucciones a la unidad de adición para que sume los términos de sumandos formados en cada caso, a excepción del primer término de sumandos, a la primera palabra de datos correspondiente, y para que, después

de comprobar que una palabra de datos de suma determinada tiene una longitud no mayor que m, sume cada primer término de sumandos determinado entre tanto a la palabra de datos de suma determinada con el fin de formar la segunda palabra de datos.

Este ejemplo de realización aplica el procedimiento del segundo aspecto de la invención.

Otro ejemplo de realización preferente incluye una primera y una segunda unidad de justificación. La primera unidad de justificación está configurada para desplazar a la izquierda una distancia correspondiente a una anchura de paso de relleno una primera palabra de datos entrante, que presenta una longitud menor que 2n-1, antes de la operación de desplazamiento a la derecha, y añadir a la primera palabra de datos, a ambos lados de la misma, una cantidad de ceros correspondiente a la anchura de paso de relleno, de tal modo que la longitud de la primera palabra de datos así modificada es igual a 2n-1 y que, en la primera palabra de datos modificada, aquellos términos del polinomio C(x) correspondiente a la primera palabra de datos que tienen un orden mayor que m están dispuestos en las mismas posiciones de bit que ocuparían si la primera palabra de datos ya hubiera tenido desde un principio la longitud 2n-1.

La segunda unidad de justificación está configurada para desplazar a la derecha en la anchura de paso de relleno la palabra de datos de suma determinada con una longitud máxima igual a m, y retirar los ceros añadidos al principio.

Para acelerar la reducción, la unidad de desplazamiento incluye preferentemente una cantidad de dispositivos de desplazamiento a la derecha conectados en paralelo, a los que se lleva la subpalabra de datos.

Alternativamente, la unidad de desplazamiento incluye exactamente un dispositivo de desplazamiento a la derecha y la unidad de control está configurada para llevar a cabo la repetición del paso de desplazamiento a la derecha para formar otros términos de sumandos mediante un desplazamiento adicional a la derecha del término de sumandos indicado en último lugar por el dispositivo de desplazamiento a la derecha con una anchura de paso de diferencia correspondiente, consistiendo la anchura de paso de diferencia correspondiente en la diferencia entre los desplazamientos a la derecha de términos de sumandos sucesivos en cada caso con respecto al primer término de sumandos.

Un sexto aspecto de la invención constituye un dispositivo criptográfico, en particular un dispositivo criptográfico electrónico, que incluye un dispositivo de reducción de acuerdo con el quinto aspecto de la invención o un ejemplo de realización de este dispositivo de reducción descrito en el marco de esta solicitud.

En una forma de realización, el dispositivo criptográfico está configurado para la codificación o descodificación de datos de acuerdo con un procedimiento de criptografía de curva elíptica. Evidentemente, esto significa que el dispositivo criptográfico está configurado sólo para la codificación, sólo para la descodificación, o tanto para la codificación como para la descodificación de datos.

En otra forma de realización, el dispositivo criptográfico electrónico incluye una unidad de multiplicación configurada para multiplicar dos palabras de datos factor correspondientes a polinomios factor A(x) y B(x) para obtener una primera palabra de datos que corresponde a un polinomio C(x) y que presenta una longitud máxima de 2n-1. La unidad de multiplicación puede estar integrada junto con el dispositivo de reducción en un mismo chip. No obstante, también puede estar prevista en un chip independiente.

A continuación se explican más detalladamente la invención y diferentes ejemplos de realización con referencia a las figuras adjuntas.

- La Figura 1 muestra un diagrama que ilustra una reducción de polinomios simple.

- Las Figuras 2a) y 2b) muestran dos formas de realización alternativas del procedimiento según la invención.

- La Figura 3 muestra otro ejemplo de realización alternativo del procedimiento según la invención.

- La Figura 4 muestra un diagrama de bloques de un ejemplo de realización de un reductor flexible.

- La Figura 5 muestra un diagrama de bloques que ilustra una estructura alternativa de una unidad de reducción para el reductor flexible de la Figura 4.

La Figura 1 muestra un diagrama que ilustra una reducción de polinomios simple. El problema básico de la reducción de polinomios en campos binarios finitos consiste en que una multiplicación de polinomios produce una primera palabra de datos que tiene una longitud mayor que la longitud máxima m del campo. En lugar de longitud de campo también se habla de grado de campo. Para adaptar el producto de los polinomios al campo finito binario, es necesario reducirlo. El proceso de reducción corresponde a la determinación de una palabra de datos equivalente a la palabra de datos inicial en el campo finito binario $GF(2^m)$. La operación corresponde a la ya conocida operación módulo en campos primos.

Por consiguiente, un planteamiento de reducción obvio consiste en dividir la primera palabra de datos inicial por el polinomio irreducible. El resto de esta división es la palabra de datos reducida, que aquí también se designa como segunda palabra de datos.

Un método de reducción alternativo consiste en la reducción multiplicativa. En este procedimiento, la parte sobresaliente de la palabra de datos, que aquí también se designa como segunda subpalabra de datos, se multiplica por el polinomio de reducción y se resta de la primera palabra de datos inicial. Como es sabido, la sustracción corresponde a un enlace XOR, al igual que la adición.

