(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 373 334**

(51) Int. CI.:
H04L 9/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07730938 .3**
(96) Fecha de presentación: **07.02.2007**
(97) Número de publicación de la solicitud: **1982461**
(97) Fecha de publicación de la solicitud: **22.10.2008**

(54) Título: **PROTECCIÓN DE UN ALGORITMO CRIPTOGRÁFICO.**

(30) Prioridad:
08.02.2006 FR 0601135

(45) Fecha de publicación de la mención BOPI:
02.02.2012

(45) Fecha de la publicación del folleto de la patente:
02.02.2012

(73) Titular/es:
SAGEM DÉFENSE SÉCURITÉ
LE PONANT DE PARIS 27 RUE LEBLANC
75015 PARIS, FR

(72) Inventor/es:
CHABANNE, Hervé;
BRINGER, Julien y
DOTTAX, Emmanuelle

(74) Agente: **de Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Protección de un algoritmo criptográfico

La presente invención concierne al ámbito criptográfico y de modo más particular a la protección de las informaciones relativas a los cálculos ejecutados de acuerdo con un algoritmo criptográfico.

Los algoritmos criptográficos permiten especialmente encriptar datos y/o desencriptar datos. Tales algoritmos pueden emplearse igualmente para otras numerosas aplicaciones. En efecto, pueden servir igualmente para firmar, o todavía autenticar ciertas informaciones. Estos pueden ser útiles también en el ámbito del marcado de la fecha y la hora.

Tales algoritmos comprenden generalmente un encadenamiento de varias operaciones, o cálculos, que se aplican sucesivamente a un dato que hay que encriptar con el fin de obtener un dato encriptado, o también a un dato encriptado con el fin de obtener un dato desencriptado.

Entre estos algoritmos, algunos están fundados en una utilización de claves secretas mientras que otros se basan en una utilización mixta de claves públicas y de claves secretas.

Cualquiera que sea el tipo de algoritmo criptográfico, con el fin de conservar el carácter confidencial del algoritmo, de las claves y de otros datos secretos, es importante que los cálculos ejecutados se mantengan secretos.

En efecto, cuando un atacante está en condiciones de determinar los cálculos ejecutados de acuerdo con un algoritmo criptográfico, éste a continuación puede acceder a informaciones secretas y violar el carácter confidencial de los datos de acuerdo con este algoritmo.

En ciertos algoritmos, la protección del carácter confidencial se basa en el hecho de que los cálculos son ejecutados en un entorno protegido, que no es accesible a potenciales atacantes.

En otros ciertos algoritmos, los cálculos pueden ejecutarse en un entorno accesible a potenciales atacantes. Se requiere entonces para tales algoritmos que estos presenten una resistencia a pruebas denominadas pruebas de 'Caja Blanca", o en inglés 'White Box'. Estas pruebas son con miras a intentar violar el carácter confidencial del algoritmo a partir de los cálculos ejecutados en el transcurso de la puesta en práctica del algoritmo.

El documento 'A white-box DES implementation for DRM applications' de S. Chow, P.Elsen, H. Johnson, y P.C. van Oorschot, propone un método que permite una protección contra las pruebas de 'caja blanca', es decir cuando la implementación completa del algoritmo está disponible para el atacante. La técnica empleada se basa en la utilización de tablas que permiten implementar las operaciones del algoritmo, después de que hayan sido introducidas codificaciones con la ayuda de biyecciones entre diferentes rondas del algoritmo.

Sin embargo, el documento « Attacking an obfuscated cipher by injecting faults » de Matthias Jacob, Dan Boneh, y Edward W. Felten en 2003 expone un método que permite encontrar las informaciones secretas utilizadas en la ejecución del algoritmo de acuerdo con el método descrito en el documento anteriormente citado.

El documento « White-Box Cryptography and an AES implementation » de S. Chow, P. Elsen, H. Johnson, y P.C. van Oorschot propone otra implementación basada en principios similares a los que enuncia el documento 'A white-box DES implementation for DRM applications'. Pero, se añaden codificaciones al exterior de las rondas.

El documento « Cryptanalysis of a White-Box AES implementation » de Olivier Billet, Henri Gilbert, y Charaf Ech-Chatbi expone un ataque de esta otra implementación.

Así, los métodos de protección de este tipo presentan fallos que permiten violar el carácter confidencial del algoritmo.

De modo suplementario, el documento FR-A-2776445 expone un procedimiento y un componente electrónico de ejecución de un cálculo criptográfico para facilitar un bloque de datos encriptado a partir de un bloque de datos inicial y que comprende también la introducción de una operación aleatoria para proteger el resultado del cifrado contra el criptoanálisis.

La presente invención pretende aumentar el nivel de una protección de la confidencialidad de un algoritmo contra las pruebas de tipo 'caja blanca'.

Un primer aspecto de la presente invención propone un procedimiento de ejecución de un cálculo criptográfico en un componente electrónico, de acuerdo con un algoritmo criptográfico determinado que incluya al menos una primera y una segunda operación criptográfica. El algoritmo está adaptado para facilitar un bloque de datos encriptado a partir de un bloque de datos inicial.

