(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 377 715**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03727434 .7**
(96) Fecha de presentación: **05.05.2003**
(97) Número de publicación de la solicitud: **1504337**
(97) Fecha de publicación de la solicitud: **09.02.2005**

(54) Título: **Cálculo del inverso modular de un valor**

(30) Prioridad:
06.05.2002 DE 10220262

(45) Fecha de publicación de la mención BOPI:
30.03.2012

(45) Fecha de la publicación del folleto de la patente:
30.03.2012

(73) Titular/es:
GIESECKE & DEVRIENT GMBH
PRINZREGENTENSTRASSE 159
81677 MÜNCHEN, DE

(72) Inventor/es:
KAHL, Helmut

(74) Agente/Representante:
Torner Lasalle, Elisabet

DESCRIPCIÓN

Cálculo del inverso modular de un valor.

La invención se refiere en general al campo técnico de los algoritmos ejecutables de manera eficaz mediante un procesador automático y en especial a un algoritmo mejorado para la inversión modular. En particular la invención es adecuada para aplicaciones criptográficas, tal como aparecen, por ejemplo, en relación con tarjetas con circuito integrado.

En el campo de la criptografía se utilizan procedimientos para la inversión modular por ejemplo, en la generación de un par de claves para el procedimiento de firma y de codificación RSA descrito en la patente US 4.405.829. El procedimiento RSA emplea una clave (E, N) pública y una clave R privada secreta, siendo el valor N el producto de dos números P y Q primos grandes. Para el cálculo de pares de claves se fijan en primer lugar los valores P, Q y E. La clave R privada se calcula entonces como el inverso modular del valor E respecto al módulo M con M = (P-1)·(Q-1).

En general para dos números E y M enteros dados el inverso modular del valor E respecto al módulo M está definido como aquel número R, para el que se cumple que $0 \leq R < M$ y $1 = E \cdot R \bmod M$; el resultado R se designa también con 1/E. Un inverso R modular existe, cuando E y M son primos entre sí.

Se conocen como tales algoritmos para el cálculo del inverso modular de un valor E preestablecido respecto a un módulo M preestablecido. Así por ejemplo, se describe el empleo del algoritmo de Euclides ampliado para la inversión modular en las páginas 47 y 67 del libro de J. v. z. Gathen y J. Gerhard, “Modern Computer Algebra”,1ª edición, Cambridge University Press, 1999 (algoritmo 3.6 y teorema 4.1). Un pequeño aumento de la eficiencia en el ejemplo de aplicación del cálculo de pares de claves RSA es posible mediante una transformación según el teorema chino del resto. Una modificación ventajosa del algoritmo de Euclides ampliado en particular en relación con números binarios es el procedimiento de Stein, que se describe en las páginas 321 a 324 del libro de Donald E. Knuth, “The Art of Computer Programming”, tomo 2, 2ª edición, Addison-Wesley, 1981 en relación con el problema 35 de la página 339 y la solución para el mismo en la página 606.

Los procedimientos mencionados para la inversión modular requieren sin embargo relativamente mucho esfuerzo de cálculo. Necesitan un múltiplo del tiempo de cálculo de otras operaciones de cálculo modulares elementales tales como, por ejemplo, de la multiplicación modular (véase la página 304, corolario 11.6 del libro mencionado de Gathen y Gerhard). Esto es especialmente problemático, cuando la inversión modular debe realizarse por un procesador con una capacidad de potencia relativamente reducida, como se produce por ejemplo, en el caso del procesador de una tarjeta con circuito integrado u otro soporte informático portátil.

La invención tiene por tanto el objetivo de proporcionar un procedimiento eficaz en la ejecución a máquina para la inversión modular. El procedimiento debe ser adecuado en particular para su empleo para cálculos criptográficos en un soporte informático portátil.

Según la invención este objetivo se soluciona parcial o totalmente mediante un procedimiento con las características de la reivindicación 1, un producto de programa informático según la reivindicación 9 y un soporte informático portátil según la reivindicación 10. Las reivindicaciones dependientes definen configuraciones preferidas de la invención.