La longitud máxima del campo finito binario utilizado en el ejemplo representado en la Figura 1 es m=3. Después de un primer paso de iteración se forma una palabra de datos de sumandos C'(x), que se puede representar a su vez como $C'(x)=C1'(x)*x^m+C0'(x)$. Por tanto, la segunda subpalabra de datos C1' que constituye la parte sobresaliente se ha podido reducir con respecto a la primera palabra de datos inicial. No obstante se requiere otra reducción, que se realiza multiplicando la segunda subpalabra de datos C1'(x) por el polinomio de reducción R. Como se puede observar en la parte izquierda del diagrama de la Figura 1, después de estos dos pasos de reducción la primera palabra de datos inicial 110111 se ha reducido mediante multiplicación doble de la segunda subpalabra de datos sobresaliente en cada caso por el polinomio irreducible 1011, para obtener la palabra de datos equivalente 110 en el campo $GF(2^3)$.

Se ha de recalcar que el ejemplo de la Figura 1 sólo sirve para ilustrar el principio. El ejemplo numérico utilizado sólo se ha elegido para la explicación y en este sentido no es característico de los casos de aplicación, ya que la longitud de la primera palabra de datos es igual a 6. Esto corresponde a 2*m, mientras que después de una multiplicación la longitud de la palabra de datos a reducir no es mayor que 2*m-1.

Las Figuras 2a) y 2b) muestran dos formas de realización alternativas del procedimiento según la invención. La solución representada en las Figuras 2a) y 2b) se basa en las propiedades de los campos binarios finitos, recomendados p. ej. por el NIST para la criptografía de curva elíptica. Dado que todos los polinomios de reducción recomendados adicionalmente son trinomios o pentanomios, una multiplicación se puede sustituir por 3 o 5 operaciones de desplazamiento sumadas. Además, como la segunda posición ocupada más alta en los polinomios de reducción es por regla general menor que m/2, la reducción completa se puede concluir después de dos multiplicaciones sucesivas. En las Figuras 2a) y 2b) se ilustra el proceso de reducción correspondiente con referencia a dos casos.

La Figura 2a) muestra el procedimiento según la invención en un caso en el que la longitud del campo admisible en el hardware corresponde exactamente a la longitud del campo (m=n) en el que se ha realizado previamente una multiplicación de polinomios. Una primera palabra de datos no reducida 300, que presenta una longitud de 2n-1, se puede dividir en dos subpalabras de datos 302 y 304. Una primera subpalabra de datos C0 abarca desde la posición de bit más baja hasta la longitud m del campo finito binario $GF(2^m)$. Una segunda subpalabra de datos C1 304 corresponde a la parte sobresaliente de la primera palabra de datos 300 y tiene una longitud de 2n-m-1.

La partición arriba mencionada de la primera palabra de datos 300 en las dos subpalabras de datos 302 y 304 no requiere ningún paso de descomposición real. Basta con tomar por separado los bits de las subpalabras correspondientes de sus respectivas posiciones para los pasos de cálculo subsiguientes.

A continuación, la segunda subpalabra de datos 304 se desplaza a la derecha en distintas copias con diferentes anchuras de paso. Esto está simbolizado esquemáticamente en la Figura 2a) mediante las cinco copias 306 a 314 de la segunda subpalabra de datos 304. Cada copia está desplazada a la derecha con una anchura de paso predeterminada para ella y basada en el polinomio de reducción utilizado. La cantidad de términos de sumandos realmente desplazados 308 a 314 corresponde a la cantidad de los términos que no desaparecen del polinomio de reducción R(x) previamente conocido y que no constituyen el término x^m. En cambio, la copia 306 no ha de ser desplazada. La anchura de paso de cada desplazamiento a la derecha es igual a la diferencia entre m y el orden de cada término que no desaparece del polinomio de reducción.

El orden de un término x^{74}, tomado como ejemplo, de un polinomio de reducción R(x) es 74. En el campo $GF(2^{233})$ se genera para este término un término de sumandos a partir de la segunda subpalabra 304, que está desplazada 159 posiciones a la derecha. Los parámetros s0 a s3 indicados en la Figura 2 representan la anchura de paso respectiva de un desplazamiento a la derecha correspondiente.

Mediante la adición subsiguiente de los términos de sumandos formados 306 a 314 a la primera subpalabra de datos 302 (C0) se obtiene un resultado intermedio $C'(x)= C'0(x) + C'1(x)$, que está representado en forma del bloque 320 e incluye dos subpalabras de datos 322 y 324 correspondientes. Una zona 324.1, identificada con un sombreado, sólo contiene ceros debido a los pasos de procedimiento realizados hasta el momento.

Sin embargo, dado que la palabra de datos de suma 320 así formada todavía no está reducida por completo, se repiten los pasos consistentes en tomar la segunda subpalabra de datos 324 y desplazar a la derecha la segunda subpalabra de datos 324 correspondientemente a los parámetros s0 a s3 del polinomio irreducible R, tal como se explica más arriba. La Figura 2a) muestra copias correspondientes 326 a 334 de la segunda subpalabra de datos 324 desplazadas a la derecha.

Evidentemente, en lugar del desplazamiento de copias en paralelo también se pueden realizar pasos de desplazamiento en serie en una misma subpalabra de datos. Sin embargo, es más rápida la generación en paralelo de las copias desplazadas a la derecha con diferentes dispositivos de desplazamiento a la derecha conectados en paralelo.

Dado que el término con el segundo orden fijado más alto en el polinomio de reducción es menor que la mitad del grado máximo m, para lograr una reducción completa sólo se requieren dos pasos de iteración sucesivos.

En consecuencia, la palabra de datos de suma 336 formada después de llevar a cabo la adición de los términos de sumandos 326 a 334 a la primera subpalabra de datos 322 sólo tiene una longitud máxima m y constituye la segunda palabra de datos reducida buscada.