El procedimiento comprende las etapas siguientes:

Ial aplicación de un primer sistema operativo al bloque de datos inicial y obtención de un primer bloque de datos intermedio, correspondiendo el citado primer sistema operativo a una combinación de al menos la primera operación criptográfica, una primera operación aleatoria que facilita un valor determinado con una valor de probabilidad definido, una segunda operación aleatoria, y una operación biyectiva;

Ibl aplicación de un segundo sistema operativo al bloque de datos intermedio facilitado en la etapa precedente y obtención de un segundo bloque de datos intermedio, correspondiendo el segundo sistema operativo a una combinación de al menos la operación inversa de la operación biyectiva del sistema operativo precedente, la segunda operación criptográfica, y una operación que facilita el valor nulo para un valor asociado al citado valor determinado;

Icl repetición de las etapas Ial y Ibl N veces, siendo N un número entero determinado en función del citado valor de probabilidad definido; y

Idl determinación del bloque de datos encriptado a partir del segundo o de los segundos bloques de datos intermedios, en función del valor de probabilidad definido.

Gracias a estas disposiciones, las operaciones criptográficas que hay que aplicar de acuerdo con el algoritmo que debe protegerse siguen siendo secretas para cualquier atacante. En efecto, éstas son aplicadas a los datos que hay que encriptar de manera combinada con al menos dos operaciones aleatorias, facilitando una de estas dos operaciones con una probabilidad definida un valor determinado. El efecto de esta primera operación aleatoria solamente es anulado ventajosamente con la aplicación de la operación que facilita el valor cero para un valor asociado al citado valor determinado. Así, desde la aplicación de la primera operación aleatoria y hasta la aplicación de la operación que facilita cero para un valor asociado al valor determinado, los datos que son manipulados en el transcurso de la puesta en práctica de dicha ejecución de cálculos quedan protegidos contra los ataques.

Cuando el procedimiento corresponde a la aplicación únicamente de un primero y de un segundo sistemas operativos, el valor asociado es igual al valor determinado.

Conviene observar que los términos ‘operación criptográfica’ corresponden a una operación criptográfica en el sentido amplio, es decir que estos términos designan también una sucesión de operaciones criptográficas.

La aplicación del primer sistema operativo puede corresponder a la aplicación de manera combinada de:

- la primera operación criptográfica que facilita un primer resultado del primer sistema operativo a partir del bloque de datos inicial;
- la primera operación aleatoria que facilita un segundo resultado del primer sistema operativo a partir del bloque de datos inicial;
- la segunda operación aleatoria que facilita un tercer resultado del primer sistema operativo a partir del bloque de datos inicial; y
- la operación biyectiva que facilita el primer bloque de datos intermedio a partir de los primero, segundo y tercero resultados del primer sistema operativo.

La aplicación del segundo sistema operativo puede corresponder a la aplicación, de manera combinada, de:

- la operación inversa de la operación biyectiva del sistema operativo precedente que facilita, a partir del bloque de datos intermedio obtenido por el sistema operativo precedente, los citados primero y segundo resultados del sistema operativo precedente;
- la segunda operación criptográfica que facilita un primer resultado del segundo sistema operativo a partir del primer resultado del sistema operativo precedente;
- la operación que facilita el valor nulo para un valor asociado al valor determinado a partir del segundo resultado del sistema operativo precedente, que facilita así un segundo resultado del segundo sistema operativo; y
- una adición del primero y del segundo resultados del segundo sistema operativo que facilita el segundo bloque de datos intermedio.

Cada dato del primero y del segundo bloques de datos intermedios puede ser obtenido en forma polinómica a partir respectivamente de los datos del bloque de datos inicial y de los datos del primer bloque de datos intermedio.

Los primero y segundo sistemas operativos pueden ser aplicados en forma de tablas de valores respectivamente al bloque de datos inicial y al primer bloque de datos intermedio.

La primera operación aleatoria que facilita un valor determinado con un valor de probabilidad definido puede ser efectuada en un espacio matemático finito en el cual ésta facilita como mucho un conjunto determinado de valores; y

en el cual la operación que facilita el valor nulo para un valor asociado al citado valor determinado facilita el valor nulo además para los otros valores del citado conjunto.

Así, el número N correspondiente al número de iteraciones de las etapas para determinar el bloque de datos encriptados puede ser ventajosamente igual a 1.

El procedimiento puede comprender además entre la etapa Ial y la etapa Ibl, cuando el algoritmo incluye un conjunto de K operaciones criptográficas suplementarias entre las primera y segunda operaciones criptográficas, siendo K un entero positivo, la etapa siguiente:

- aplicación de un número K de sistemas operativos suplementarios (108) sucesivos respectivamente asociados al citado conjunto de operaciones criptográficas suplementarias, facilitando cada sistema operativo suplementario un bloque de datos intermedio suplementario (114), a partir del bloque de datos intermedio (107) facilitado por el sistema operativo precedente;

en el cual cada sistema operativo suplementario corresponde a una combinación de al menos la operación inversa (109) de la operación biyectiva del sistema operativo precedente, la operación criptográfica suplementaria (110) asociada al citado sistema operativo suplementario, una operación suplementaria (111), una operación aleatoria (112) y una operación biyectiva (113).

En este caso, el valor asociado al valor determinado para el cual la función se anula corresponde ventajosamente al valor resultante de la aplicación de la operación suplementaria al citado valor determinado, o también de las aplicaciones sucesivas de las operaciones suplementarias al valor determinado.