La invención parte de la reflexión básica de que el esfuerzo para el cálculo del inverso modular depende en gran parte de la longitud del módulo. La invención propone por tanto dividir el cálculo total en varios cálculos parciales, basados en cada caso en un módulo más corto. Más concretamente el módulo se descompone según la invención en al menos dos factores. Entonces para el cálculo de un valor auxiliar se recurre a cada uno de estos factores, que es el inverso modular del valor original respecto al factor como módulo. A partir de los valores auxiliares calculados y dado el caso de datos adicionales se determina entonces el resultado total.

La idea básica según la invención es sorprendente, porque en general la factorización de un valor, en este caso del módulo, va unida a esfuerzos prohibitivos. El inventor ha reconocido sin embargo, que en muchas situaciones relevantes de modo práctico ya se conoce una factorización al menos parcial del módulo o los factores pueden calcularse fácilmente a partir de otra información. Este es el caso, por ejemplo, en el cálculo de pares de claves descrito al principio para el procedimiento RSA, en el que los factores P-1 y Q-1 del módulo M están fácilmente a disposición.

La invención ofrece un aumento considerable de la eficiencia, que es mayor, cuanto mayor sea la dependencia del esfuerzo de cálculo de la longitud del módulo en el procedimiento de inversión empleado finalmente. Con ello la invención es especialmente adecuada para su realización mediante procesadores relativamente poco potentes. La seguridad del cálculo frente a ataques de espionaje no se ve perjudicada por la utilización de la invención, en comparación con los procedimientos de inversión habituales. Cuando existen requisitos de seguridad especialmente altos, la invención puede combinarse sin embargo fácilmente con medidas adecuadas para la protección frente al espionaje.

El orden de enumeración de las etapas del procedimiento en las reivindicaciones no debe entenderse como una limitación del alcance de la invención. Están previstas muchas más configuraciones de la invención, en las que estas etapas de procedimiento se ejecutan en otro orden y/o total o parcialmente paralelas y/o total o parcialmente entrelazadas entre sí (*interleaved*). Además la invención no está limitada al tratamiento de número enteros. El procedimiento según la invención puede utilizarse más bien como valores por ejemplo polinomios o en general los elementos de un anillo conmutativo con elemento universal.

Según la invención está previsto determinar una descomposición factorial del módulo. El término “determinar” debe comprender a este respecto también casos, en los que solamente se accede a factores ya conocidos, preestablecidos. Cuando solamente se conocen dos factores, a este respecto no se realiza ningún tipo de selección. Si se conocen más factores, entonces se selecciona preferiblemente el número necesario de factores. A este respecto los factores pueden clasificarse según su longitud o tamaño o agruparse adecuadamente. Por el término “longitud” debe entenderse a este respecto en particular el número de las posiciones del factor en un sistema de notación posicional tal como por ejemplo el sistema binario o decimal.

Los factores no necesitan ser primos. Por los términos “factorización” o “descomposición” no debe entenderse por tanto necesariamente una descomposición de factores primos. En configuraciones preferidas de la invención está previsto más bien tratar también factores compuestos sin división adicional, cuando por ejemplo no se conoce una división tal o si condujera a factores de longitudes muy diferentes. Por motivos de eficacia es deseable, que las longitudes de los factores, a los que solamente se recurre como módulos para la determinación de inversos según un procedimiento conocido, se diferencien lo menos posible (por ejemplo en menos del 20% o en menos del 50% de la mayor longitud).

Dado que en general la factorización de un valor requiere un extraordinario esfuerzo de cálculo, el procedimiento se utiliza preferiblemente sólo cuando se conocen al menos dos factores del módulo o pueden determinarse con poco esfuerzo. Un esfuerzo pequeño en este sentido se considera en particular cuando la descomposición factorial ya no requiere más operaciones de cálculo que la determinación de inversos del valor respecto al más largo de los factores determinados como módulo.