La Figura 2b) muestra un procedimiento correspondiente al procedimiento de la Figura 2a), en el que la longitud de campo máxima de las palabras de datos entrantes es menor que la longitud de palabra de datos admisible n del reductor según la invención.

Además de los pasos de procedimiento representados en la Figura 1, al principio se lleva a cabo un primer paso de justificación con el que se logra que la longitud de la primera palabra de datos así modificada sea igual a la longitud 2n-1 soportada por el hardware y que, en la primera palabra de datos 350 así modificada, aquellos términos del polinomio C(x) correspondiente a la primera palabra de datos que tienen un orden mayor que m estén dispuestos en las mismas posiciones de bit que ocuparían si la primera palabra de datos 350 ya hubiera tenido desde un principio la longitud 2n-1. Como resultado de ello, del desplazamiento a la izquierda realizado en el primer paso de justificación corresponde a un desplazamiento en una distancia (n-m), siendo n igual a la longitud máxima de una palabra de datos soportada por el hardware. Por tanto, la longitud de palabra soportada en la entrada del reductor es igual a 2n-1.

La anchura de paso de este desplazamiento a la izquierda en el primer paso de justificación se denomina también anchura de paso de relleno, porque las posiciones de bit en los campos 352.1 y 354.1 producidas por dicho desplazamiento en el borde de las subpalabras de datos 352 y 354 se rellenan con ceros.

Con esta primera palabra de datos 350 así modificada se lleva a cabo a continuación el procedimiento de reducción tal como se describe en la Figura 2a). En un primer paso de iteración se forman términos de sumandos 356 y 364 y se suman a la primera subpalabra de datos 352. La palabra de datos de suma 370 así obtenida incluye en su segunda subpalabra de datos sobresaliente 374 un bloque 374.1 que consiste íntegramente en ceros. Las posiciones de bit restantes que no desaparecen de la segunda subpalabra de datos sobresaliente 374 se eliminan en un segundo paso de iteración mediante la formación de los términos de sumandos 376 a 384 y su adición a la primera subpalabra de datos 372, con lo que se obtiene una palabra de datos de suma 386. En un segundo paso de justificación, ésta se desplaza a la derecha la misma cantidad de posiciones de bit, es decir, una distancia correspondiente a la anchura de paso de relleno, para eliminar el bloque derecho 386.1 formado inicialmente mediante la adición de ceros. El bloque restante 386.2 corresponde a la segunda palabra de datos buscada, que es equivalente a la primera palabra de datos.

La Figura 3 muestra un flujo de procedimiento alternativo para el caso m<n, que también ha servido como base para el procedimiento mostrado en la Figura 2b). La representación de la Figura 3 está dividida en cuatro bloques de procedimiento principales S400, S410, S420 y S430.

El bloque de procedimiento S400 incluye un primer paso de justificación S402 en el que una palabra de datos entrante 450, cuya longitud 2m-1 es menor que la longitud 2n-1 soportada por el hardware, se desplaza a la izquierda una distancia correspondiente a una anchura de paso de relleno sf. La palabra de datos 450' así modificada incluye una primera subpalabra de datos 452 y una segunda subpalabra de datos 454. Igual que anteriormente, éstas también están identificadas con C0 y C1 en la Figura 4. Esta designación incluye también los bloques 452.1 y 454.1 situados a la izquierda y la derecha, que están rellenados con ceros.

La segunda palabra de datos 454 se desplaza después a la derecha en tres pasos de desplazamiento a la derecha realizados en paralelo con las anchuras de paso S1, S2 y S3 en los pasos correspondientes S412, S414 y S416. A continuación, los términos de sumando así formados se suman a la primera subpalabra de datos 452 en un paso de adición S418.

Se ha de tener en cuenta que en el procedimiento de la Figura 2 los términos de sumandos se han añadido a C (300). En el procedimiento de la Figura 2 ya sólo se añaden a C0 (452). Así (recurriendo a los símbolos de referencia utilizados) en el presente ejemplo de realización se elimina la operación (304) + (306), cuyo resultado siempre es cero. Por tanto, en el presente procedimiento sólo se añaden en total cuatro términos a la primera subpalabra de datos.

Después de la reducción parcial, la palabra de datos de suma 470 disponible en la salida del paso de adición 418 se somete en el siguiente paso de iteración S420 a una sucesión de pasos correspondiente S422 a S428, tal como se ha descrito detalladamente en relación con la Figura 2b).

En un segundo paso de justificación subsiguiente, la palabra de datos de suma 486 disponible en la salida del paso de adición S428 se desplaza a la derecha una distancia correspondiente a la anchura de paso de relleno sf, con lo que se forma una palabra de datos de suma 488 correspondientemente modificada. A ésta se le añaden las segundas subpalabras de datos 454 y 474 en otro paso de adición S434, con lo que en la salida del paso de adición 434 se obtiene la segunda palabra de datos reducida 490 buscada.

La ventaja de este procedimiento consiste en que en cada paso de iteración se evita un paso de desplazamiento a la derecha. Esto significa que en una implementación de hardware correspondiente se requiere un dispositivo de desplazamiento a la derecha menos, lo que conduce por un lado a una aceleración adicional del procedimiento y, por otro, a un ahorro de espacio.