El sistema operativo suplementario puede corresponder a la aplicación, de manera combinada, de:

- la operación inversa de la operación biyectiva del sistema operativo precedente, que facilita, a partir del bloque de datos intermedio facilitado por el sistema operativo precedente, los primero, segundo y tercero resultados del sistema operativo precedente;
- la operación criptográfica suplementaria que facilita un primer resultado del sistema operativo suplementario a partir del primer resultado del sistema operativo precedente;
- la operación suplementaria que facilita un segundo resultado del sistema operativo suplementario a partir del segundo resultado del sistema operativo precedente;
- la operación aleatoria que facilita un tercer resultado del sistema operativo suplementario a partir de al menos uno entre los primero, segundo y tercero resultados del sistema operativo precedente; y
- una operación biyectiva que facilita el bloque de datos intermedio suplementario a partir de los pimero, segundo y tercero resultados del sistema operativo suplementario.

La operación suplementaria puede corresponder ventajosamente a una operación de identidad y así facilitar los cálculos. En tal caso, el valor asociado al valor determinado, para el cual la segunda operación específica facilita un valor nulo, es de modo más preciso igual a este valor determinado.

Asimismo, las operaciones biyectivas pueden corresponder ventajosamente a operaciones biyectivas lineales y así aligerar los cálculos.

Un segundo aspecto de la presente invención propone un componente electrónico de ejecución de un cálculo criptográfico de acuerdo con un algoritmo criptográfico que incluye al menos una primera y una segunda operación criptográfica, estando adaptado este componente electrónico para poner en práctica un procedimiento de ejecución de cálculos de acuerdo con el primer aspecto de la presente invención.

Al menos una entre la primera operación aleatoria, la segunda operación aleatoria y la operación biyectiva pueden diferir en cada repetición de los primero y segundo sistemas operativos.

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

La invención será igualmente comprendida mejor con la ayuda de los dibujos, en los cuales:

- la figura 1 ilustra las diferentes etapas de un algoritmo criptográfico que comprende una pluralidad de operaciones criptográficas; y
- la figura 2 ilustra las principales etapas de un procedimiento de ejecución de acuerdo con un modo de realización de la presente invención.

Un objetivo de la presente invención es mejorar la resistencia a los ataques con-tra los algoritmos criptográficos en el transcurso de pruebas denominadas de 'caja blanca', es decir cuando la implementación del algoritmo criptográfico que hay que proteger es accesible a potenciales atacantes. A tal efecto, se modifican las operaciones criptográficas que hay que aplicar a un bloque de datos de acuerdo con el algoritmo determinado que hay que proteger. Así, en lugar de aplicar di-recta y sucesivamente las operaciones criptográficas del algoritmo que hay que proteger, se aplican sucesivamente respectivos sistemas operativos de modo que, por una parte, los datos obtenidos a la salida de las operaciones criptográficas del algoritmo que hay que proteger y, por otra, los datos a la salida de los diferentes sistemas operativos, no permitan violar la confidencialidad del algoritmo criptográfico que hay que proteger.

De acuerdo con un modo de realización de la presente invención, cada sistema operativo es generado respectivamente a partir de cada operación criptográfica del algoritmo. De modo más preciso, en cada sistema operativo correspondiente a una operación criptográfica determinada, se introducen variables aleatorias. Después, al menos dos sistemas operativos, entre los sistemas operativos así generados a partir de las diferentes operaciones criptográficas del algoritmo que hay que proteger, comprenden respectivamente además una primera y una segunda operación específica.

Además del aleatorio introducido por las operaciones aleatorias introducidas en cada sistema operativo, estas dos operaciones específicas permiten mejorar eficazmente la protección del algoritmo criptográfico, especialmente con respecto a las operaciones criptográficas que son ejecutadas entre las dos operaciones criptográficas a la cuales corresponden los dos sistemas operativos que comprenden estas dos operaciones específicas.

En efecto, los datos de salida de cada sistema operativo puesto en práctica entre estos dos sistemas operativos que comprenden las dos operaciones específicas, pueden ser captados por un potencial atacante sin que esto pueda amenazar la confidencialidad de la parte del algoritmo que hay que proteger que está comprendida entre las dos operaciones criptográficas del algoritmo que son ejecutadas en el seno de estos dos sistemas operativos.

Con el objetivo de proteger el conjunto de las operaciones criptográficas del algoritmo, las dos operaciones específicas pueden ser introducidas ventajosamente en el primer sistema operativo generado a partir de la primera operación criptográfica del algoritmo y en el último sistema operativo generado a partir de la última operación criptográfica del algoritmo.

La primera operación específica corresponde a una función aleatoria que facilita de manera aleatoria un valor de salida, tomando este valor de salida un valor determinado con una probabilidad definida.

La segunda operación específica corresponde a una función que facilita el valor nulo en valor de salida para un valor de entrada correspondiente a un valor asociado al valor determinado. De manera general, este valor asociado corresponde a la transformación que experimenta el valor determinado, en su caso, después de la aplicación de las operaciones suplementarias de los sistemas operativos suplementarios puestos en práctica entre el primero y el segundo sistemas operativos de acuerdo con un modo de realización de la presente invención.

Por consiguiente, en un caso general, cuando se reitera, un número de veces predeterminado en función del valor de la probabilidad definida, una aplicación del primero y segundo sistemas operativos asociados, tal como la descrita anteriormente, se está incondiciones de anular el efecto de la primera operación específica por el de la segunda operación específica que le está asociada. Se observa que cada conjunto del primero y segundo sistemas operativos asociados puede ventajosamente ser construido con primeras y segundas operaciones específicas asociadas diferentes, operaciones aleatorias y operaciones biyectivas diferentes también.

En tanto que el efecto de la primera operación específica no sea anulado, las informaciones accesibles a un atacante, durante la ejecución del algoritmo de acuerdo con un modo de realización de la presente invención, difieren ligeramente de los datos que son obtenidos en diferentes etapas de una ejecución directa del algoritmo que hay que proteger.