El procedimiento ya puede utilizarse de manera útil con una única división del módulo en dos o tres o más factores. Si se conocen más factores o pueden determinarse fácilmente, así el procedimiento puede ejecutarse repetidamente, siendo posible una programación recursiva o una iterativa. Preferiblemente el módulo M presenta factores primos diferentes o se descompone en al menos una etapa de cálculo en al menos dos factores diferentes.

El producto de programa informático según la invención presenta instrucciones de programa, para implementar el procedimiento según la invención. Un producto de programa informático de este tipo puede ser, por ejemplo, una memoria semiconductora o un disquete o un CD-ROM, en el que está almacenado un programa de cálculo según la invención. En particular está previsto un producto de programa informático de este tipo para su empleo en la producción de tarjetas con circuito integrado.

En configuraciones preferidas el producto de programa informático y/o el soporte informático portátil están perfeccionados con características que se corresponden con las características descritas anteriormente y/o con las mencionadas en las reivindicaciones de procedimiento dependientes.

Otras características, ventajas y objetivos de la invención se deducen de la siguiente descripción detallada de varios ejemplos de realización y alternativas de realización. Se hace referencia a los dibujos esquemáticos, en los que muestran:

la figura 1 una vista de las etapas de cálculo ejecutadas en un ejemplo de realización de la invención,

la figura 2 una representación esquemática de un desarrollo de cálculo con estructura de llamada recursiva, y

la figura 3 una representación esquemática de un desarrollo de cálculo iterativo.

El procedimiento representado esquemáticamente en la figura 1 está previsto para ejecutarse por un procesador de un soporte informático portátil, en particular de una tarjeta con circuito integrado (*smart card*) o de un módulo de circuito integrado. El procedimiento está implementado para ello en forma de instrucciones de programa para este procesador, que se almacenan en una ROM o EEPROM del soporte informático.

Según la invención el procedimiento se emplea para el cálculo de la clave R privada para un procedimiento de codificación RSA o un procedimiento de firma RSA. Para un valor E dado y números P y Q primos dados la clave R privada es el inverso modular del valor E respecto al módulo M con $M = (P-1)\cdot(Q-1)$. Por tanto los factores P-1 y Q-1 del módulo M ya son conocidos. El hecho de que estos mismos factores no sean primos, no perjudica el desarrollo del procedimiento.

En la etapa 10 del procedimiento se determina una descomposición del módulo M en dos factores M1 y M2. Estos dos factores M1 y M2 en el presente ejemplo de realización son simplemente los valores P-1 y Q-1 ya presentes, de modo que no se necesita ni una selección entre varias posibilidades ni etapas de cálculo adicionales.

En las etapas 12 y 14 se llevan a cabo entonces dos cálculos para la determinación del inverso modular del valor M respecto a los módulos M1 o M2, para obtener los valores R1 y R2 auxiliares. Para estos cálculos puede emplearse cualquier procedimiento conocido, tal como por ejemplo el algoritmo de Euclides ampliado mencionado al principio con o sin el empleo del teorema chino del resto. También es posible, en las etapas 12 y 14 llamar recursivamente el procedimiento según la invención, a lo que se hará referencia en detalle más tarde.

Cuando existen los dos valores R1 y R2 auxiliares, se realiza en la etapa 16 el cálculo del resultado R mediante la valoración de la siguiente relación:

$$R = R1 + R2 - R1 \cdot R2 \cdot E \bmod M \qquad (*)$$

Por razonamiento matemático se deduce que el valor R así calculado es de hecho el inverso modular de E respecto al módulo M, por tanto que se cumple R =1/E mod M.

Cuando los factores M1 y M2 presentan aproximadamente el mismo orden de magnitud, esto es, por ejemplo, aproximadamente la misma longitud en su representación binaria, el esfuerzo de cálculo para cada una de las dos etapas 12 y 14 en el procedimiento de inversión habitual asciende sólo aproximadamente a un cuarto del esfuerzo de cálculo para la inversión de E respecto al módulo M. La etapa 10 no requiere ninguna operación de cálculo. El esfuerzo para la etapa 16 se determina esencialmente por las dos multiplicaciones modulares, que se desarrollan notablemente más rápido, por ejemplo, 8 veces más rápido, que una inversión modular. El procedimiento necesita por tanto para las etapas 12, 14 y 16 sólo aproximadamente 1/4 + 1/4 + 2/8 = 3/4 del esfuerzo de una inversión de E respecto al módulo M. Incluso en la configuración más sencilla descrita en este caso del procedimiento, en el caso de que tenga lugar sólo una única división del módulo M en dos factores M1, M2, se obtiene con ello un ahorro de aproximadamente el 25%.