La Figura 4 muestra un diagrama de bloques de un reductor configurado para la implementación del procedimiento correspondiente a las Figuras 2a) y 2b). El reductor 500 está posconectado a un multiplicador M en cuya salida hay palabras de datos con una longitud de 2m-1. Una de estas palabras de datos, que consiste en el producto de una multiplicación realizada en el multiplicador M, se lleva a una primera unidad de justificación 502, que realiza un desplazamiento a la izquierda correspondientemente al paso S402 de la Figura 3. La primera unidad de justificación 502 se activa mediante una unidad de control 504, que predetermina el parámetro m, es decir, el tamaño de campo de las palabras de datos. A partir de este parámetro, la primera unidad de justificación calcula una anchura de paso de relleno, tal como se describe más arriba. Después de desplazar a la izquierda la primera palabra de datos inicialmente presente una distancia correspondiente a la anchura de paso de relleno, la unidad de justificación rellena los bordes izquierdo y derecho con ceros, de modo que en la salida de la primera unidad de justificación 502 se obtiene una palabra de datos con la longitud de palabra 2n-1 soportada por el reductor 500. En la primera palabra de datos así modificada, aquellos términos del polinomio C(x) correspondiente a la primera palabra de datos original que tienen un orden mayor que m estén dispuestos en las mismas posiciones de bit que ocuparían si la primera palabra de datos original ya hubiera tenido desde un principio la longitud 2n-1.

La primera unidad de justificación 502 tiene posconectada una unidad de reducción 506, cuyo funcionamiento también se controla mediante la unidad de control 504. Ésta proporciona a la unidad de reducción en particular los parámetros S0 a S3 necesarios para los desplazamientos a la derecha descritos detalladamente en relación con las Figuras 2a) y 2b) y la Figura 3. La estructura más detallada de la unidad de reducción se describe mediante ejemplos de realización alternativos con referencia a las Figs. 6 y 7.

La unidad de reducción 506 tiene posconectada una segunda unidad de justificación 508. Ésta lleva a cabo una transformación inversa de la palabra de datos de suma presente en la salida del reductor mediante un desplazamiento a la derecha y una eliminación de los ceros introducidos inicialmente en la primera unidad de justificación. En la salida de la segunda unidad de justificación 508 se obtiene entonces la segunda palabra de datos reducida buscada.

La Figura 5 muestra una implementación alternativa de la unidad de reducción, que funciona únicamente con un dispositivo de desplazamiento a la derecha 702 que genera en serie copias de la segunda subpalabra de datos con diferentes distancias de desplazamiento, que se suman a la primera subpalabra de datos correspondiente.

En consecuencia, la unidad de reducción 706 de la Figura 5 requiere muchos ciclos para un paso de reducción, suponiéndose que los desplazamientos a la derecha se realizan en el orden $S3 \leq S2 \leq S1 \leq S0$, de modo que se llevan a cabo desplazamientos sucesivos a la derecha.

REIVINDICACIONES

1. Procedimiento utilizable en un procedimiento criptográfico en un dispositivo electrónico para reducir una primera palabra de datos binaria, que corresponde a un polinomio C(x) y que presenta una longitud máxima de 2n-1, a una segunda palabra de datos con una longitud máxima igual a m, que corresponde a un polinomio C"0(x) equivalente a C(x) en un campo finito binario $GF(2^m)$ cuyos elementos tienen una longitud máxima igual a m, siendo m menor o igual que n, que incluye los siguientes pasos:

- preparación de un polinomio de reducción R(x) consistente en un trinomio o un pentanomio;

- partición de la primera palabra de datos en una primera subpalabra de datos binaria C0 y una segunda subpalabra de datos binaria C1 cuyos polinomios correspondientes, C0(x) y C1(x), satisfacen la ecuación $C(x)=C1(x)*x^m+C0(x)$, y toma de la segunda subpalabra de datos para formar un primer término de sumandos;

- desplazamiento a la derecha de la segunda subpalabra de datos para formar un segundo término de sumandos, y repetición del paso de desplazamiento a la derecha para formar otros términos de sumandos hasta que cada término que no desaparezca del polinomio de reducción, que no sea el término x^m, tenga asignado un término de sumandos, siendo la anchura de paso de cada desplazamiento a la derecha igual a la diferencia entre m y el orden de un término correspondiente que no desaparece del polinomio de reducción;

- adición de los términos de sumandos formados a la primera subpalabra de datos para formar una palabra de datos de suma;

- si la palabra de datos de suma así determinada tiene una longitud mayor que m, aplicación de los pasos de procedimiento a partir del paso de partición a la palabra de datos de sumandos formada, hasta que la palabra de datos de suma así determinada tenga una longitud máxima igual a m y por consiguiente constituya la segunda palabra de datos.

2. Procedimiento utilizable en un procedimiento criptográfico en un dispositivo electrónico para reducir una primera palabra de datos, que corresponde a un polinomio C(x) y que presenta una longitud máxima de 2n-1, a una segunda palabra de datos con una longitud máxima igual a m, que corresponde a un polinomio C"0(x) equivalente a C(x) en un campo finito binario $GF(2^m)$ cuyos elementos tienen una longitud máxima igual a m, siendo m menor o igual que n, que incluye los siguientes pasos:

- preparación de un polinomio de reducción R(x) consistente en un trinomio o un pentanomio;

- partición de la primera palabra de datos en una primera subpalabra de datos binaria C0 y una segunda subpalabra de datos binaria C1 cuyos polinomios correspondientes, C0(x) y C1(x), satisfacen la ecuación $C(x)=C1(x)*x^m+C0(x)$, y toma de la segunda subpalabra de datos para formar un primer término de sumandos;