Los datos susceptibles de ser captados por un atacante a la salida de cada uno de los sistemas operativos, no solamente corresponden a los datos que serían obtenidos por aplicación directa de las operaciones criptográficas correspondientes, sino que, además, estos presentan un carácter aleatorio con respecto a los datos que deberían obtenerse. Así, los potenciales ataques durante la ejecución de un algoritmo de este tipo resultan vanos.

La presente invención es descrita en su aplicación a un algoritmo que comprende una pluralidad de rondas, pudiendo corresponder cada ronda a una pluralidad de operaciones criptográficas. Sin embargo, conviene observar que ninguna limitación está ligada al tipo de algoritmo criptográfico. En efecto, la presente invención puede ser aplicada fácilmente a cualquier algoritmo criptográfico que comprenda al menos una primera y una segunda operaciones criptográficas.

En un modo de realización de la presente invención, las dos operaciones específicas son introducidas en la primera ronda y la última ronda. Sin embargo, se puede prever introducir estas dos operaciones específicas en cualquier etapa del algoritmo que hay que proteger.

La figura 1 ilustra las etapas de un algoritmo criptográfico que comprende una pluralidad de rondas. En una etapa 10, se aplica a un bloque de datos X inicial 101 que hay que encriptar una ronda del algoritmo que comprende una o varias operaciones criptográficas. La aplicación de las operaciones criptográficas de esta ronda es una ronda operativa R_1. En la etapa 11, se obtiene entonces un bloque de datos Y_1. Éste verifica la ecuación:

$$Y_1 = R_1(X)$$

Después, en la etapa 12, se aplican a este bloque Y_1 las operaciones de la segunda ronda R_2 del algoritmo criptográfico. Se obtiene entonces un bloque Y_2 que verifica la ecuación siguiente:

$$Y_2 = R_2(Y_1)$$

Se aplican, así, sucesivamente las diferentes rondas R_i, para i comprendido entre 1 y r. Una etapa 14 representa el bloque de datos Y_{r-1} así obtenido a la salida de la penúltima ronda R_{r-1}. Este bloque de datos verifica la ecuación siguiente:

$$Y_{r-1} = R_{r-1}(Y_{r-2})$$

Después, en la etapa 15, se aplican a este bloque Y_{r-1} las operaciones de la última ronda R_r del algoritmo considerado, y en la etapa 16, se obtiene el bloque de datos encriptado Y_r que verifica la ecuación siguiente:

$$Y_r = R_r(Y_{r-1})$$

La figura 2 describe las etapas de un procedimiento de ejecución de cálculos criptográficos de acuerdo con un modo de realización de la presente invención aplicado a un algoritmo correspondiente al descrito anteriormente refiriéndose a la figura 1.

En un modo de realización de la presente invención, cuando un sistema operativo comprende una pluralidad de operaciones criptográficas que hay que aplicar a un bloque de datos inicial X=(x1,…,xn) con el fin de facilitar un bloque de datos Z=(z1, …, zn) resultante de la serie de las operaciones sucesivas, cada componente del bloque de datos resultante es expresado en forma polinómica en función de los diferentes componentes x_1, …, x_n del bloque de datos inicial X.

De modo más preciso, cuando un sistema operativo S, que hay que aplicar a un bloque de datos X inicial para obtener un bloque de datos resultante Z, comprende una sucesión de operaciones, este bloque de datos X es descompuesto en una pluralidad de bloques de datos de tamaño inferior x_1, ,,,, x_n. Después, cada bloque de datos z_i que componen el bloque de datos Z puede ser obtenido en forma polinómica en función de los diferentes componentes x_i del bloque de datos inicial. Así, cada componente del bloque de datos resultante de la aplicación de las operaciones del sistema operativo considerado es facilitado entonces en una sola transformación. En tales condiciones, la sucesión y la distinción de las operaciones que componen el sistema operativo aplicado es entonces de acceso difícil para un potencial atacante.

Así pues, se puede escribir la ecuación siguiente:

$$Z = S(X) \qquad [1]$$

y para i comprendido entre 1 y n, existe un polinomio tal que:

$$Z_i = p_i(x_1,\ldots, x_n) \qquad [2]$$

Las secciones siguientes utilizan la aplicación de las diferentes operaciones criptográficas en la forma combinada expresada anteriormente.

En una variante, se puede prever también obtener los diferentes componentes del bloque de datos resultante de las operaciones criptográficas del sistema operativo en forma de tablas de valores.

Cualquiera que sea el método de aplicación utilizado, sea en una forma polinómica, o también en una forma de tablas de valor, las operaciones que hay que aplicar de acuerdo con un sistema operativo son aplicadas preferentemente de manera combinada, de modo que cada componente del bloque de datos resultante del sistema operativo es obtenido en una sola transformación.

En un modo de realización de la presente invención, el algoritmo que hay que proteger es puesto en práctica modificando las rondas operativas R_i, para i comprendido entre 1 y r, tales como las descritas anteriormente. En un modo de realización de la presente invención, al menos una ronda operativa R_i del algoritmo está asociada a un sistema operativo S_i que es una combinación de al menos un modo operativo aleatorio R_i del algoritmo que hay que proteger, una operación aleatoria A_i y una operación aleatoria V que facilita un valor determinado v con una probabilidad definida. Una ejecución combinada de las diferentes operaciones de tales sistemas operativos S_i permite ventajosamente obtener un bloque de datos resultante en una sola transformación a partir del bloque de datos inicial. Así, un potencial atacante no puede distinguir las diferentes operaciones de manera separada.