En una modificación del procedimiento de la figura 1 en la etapa 10 no está previsto un desdoblamiento en dos, sino en tres o más factores M1, M2,.... En el cálculo en la etapa 16 se emplea entonces una forma ampliada de la relación (*) para el cálculo de R a partir del correspondiente número de valores R1, R2,... auxiliares.

Como ya se mencionó, el procedimiento en las etapas 12 y/o 14 puede llamarse recursivamente. En todo caso esto es evidentemente útil, cuando se conoce una descomposición factorial adicional de los valores M1 y/o M2 o puede calcularse fácilmente. En caso contrario, se interrumpe la recurrencia para la correspondiente rama de cálculo y se recurre a otro algoritmo en sí conocido para el cálculo del inverso.

Condiciones de interrupción adicionales para la recurrencia pueden ser que para el valor que va a descomponerse existan sólo factores con una longitud notablemente diferente, o que una magnitud mínima preestablecida del valor que va a descomponerse o de sus factores quede por debajo. Cuando por ejemplo, en el cálculo de la clave R privada en la etapa 12 debe calcularse el inverso modular respecto al módulo M1 = P-1 para el número P primo (impar), existe evidentemente una factorización P-1= 2.((P-1)/2) de número enteros. En caso de que no se conozca ningún factor adicional para (P-1)/2, por regla general en este caso no es útil una llamada recursiva con los factores 2 y (P-1)/2.

La estructura de llamada de un cálculo recursivo mostrada en la figura 2 a modo de ejemplo está completamente compensada. El módulo M original se dividió en la primera etapa 10 en dos factores M1 y M2, cada uno de estos factores Mx en una primera fase de recurrencia en los factores Mx1 y Mx2, y cada uno de estos factores Mxy en una segunda fase de recurrencia en los factores Mxy1 y Mxy2. Para los ocho factores Mxyz así obtenidos se calculó como valor auxiliar el inverso Rxyz modular correspondiente del valor E respecto al factor Mxyz. En los retornos de las llamadas recursivas se calcularon a partir de los valores Rxyz auxiliares según la etapa 16 en primer lugar los valores Rxy auxiliares, entonces los valores Rx auxiliares y finalmente el resultado R.

Para un cálculo compensado como el mostrado en la figura 2, en el que la recurrencia se lleva a cabo con un nivel de anidamiento n homogéneo hasta la existencia de $k = 2^n$ factores, el esfuerzo asciende a sólo a O(m(k)) operaciones básicas, indicando m(k) el esfuerzo para la multiplicación modular de dos números de la longitud k. Esta estimación parte de la base de que todos los 2^n factores existentes en último término presentan aproximadamente la misma longitud. Esto es una mejora notable en comparación con los procedimientos habituales, que requieren un esfuerzo en el orden de magnitud de O(m(k)·log(m(k))) operaciones básicas (véase por ejemplo el corolario 11.10, página 305 del ya citado libro de Gathen y Gerhard).

En muchas aplicaciones prácticas no podrá alcanzarse un desarrollo completamente compensado tal como en la figura 2. La figura 3 muestra el caso extremo de un desarrollo de cálculo completamente descompensado, que parte de que el módulo M = M1·M2·M3·M4·M5. Un cálculo de este tipo corresponde a una implementación iterativa del procedimiento por ejemplo por medio de un bucle de programa. El bucle parte de un par de valores R1, R2 auxiliares y a continuación

aplica la relación (*). En cada ejecución de bucle se añade mediante una aplicación adicional de la relación (*) un valor R3, R4,... auxiliar adicional, hasta que finalmente se calcula el inverso R. Además en cada ejecución de bucle el en cada caso valor R1, R2,... auxiliar necesario nuevo puede calcularse a partir del correspondiente factor M1, M2,.... Como alternativa es posible determinar todos los valores R1, R2,... auxiliares de antemano en un bucle separado a partir de los factores M1, M2,....