- desplazamiento a la derecha de la segunda subpalabra de datos para formar un segundo término de sumandos, y repetición del paso de desplazamiento a la derecha para formar otros términos de sumandos hasta que cada término que no desaparezca del polinomio de reducción, que no sea el término x^m, tenga asignado un término de sumandos, siendo la anchura de paso de cada desplazamiento a la derecha igual a la diferencia entre m y el orden de un término correspondiente que no desaparece del polinomio de reducción;

- adición de los términos de sumandos formados, a excepción del último término de sumandos asignado al término x^0, a la primera subpalabra de datos;

- si la palabra de datos de suma así determinada tiene una longitud mayor que m, aplicación de los pasos de procedimiento a partir del paso de partición a la palabra de datos de sumandos formada, hasta que la palabra de datos de suma así determinada tenga una longitud máxima igual a m;

- adición del último término de sumandos y, en el caso mencionado de una aplicación de los pasos de procedimiento a partir del paso de partición a la palabra de datos de sumandos formada, de cada último término de sumandos determinado entre tanto, a la palabra de datos de suma determinada en último lugar para formar la segunda palabra de datos.

3. Procedimiento según la reivindicación 1 o 2, en el que la primera palabra de datos tiene una longitud menor que 2n-1, con un primer paso de justificación adicional realizado antes de la operación de desplazamiento a la derecha, que incluye un desplazamiento a la izquierda de la primera palabra de datos con una anchura de paso de relleno y una adición de una cantidad de ceros correspondiente a la anchura de paso de relleno a ambos lados de la primera palabra de datos, de tal modo que la longitud de la primera palabra de datos así modificada es igual a 2n-1 y que, en la primera palabra de datos modificada, aquellos términos del polinomio C(x) correspondiente a la primera palabra de datos que tienen un orden mayor que m están dispuestos en las mismas posiciones de bit que ocuparían si la primera palabra de datos ya hubiera tenido desde un principio la longitud 2n-1.

4. Procedimiento según la reivindicación 3, con un segundo paso de justificación que incluye una eliminación de los ceros añadidos inicialmente a la palabra de datos de suma determinada y un desplazamiento a la derecha de la palabra de datos de suma en una distancia correspondiente a la anchura de paso de relleno.

5. Procedimiento según una de las reivindicaciones 1 a 4, en el que el polinomio irreducible se representa exclusivamente mediante las potencias de los términos que no desaparecen del polinomio de reducción y que no son el término x^m.

6. Procedimiento según la reivindicación 5, en el que el polinomio irreducible se representa adicionalmente mediante la longitud máxima conocida m de las palabras de datos del campo finito binario.

7. Procedimiento criptográfico asimétrico utilizable en un dispositivo criptográfico electrónico, que incluye

- la reducción de una primera palabra de datos, que corresponde a un polinomio C(x) y que presenta una longitud máxima de 2n-1, a una segunda palabra de datos con una longitud máxima igual a m, que corresponde a un polinomio C"0(x) equivalente a C(x) en un campo finito binario GF(2^m) cuyos elementos tienen una longitud máxima igual a m, siendo m menor o igual que n, según una de las reivindicaciones 1-6.

8. Procedimiento criptográfico asimétrico según la reivindicación 7, que constituye un procedimiento de criptografía de curva elíptica, que antes de la reducción incluye

- la multiplicación de dos palabras de datos factor correspondientes a polinomios factor A(x) y B(x) para obtener la primera palabra de datos que corresponde a un polinomio C(x) y que presenta una longitud máxima de 2n-1.

9. Procedimiento para el cálculo de una firma digital, que incluye un procedimiento criptográfico asimétrico según la reivindicación 8.

10. Dispositivo para reducir una primera palabra de datos, que corresponde a un polinomio C(x) y que presenta una longitud máxima de 2n-1, a una segunda palabra de datos con una longitud máxima igual a m, que corresponde a un polinomio C"0(x) equivalente a C(x) en un campo finito binario GF(2^m) cuyos elementos tienen una longitud máxima igual a m, siendo m menor o igual que n, que incluye:

- una memoria que contiene una representación de al menos un polinomio de reducción R(x) consistente en un trinomio o un pentanomio;

- una unidad de selección configurada para tomar una subpalabra de datos binaria de la primera palabra de datos, cuyo polinomio correspondiente C1(x) satisface la ecuación $C(x)= C1(x)*x^m+C0(x)$ y que constituye un primer término de sumandos;

- una unidad de desplazamiento que está conectada con la unidad de selección y configurada para desplazar la subpalabra de datos a la derecha con una anchura de paso predeterminada en cada caso con el fin formar un segundo término de sumandos o términos de sumandos adicionales, y para emitir los términos de sumandos formados;

- una unidad de adición que está conectada con la unidad de desplazamiento y configurada para añadir a la primera palabra de datos un término de sumandos correspondiente y también los sumandos emitidos por la unidad de desplazamiento; y

- una unidad de control configurada para

  determinar la anchura de paso de un desplazamiento a la derecha correspondiente a realizar por la unidad de desplazamiento con el fin de formar un término de sumandos como la diferencia entre m y el orden de un término correspondiente que no desaparece del polinomio de reducción;

  dar instrucciones a la unidad de desplazamiento para que repita la realización del paso de desplazamiento a la derecha con el fin de formar otros términos de sumandos con una anchura de paso determinada de nuevo en cada caso, hasta que cada término que no desaparezca de un polinomio de reducción predeterminado en cada caso, y que no sea el término x^m, tenga asignado un término de sumandos;

  dar instrucciones a la unidad de adición para que añada los términos de sumandos correspondientes a la primera palabra de datos, con el fin de determinar una palabra de datos de suma;

  y, en caso necesario, activar de nuevo la unidad de cálculo, la unidad de desplazamiento y la unidad de adición, hasta que una palabra de datos de suma determinada presente una longitud máxima igual a m y, en consecuencia, constituya la segunda palabra de datos.