Conviene observar que la presente invención encuentra también una aplicación fácil al caso en que una ronda operativa del algoritmo R_i corresponda a una sola operación criptográfica.

En una etapa 102, se aplica un primer sistema operativo S_1 al bloque de datos inicial 101. De modo más preciso, en un modo de realización de la presente invención, este primer sistema operativo corresponde a aplicar de manera combinada al bloque de datos inicial 101:

- la primera ronda operativa R_1 del algoritmo que hay que proteger;
- la operación aleatoria A_1; y
- la primera operación aleatoria V; después

en combinar los diferentes bloques de datos resultantes de estas tres operaciones aplicadas al bloque de datos inicial 101 de modo que se obtenga un primer bloque de datos intermedio 107. Esta combinación es obtenida por aplicación de una aplicación biyectiva a los resultados de estas tres operaciones antes citadas.

Este sistema operativo es puesto en práctica en forma de una sola transformación, que permite obtener, componente a componente, a partir del bloque de datos inicial, el primer bloque de datos intermedio, como se describió anteriormente. Así, éste puede ser puesto en práctica en forma polinómica o también en forma de tablas de valores.

La sección siguiente detalla las operaciones a las cuales corresponde la aplicación del primer sistema operativo S_1 de acuerdo con un modo de realización de la presente invención.

Se aplica al bloque de datos X inicial 101, que puede escribirse en forma de una sucesión de datos x_1, …, x_n, la ronda operativa R_1 del algoritmo considerado. Se obtiene un primer resultado 103 del primer sistema operativo, indicado por $Y_{1,1}$ correspondiente a un bloque de datos que verifica la ecuación siguiente:

$$Y_{1,1} = R_1(X)$$

Se observa que $Y_{1,1}$ es igual a Y_1 tal como se definió anteriormente refiriéndose a la figura 1. Pero, tal resultado no es accesible a un potencial atacante puesto que en el transcurso de la ejecución de las operaciones que componen el sistema operativo S_1, esta etapa inicial es mezclada con las otras operaciones que hay que aplicar descritas a continuación, en forma polinómica o en forma de tablas de valores.

Después, cuando se aplica la función V al bloque de datos inicial, se obtiene un segundo resultado 104 de este primer sistema operativo en forma de un bloque de datos que verifica la ecuación siguiente:

$$Y_{1,2} = V(X)$$

Aplicando la operación aleatoria A_1 a un bloque de datos inicial X, se obtiene un tercer resultado 105 del primer sistema operativo en forma de un bloque de datos $Y_{1,3}$ que verifica la ecuación siguiente:

$$Y_{1,3} = A_1(X)$$

Con el fin de no permitir una distinción de los tres resultados descritos anteriormente a la salida del primer sistema operativo, se efectúa una combinación 106 de estos tres resultados para facilitar el primer bloque de datos intermedio 107 que corresponde a la ejecución de la primera ronda del algoritmo de acuerdo con un modo de realización de la presente invención.

Así, a la salida del primer sistema operativo S_1, se obtiene el bloque de datos intermedio XI_1 que verifica la ecuación siguiente:

$$XI_1 = M1(Y_{1,1}; Y_{1,2}; Y_{1,3})$$

donde M1 es la combinación biyectiva aplicada en el primer sistema operativo S_1.

Ventajosamente, el bloque de datos intermedio XI_1 difiere del bloque de datos Y_1 obtenido a la salida de la primera ronda de acuerdo con el algoritmo criptográfico refiriéndose a la figura 1. Tal diferencia no permite encontrar, a partir del bloque de datos XI_1, el bloque de datos Y_1 que es igual al bloque de datos $Y_{1,1}$.

Después, se aplica al primer bloque de datos intermedio 107 un segundo sistema operativo 108, correspondiente a la ejecución de la segunda ronda del algoritmo que hay que proteger de acuerdo con un modo de realización de la presente invención. Éste corresponde a la aplicación combinada de una operación inversa de la operación biyectiva del sistema operativo precedente, de la segunda ronda operativa del algoritmo que hay que proteger R_2, de una operación aleatoria A_2, de una operación correspondiente a la identidad I_2 y de una operación biyectiva M_2.

Este segundo sistema operativo corresponde a la aplicación de las operaciones que se escriben de manera separada en detalle en las secciones siguientes pero que son aplicadas en una sola transformación, componente por com-

ponente, como para todos los sistemas operativos descritos de acuerdo con un modo de realización de la presente invención.

Este sistema operativo corresponde a la aplicación en primer lugar de la operación inversa M_1^{-1} 109 de la operación M_1 al bloque de datos XI_1 de modo que se obtienen de manera distinta los tres resultados descritos para el primer sistema operativo, $Y_{1,1}$; $Y_{1,2}$ e $Y_{1,3}$.

Después, se aplican al primer resultado $Y_{1,1}$ 110 las operaciones criptográficas de la ronda R_2 del algoritmo criptográfico y se obtiene entonces un primer resultado $Y_{2,1}$ del segundo sistema operativo S_2 que verifica la ecuación siguiente:

$$Y_{2,1} = R_2(Y_{1,1})$$

A continuación, se aplica la operación I_2 al segundo resultado del sistema operativo precedente $Y_{1,2}$ y se obtiene un segundo resultado 111 del segundo sistema operativo, que verifica la operación siguiente:

$$Y_{2,2} = Y_{1,2}$$

En el ejemplo descrito a continuación, se considera la operación identidad. Pero, esta operación puede ser diferente de una operación identidad. De manera más general, esta operación puede ser una operación cualquiera.