En general el procedimiento según la invención, ya sea en una implementación recursiva o iterativa, puede servir para la determinación del inverso de un valor E respecto a un módulo M, que se encuentra en una factorización no necesariamente completa con muchos factores M1, M2,... cualesquiera. Para ello se aplica la relación (*) en cada caso a un par de valores R1, R2,... auxiliares, que se han determinado a partir de los factores M1, M2,.... El esfuerzo de cálculo necesario es entonces especialmente pequeño, cuando los factores M1, M2,... presentan aproximadamente longitudes homogéneas. Para garantizar en una etapa de preparación o durante el cálculo pueden agruparse en cada caso dos o más factores Mx, My,.... Entran entonces como valor Mx·My.... en el cálculo, que no se descompone adicionalmente, aunque su factorización fuera conocida.

REIVINDICACIONES

1. Procedimiento implementado por ordenador para la determinación de pares de claves en un procedimiento de firma o de codificación RSA mediante el cálculo del inverso (R) modular de un valor (E) respecto a un módulo (M) mediante las siguientes etapas:

a) determinar (10) una descomposición del módulo (M) en al menos dos factores P-1 y Q-1, siendo P y Q los números primos preestablecidos en RSA,

b) calcular (12, 14) en cada caso un valor (R1, R2) auxiliar para cada uno de los factores (P-1, Q-1) determinados en la etapa a), siendo cada valor (R1, R2) auxiliar el inverso modular del valor (E) respecto al factor (P-1, Q-1) respectivo como módulo, y

c) calcular (16) el inverso (R) modular del valor (E) respecto al módulo (M) al menos empleando los valores (R1, R2) auxiliares calculados en la etapa b).

2. Procedimiento según la reivindicación 1, caracterizado porque en la etapa c) el inverso (R) modular del valor (E) respecto al módulo (M) se calcula según la relación

$$R = R1 + R2 - R1 \cdot R2 \cdot E \bmod M \qquad (*)$$

.

3. Procedimiento según la reivindicación 2, caracterizado porque en al menos un cálculo la relación (*), dado el caso unida al cálculo del valor auxiliar, se valora repetidamente en un procedimiento iterativo.

4. Procedimiento según una de las reivindicaciones 1 ó 2, caracterizado porque en al menos un cálculo en la etapa b) se realiza una llamada recursiva del procedimiento.

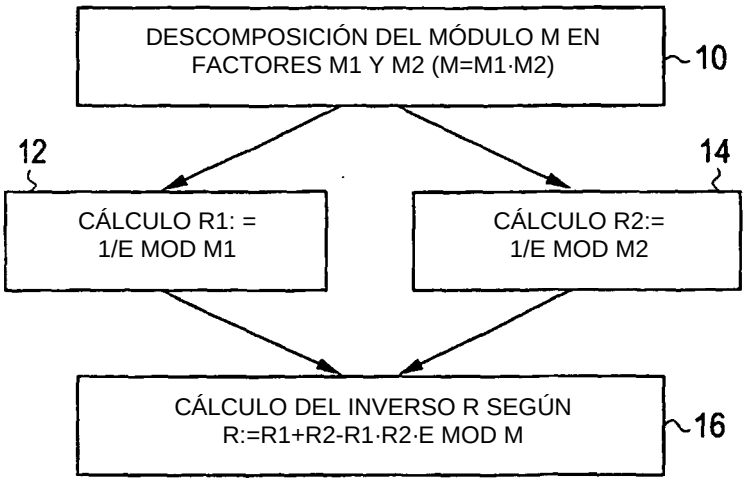
DESCOMPOSICIÓN DEL MÓDULO M EN FACTORES M1 Y M2 (M=M1·M2)
10
12
14
CÁLCULO R1: = 1/E MOD M1
CÁLCULO R2:= 1/E MOD M2
CÁLCULO DEL INVERSO R SEGÚN R:=R1+R2-R1·R2·E MOD M
16