11. Dispositivo según la reivindicación 10, en el que la unidad de control está configurada para, en caso de una repetición de los pasos de procedimiento a partir del paso consistente en la determinación de una subpalabra de datos binaria, dar instrucciones a la unidad de adición para que sume los términos de sumandos formados en cada caso, a excepción del primer término de sumandos, a la primera palabra de datos correspondiente,

y para que, después de comprobar que una palabra de datos de suma determinada tiene una longitud no mayor que m, sume cada primer término de sumandos determinado entre tanto a la palabra de datos de suma determinada con el fin de formar la segunda palabra de datos.

12. Dispositivo según la reivindicación 10 u 11, con una primera y una segunda unidad de justificación,

estando configurada la primera unidad de justificación para desplazar a la izquierda una distancia correspondiente a una anchura de paso de relleno una primera palabra de datos entrante, que presenta una longitud menor que 2n-1, antes de la operación de desplazamiento a la derecha, y añadir a la primera palabra de datos, a ambos lados de la misma, una cantidad de ceros correspondiente a la anchura de paso de relleno, de tal modo que la longitud de la primera palabra de datos así modificada es igual a 2n-1 y que, en la primera palabra de datos modificada, aquellos términos del polinomio C(x) correspondiente a la primera palabra de datos que tienen un orden mayor que m están dispuestos en las mismas posiciones de bit que ocuparían si la primera palabra de datos ya hubiera tenido desde un principio la longitud 2n-1; y

estando configurada la segunda unidad de justificación para desplazar a la derecha una distancia correspondiente a la anchura de paso de relleno la palabra de datos de suma determinada con una longitud máxima igual a m, y retirar los ceros añadidos al principio.

13. Dispositivo según una de las reivindicaciones 10 a 12, en el que la unidad de desplazamiento incluye una serie de dispositivos de desplazamiento a la derecha conectados en paralelo, a los que se lleva la subpalabra de datos.

14. Dispositivo según una de las reivindicaciones 10 a 12, en el que la unidad de desplazamiento incluye exactamente un dispositivo de desplazamiento a la derecha y la unidad de control está configurada para llevar a cabo la repetición del paso de desplazamiento a la derecha para formar otros términos de sumandos mediante un desplazamiento adicional a la derecha del término de sumandos indicado en último lugar por el dispositivo de desplazamiento a la derecha con una anchura de paso de diferencia correspondiente, consistiendo la anchura de paso de diferencia correspondiente en la diferencia entre los desplazamientos a la derecha de términos de sumandos sucesivos en cada caso con respecto al primer término de sumandos.

15. Dispositivo criptográfico electrónico que incluye un dispositivo de reducción según una de las reivindicaciones 10 a 14.

16. Dispositivo criptográfico electrónico según la reivindicación 15, que está configurado para la codificación o descodificación de datos de acuerdo con un procedimiento de criptografía de curva elíptica.

17. Dispositivo criptográfico electrónico según la reivindicación 16, con un dispositivo multiplicador configurado para multiplicar dos palabras de datos factor correspondientes a polinomios factor A(x) y B(x) para obtener una primera palabra de datos que corresponde a un polinomio C(x) y que presenta una longitud máxima de 2n-1.