Se aplica la operación aleatoria A_2 al tercer resultado del sistema operativo precedente $Y_{1,3}$ para obtener un tercer resultado 112 del segundo sistema operativo, que verifica la ecuación siguiente:

$$Y_{2,3} = A_2(Y_{1,1}; Y_{1,2}; Y_{1,3})$$

En una variante, se puede prever que la operación aleatoria tome en la entrada un subconjunto cualquiera de tres resultados $Y_{1,1}$; $Y_{1,2}$; $Y_{1,3}$.

Después, se aplica entonces una operación biyectiva M_2, indicada por 113, a los primero, segundo y tercero resultados del segundo sistema operativo para obtener un segundo bloque de datos intermedios 114 XI_2. Ese bloque de datos 114 verifica la ecuación siguiente:

$$XI_2 = M_2(Y_{2,1}: Y_{2,2}; Y_{2,3})$$

En un modo de realización de la presente invención, los sistemas operativos Si, para i comprendido entre 2 y r-1, corresponden a la aplicación de operaciones similares a las descritas refiriéndose al segundo sistema operativo.

De la descripción anterior es fácil deducir variantes de la aplicación de la presente invención en las cuales las operaciones pueden diferir en función de los sistemas operativos. Así, por ejemplo, se puede prever en ciertos sistemas operativos que la función I descrita anteriormente sea una función identidad mientras que en otros sea una función cualquiera diferente de la función identidad.

Después, el último sistema operativo 116 S_r corresponde a la aplicación combinada de una operación correspondiente a la operación inversa 117 de la operación biyectiva M_{r-1} del sistema operativo precedente, de la roda operativa R_r del algoritmo que hay que proteger, y de una operación Z_v que facilita el valor nulo para un valor asociado al valor determinado v. Las secciones siguientes detallan la aplicación separada de estas diferentes operaciones. Conviene observar que, como en cada sistema operativo S_i, estas operaciones son aplicadas de manera combinada.

El sistema operativo precedente S_{r-1} facilita un bloque de datos intermedio XI_{r-1} de orden r-1, indicado por 115. La operación inversa 117 de la operación biyectiva M_{r-1}^{-1} facilita a partir del bloque de datos intermedio XI_{r-1}, el primero y el segundo resultados del sistema operativo S_{r-1}.

Se aplica la ronda operativa R_r del algoritmo que hay que proteger al primer resultado $Y_{r-1,1}$ y se obtiene un primer resultado 118 del sistema operativo S_i que verifica la ecuación siguiente:

$$Y_{r-1} = R_r(Y_{r-1,1})$$

Se aplica la operación Z_v al segundo resultado del sistema operativo precedente $Y_{r-1,\ 2}$, y se obtiene un segundo resultado 119 que verifica la ecuación siguiente:

$$Y_{r,2} = Z_v(Y_{r-1,2})$$

Ahora bien, este segundo resultado $Y_{r-1,2}$ corresponde al segundo resultado del primer sistema operativo $Y_{1,2}$. En efecto, éste no ha sido transformado por los diferentes sistemas operativos que han sucedido al primer sistema operativo, en el caso en que se consideren las operaciones I_2, …, I_{r-1} como la operación identidad.

Así, se puede escribir:

$Y_{r,2} = Z_v(V(X))$

En el caso en que las operaciones I_2, …, I_{r-1} sean diferentes de la identidad, esta última ecuación no se verifica. Pero, en este caso, la función V es elegida ventajosamente de modo que facilite el valor cero para el valor asociado al valor determinado V(X), es decir para el valor que resulte de las transformaciones de V(X) en los diferentes sistemas operativos suplementarios.

Después, los primero y segundo resultados son finalmente combinados para facilitar un bloque de datos intermedio 120 XI_r de orden r. Este bloque de datos intermedio verifica la ecuación siguiente:

$XI_r = Y_{r,1} + Y_{r,2}$

En un caso general, se determina un número de repeticiones mínimo de versiones diferentes del algoritmo que hay que proteger de acuerdo con un modo de realización de la presente invención en función del valor de probabilidad definido con el cual la operación V facilita el valor determinado v.

Así, por ejemplo, si el valor de probabilidad definido es igual a 2/3, conviene repetir al menos 3 veces la aplicación del conjunto de los sistemas operativos sucesivos respectivamente asociados a conjunto de las operaciones criptográficas del algoritmo, tales como las definidas anteriormente, con el fin de poder determinar después una ejecución de éste, entre los últimos bloques de datos intermedios obtenidos, que corresponde al bloque de datos encriptado de acuerdo con el algoritmo inicial que hay que proteger, es decir el que corresponde al bloque de datos Y_r. El conjunto de los sistemas operativos sucesivos de cada una de las aplicaciones verifica las características descritas de acuerdo con un modo de realización de la presente invención, pero estos conjuntos de sistemas operativos pueden ser diferentes entre sí en cada nueva aplicación. Esos, especialmente, pueden estar basados en operaciones aleatorias diferentes y operaciones biyectivas diferentes.

Gracias a las disposiciones descritas en las secciones precedentes, cuando la función V es introducida en el primer sistema operativo y la función Z_v es introducida en el último sistema operativo, ningún dato accesible a un potencial atacante facilita informaciones sobre los datos de salida intermedia correspondiente a la ejecución directa del algoritmo que hay que proteger.