Fig. 1

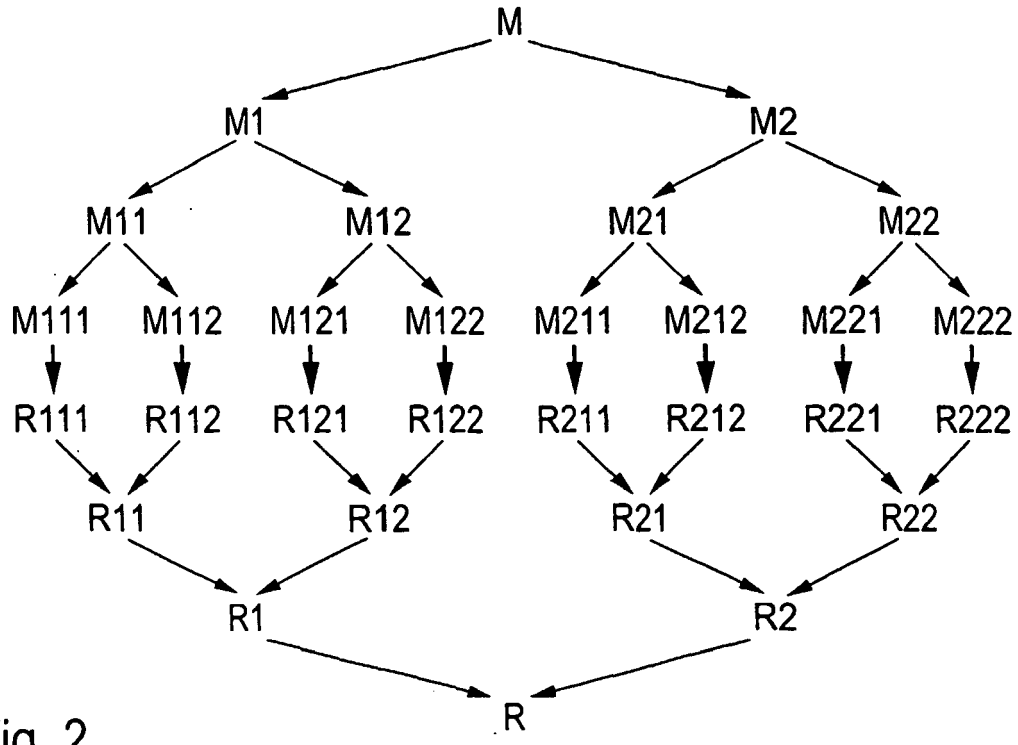
M
M1
M2
M11
M12
M21
M22
M111
M112
M121
M122
M211
M212
M221
M222
R111
R112
R121
R122
R211
R212
R221
R222
R11
R12
R21
R22
R1
R2
R

Fig. 2

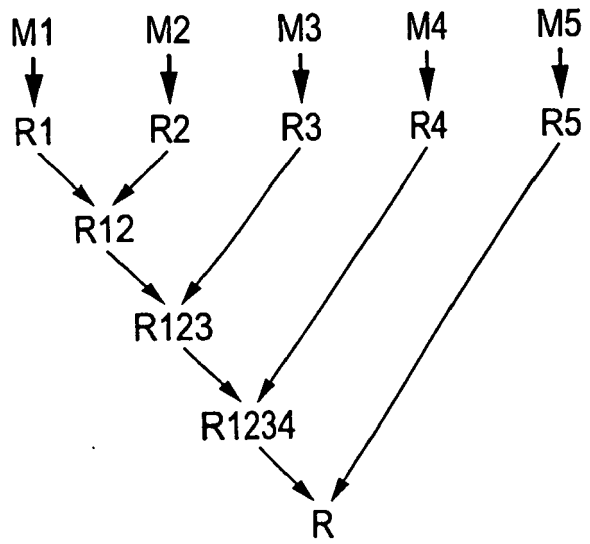

Fig. 3