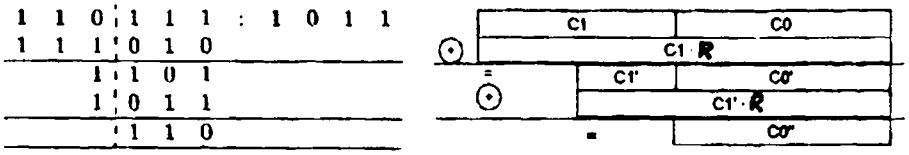

Fig. 1 **ESTADO DE LA TÉCNICA**

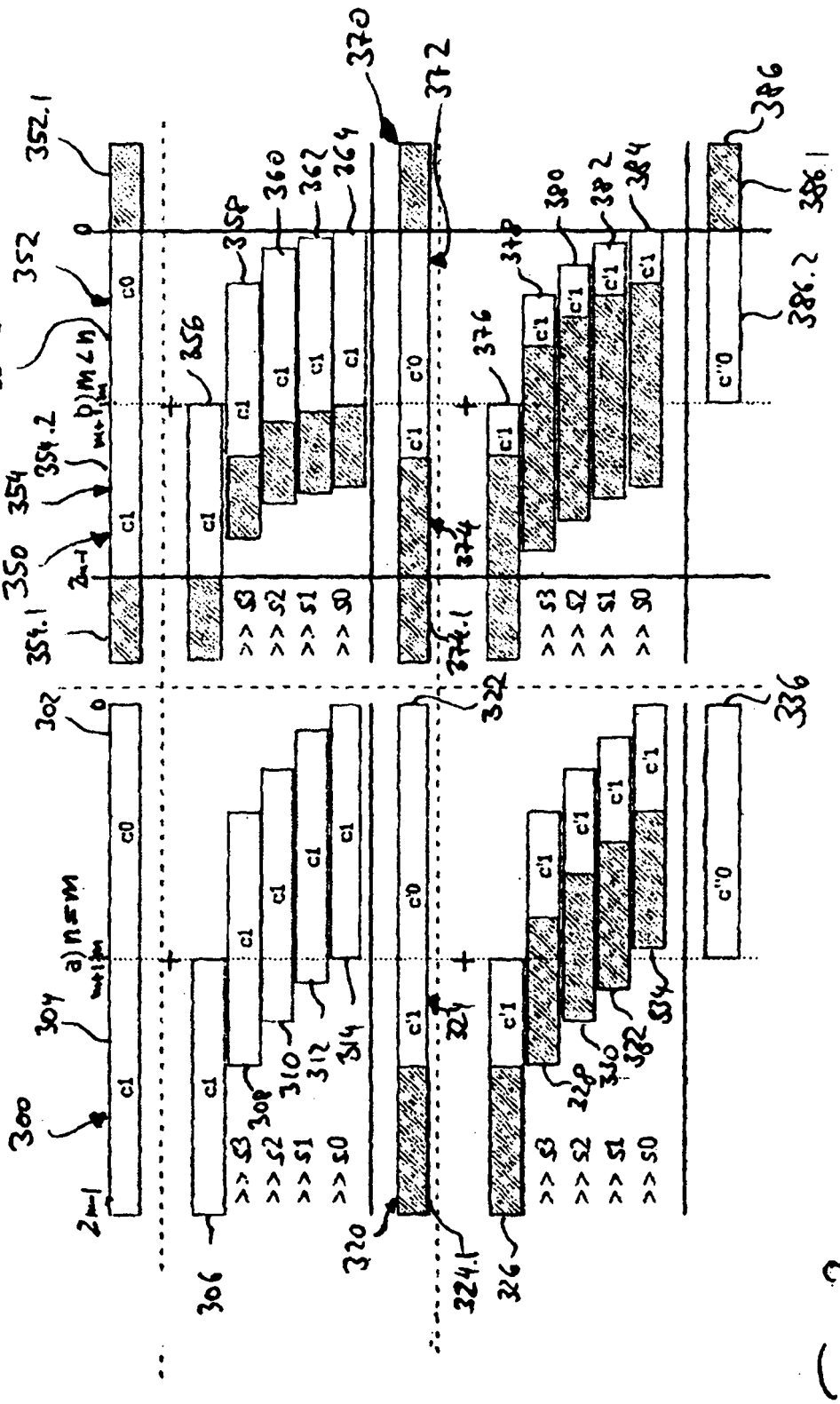

Fig. 2

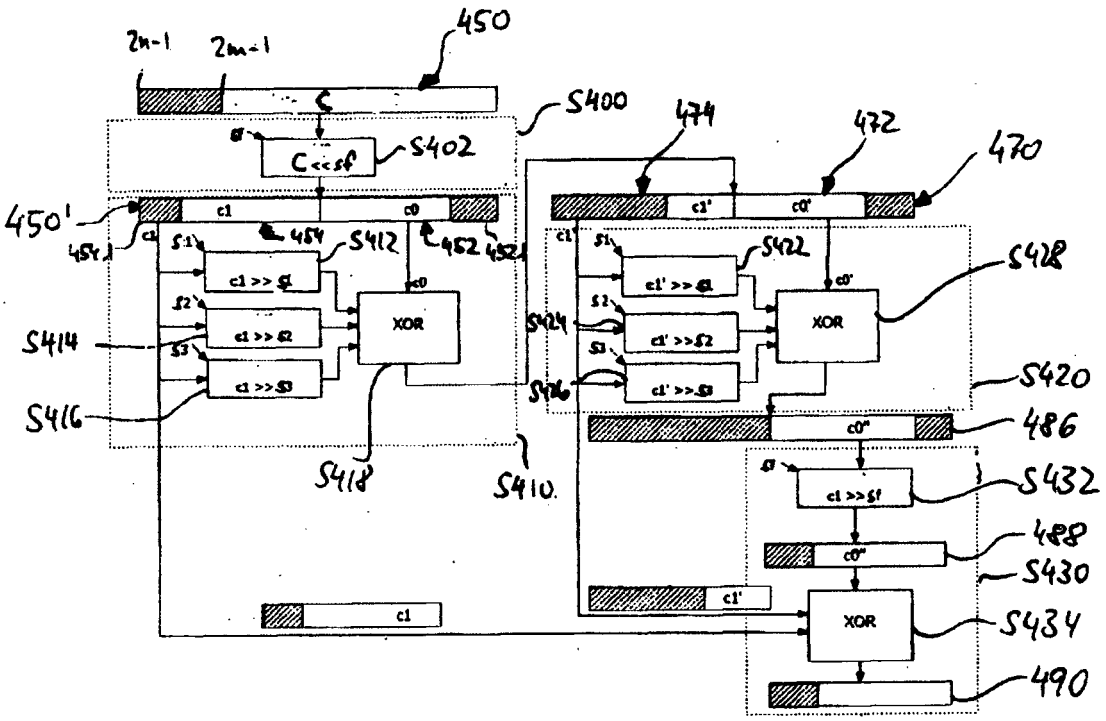
2n-1
2m-1
450
C
S400
C<<sf
S402
450'
c1
c0
454
S412
452
S414
S416
XOR
S418
S410
474
472
470
c1'
c0'
S422
S428
S424
S426
S420
c0"
486
S432
488
S430
S434
490