Las secciones siguientes describen un caso particular de aplicación de la presente invención en el cual el bloque de datos encriptado de acuerdo con el algoritmo que hay que proteger es determinado ejecutando una sola vez el procedimiento de ejecución de acuerdo con un modo de realización de la presente invención.

Situándose en el cuerpo finito GF(2), cualquier polinomio P solamente puede tener dos valores, 0 o 1. Se puede elegir:

$V(X) = (P(X) + v_1, \ldots P(X) + v_m)$

Así, V(X) solamente puede tomar dos valores diferentes, o sea:

$v = (v_1, \ldots, v_n)$, o

$v = (v_{1+1}, \ldots, v_{n+1})$

En tal contexto, si la función Z_v toma el valor 0 en los valores v y v', entonces una sola iteración de la ejecución del algoritmo que hay que proteger de acuerdo con un modo de realización de la presente invención es suficiente para obtener el bloque de datos encriptado de acuerdo con el citado algoritmo.

REIVINDICACIONES

1. Procedimiento de ejecución de un cálculo criptográfico en un componente electrónico, de acuerdo con un algoritmo criptográfico determinado que incluye al menos una primera y una segunda operación criptográfica, estando adaptado el citado algoritmo para facilitar un bloque de datos encriptado a partir de un bloque de datos inicial.

comprendiendo el citado procedimiento las etapas siguientes:

Ial aplicación de un primer sistema operativo (102) al bloque de datos inicial y obtención de un primer bloque de datos intermedio, correspondiendo el citado primer sistema operativo a una combinación de al menos la primera operación criptográfica (103), una primera operación aleatoria (104) que facilita un valor determinado con una valor de probabilidad definido, una segunda operación aleatoria (105), y una operación biyectiva (106);

Ibl aplicación de un segundo sistema operativo (116) al bloque de datos intermedio facilitado en la etapa precedente y obtención de un segundo bloque de datos intermedio, correspondiendo el citado segundo sistema operativo a una combinación de al menos la operación inversa (117) de la operación biyectiva del sistema operativo precedente, la segunda operación criptográfica (118), y una operación que facilita el valor nulo para un valor asociado al citado valor determinado (119);

Icl repetición de las etapas Ial y Ibl N veces, siendo N un número entero determinado en función del citado valor de probabilidad definido; y

Idl determinación del bloque de datos encriptado a partir del segundo o de los segundos bloques de datos intermedios, en función del valor de probabilidad definido.

2. Procedimiento de ejecución de un cálculo criptográfico de acuerdo con la reivindicación 1, en el cual la aplicación del primer sistema operativo corresponde a la aplicación de manera combinada de:

- la primera operación criptográfica que facilita un primer resultado (103) del primer sistema operativo a partir del bloque de datos inicial;
- la primera operación aleatoria que facilita un segundo resultado (104) del primer sistema operativo a partir del bloque de datos inicial;
- la segunda operación aleatoria que facilita un tercer resultado (105) del primer sistema operativo a partir del bloque de datos inicial; y
- la operación biyectiva (106) que facilita el primer bloque de datos intermedio (107) a partir de los primero, segundo y tercero resultados del primer sistema operativo, y

en el cual la aplicación del segundo sistema operativo puede corresponder a la aplicación, de manera combinada, de:

- la operación inversa (117) de la operación biyectiva del sistema operativo precedente que facilita, a partir del bloque de datos intermedio obtenido por el sistema operativo precedente, los citados primero y segundo resultados del sistema operativo precedente;
- la segunda operación criptográfica (118) que facilita un primer resultado del segundo sistema operativo a partir del primer resultado del segundo sistema operativo precedente;
- la operación que facilita el valor nulo para un valor asociado al valor determinado (119) a partir del segundo resultado del sistema operativo precedente, que facilita así un segundo resultado del segundo sistema operativo; y
- una adición del primero y del segundo resultados del segundo sistema operativo que facilita el segundo bloque de datos intermedio (120).

3. Procedimiento de ejecución de un cálculo criptográfico de acuerdo con las reivindicaciones 1 o 2, en el cual cada dato del primero y del segundo bloques de datos intermedios puede ser obtenido en forma polinómica a partir respectivamente de los datos del bloque de datos inicial y de los datos del primer bloque de datos intermedio.

4. Procedimiento de ejecución de un cálculo criptográfico de acuerdo con las reivindicaciones 1 o 2, en el cual los primero y segundo sistemas operativos son aplicados en forma de tablas de valores respectivamente al bloque de datos inicial y al primer bloque de datos intermedio.

5. Procedimiento de ejecución de un cálculo criptográfico de acuerdo con una cualquiera de las reivindicaciones precedentes, en el cual la primera operación aleatoria que facilita un valor determinado con un valor de probabilidad definido es efectuada en un espacio matemático finito en el cual ésta facilita como mucho un conjunto determinado de valores; y

en el cual la segunda operación que facilita un valor nulo para un valor asociado al citado valor determinado facilita el valor nulo además para los valores del citado conjunto que son diferentes del citado valor determinado.