fig. 3

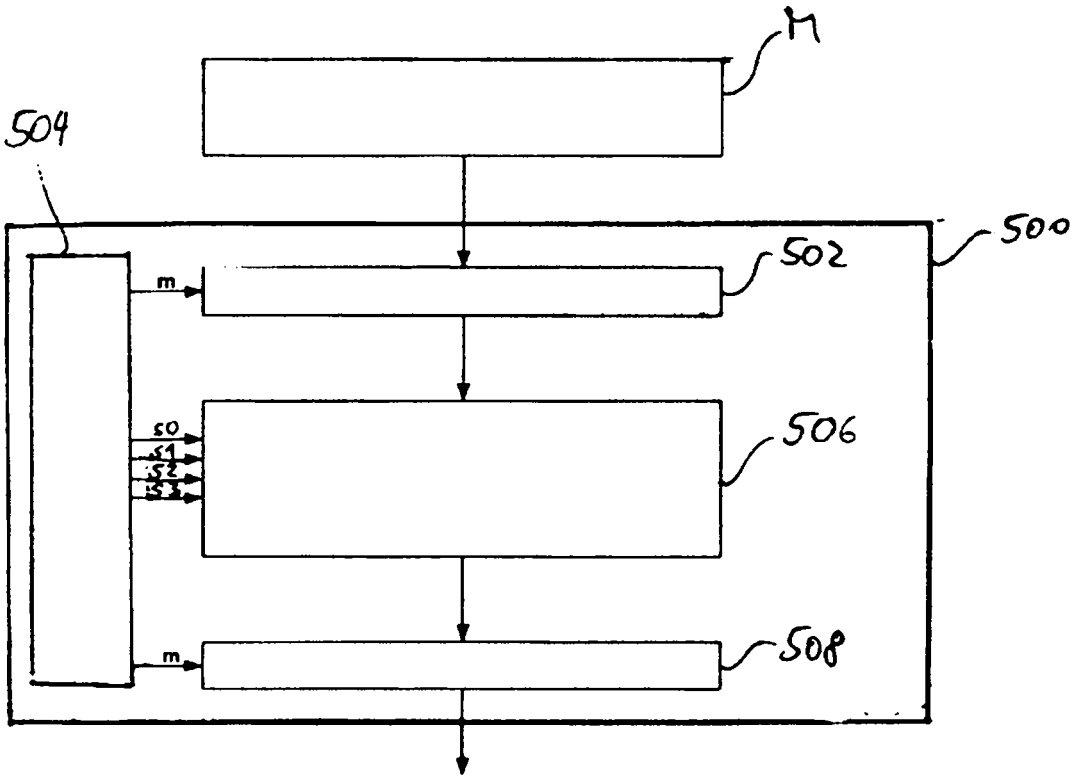

Fig. 4

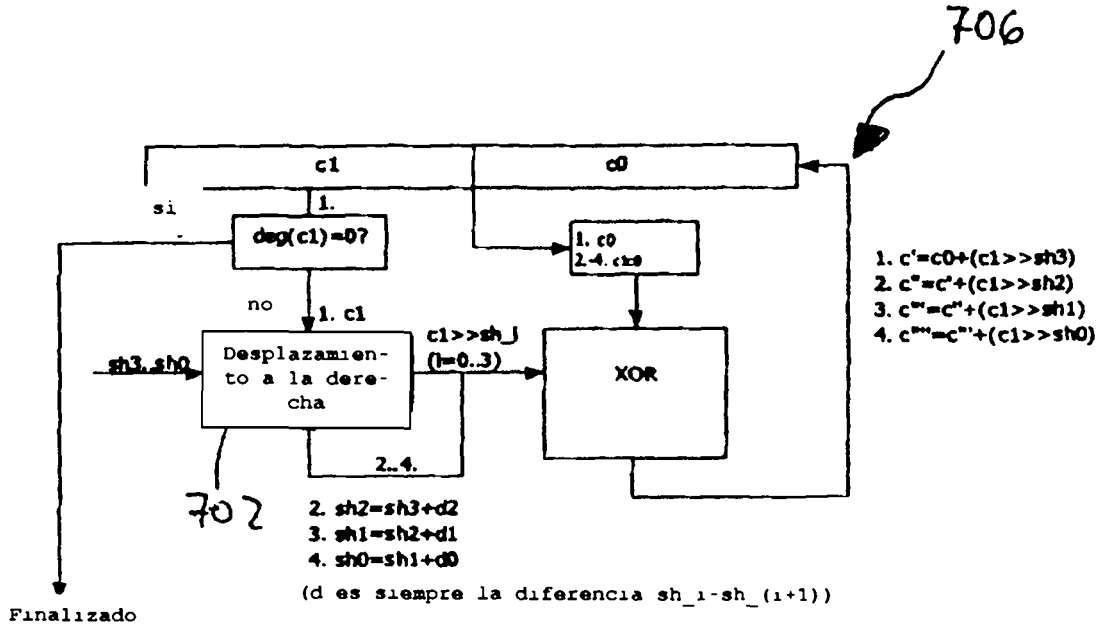
706
c1
c0
si
1.
deg(c1)=0?
1. c0
2-4. c1=0
1. c'=c0+(c1>>sh3)
2. c''=c'+(c1>>sh2)
3. c'''=c''+(c1>>sh1)
4. c''''=c'''+(c1>>sh0)
no
1. c1
sh3..sh0
Desplazamien-
to a la dere-
cha
c1>>sh_i
(i=0..3)
XOR
2..4.
707
2. sh2=sh3+d2
3. sh1=sh2+d1
4. sh0=sh1+d0
(d es siempre la diferencia sh_i-sh_(i+1))
Finalizado

Fig. 5