6. Procedimiento de ejecución de un cálculo criptográfico de acuerdo con una cualquiera de las reivindicaciones precedentes, que comprende además entre la etapa Ial y la etapa Ibl, cuando el algoritmo incluye un conjunto de K operaciones criptográficas suplementarias entre las primera y segunda operaciones criptográficas, siendo K un entero positivo, la etapa siguiente:

- aplicación de un número K de sistemas operativos suplementarios (108) sucesivos respectivamente asociados al citado conjunto de operaciones criptográficas suplementarias, facilitando cada sistema operativo suplementario un bloque de datos intermedio suplementario (114), a partir del bloque de datos intermedio (107) facilitado por el sistema operativo precedente;

en el cual cada sistema operativo suplementario corresponde a una combinación de al menos la operación inversa (109) de la operación biyectiva del sistema operativo precedente, la operación criptográfica suplementaria (110) asociada al citado sistema operativo suplementario, una operación suplementaria (111), una operación aleatoria (112) y una operación biyectiva (113).

7. Procedimiento de ejecución de un cálculo criptográfico de acuerdo con la reivindicación 6, en el cual cada sistema operativo suplementario corresponde a la aplicación, de manera combinada, de:

- la operación inversa (109) de la operación biyectiva del sistema operativo precedente, que facilita, a partir del bloque de datos intermedio facilitado por el sistema operativo precedente, los primero (131), segundo (132) y tercero (133) resultados del sistema operativo precedente;
- la operación criptográfica suplementaria (110) que facilita un primer resultado (134) del sistema operativo suplementario a partir del primer resultado del sistema operativo precedente;
- la operación suplementaria (111) que facilita un segundo resultado del sistema operativo suplementario a partir del segundo resultado (132) del sistema operativo precedente;
- la operación aleatoria (112) que facilita un tercer resultado (136) del sistema operativo suplementario a partir de al menos uno entre los primero, segundo y tercero resultados del sistema operativo precedente; y
- una operación biyectiva (113) que facilita el bloque de datos intermedio suplementario a partir de los primero, segundo y tercero resultados del sistema operativo suplementario.

8. Procedimiento de ejecución de un cálculo criptográfico de acuerdo con una de las reivindicaciones 6 y 7, en el cual la operación suplementaria (111) es una operación de identidad y en el cual el valor asociado al valor determinado es igual al valor determinado.

9. Componente electrónico de ejecución de un cálculo criptográfico de acuerdo con un algoritmo criptográfico que incluye al menos una primera y una segunda operaciones criptográficas, estando adaptado el citado algoritmo para facilitar un bloque de datos encriptado a partir de un bloque de datos inicial;

comprendiendo el citado componente:

- primeros medios para aplicar un primer sistema operativo (102) al bloque de datos inicial y facilitar un primer bloque de datos intermedio, correspondiendo el citado primer sistema operativo a una combinación de al menos la primera operación criptográfica, una primera operación aleatoria que facilita un valor determinado con un valor de probabilidad definido, una segunda operación aleatoria, y una operación biyectiva;
- segundos medios para aplicar un segundo sistema operativo (116) al bloque de datos intermedio facilitado por los medios precedentes y facilitar un segundo bloque de datos intermedio, correspondiendo el citado segundo sistema operativo a una combinación de al menos una operación inversa de la operación biyectiva de los medios precedentes, la segunda operación criptográfica y una operación que facilita el valor nulo para un valor asociado al citado valor determinado;
- medios para repetir N veces la aplicación de los primero y segundo sistemas operativos, siendo N un número entero determinado en función del citado valor de probabilidad definido; y
- medios para determinar el bloque de datos encriptado a partir del segundo o de los segundos bloques de datos intermedios, en función del valor de probabilidad definido.

10. Componente electrónico de ejecución de un cálculo criptográfico de acuerdo con la reivindicación 9, en el cual al menos una entre la primera operación aleatoria, la segunda operación aleatoria, y la operación biyectiva difieren en cada repetición de los primero y segundo sistemas operativos.

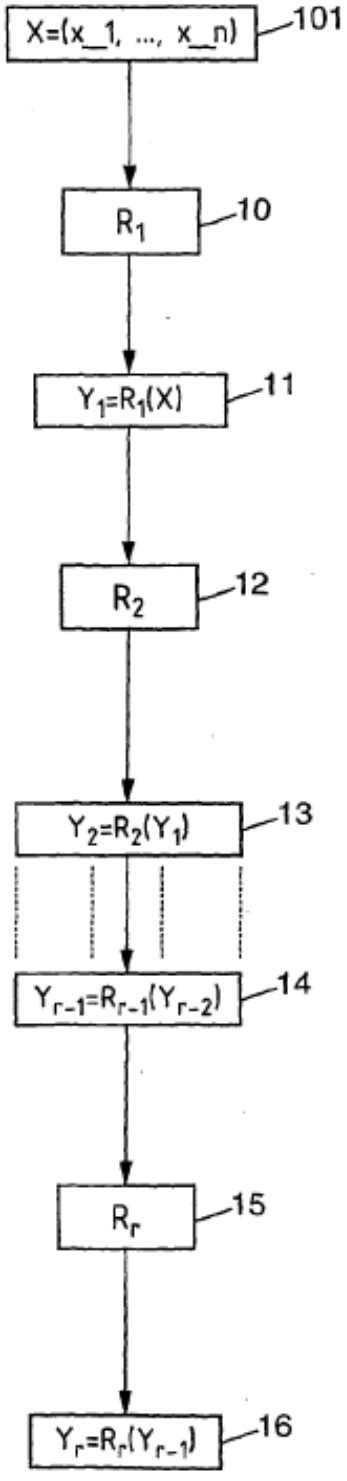
X=(x_1, ..., x_n)
101
R1
10
Y1=R1(X)
11
R2
12
Y2=R2(Y1)
13
Yr-1=Rr-1(Yr-2)
14
Rr
15
Yr=Rr(Yr-1)
16

FIG. 1

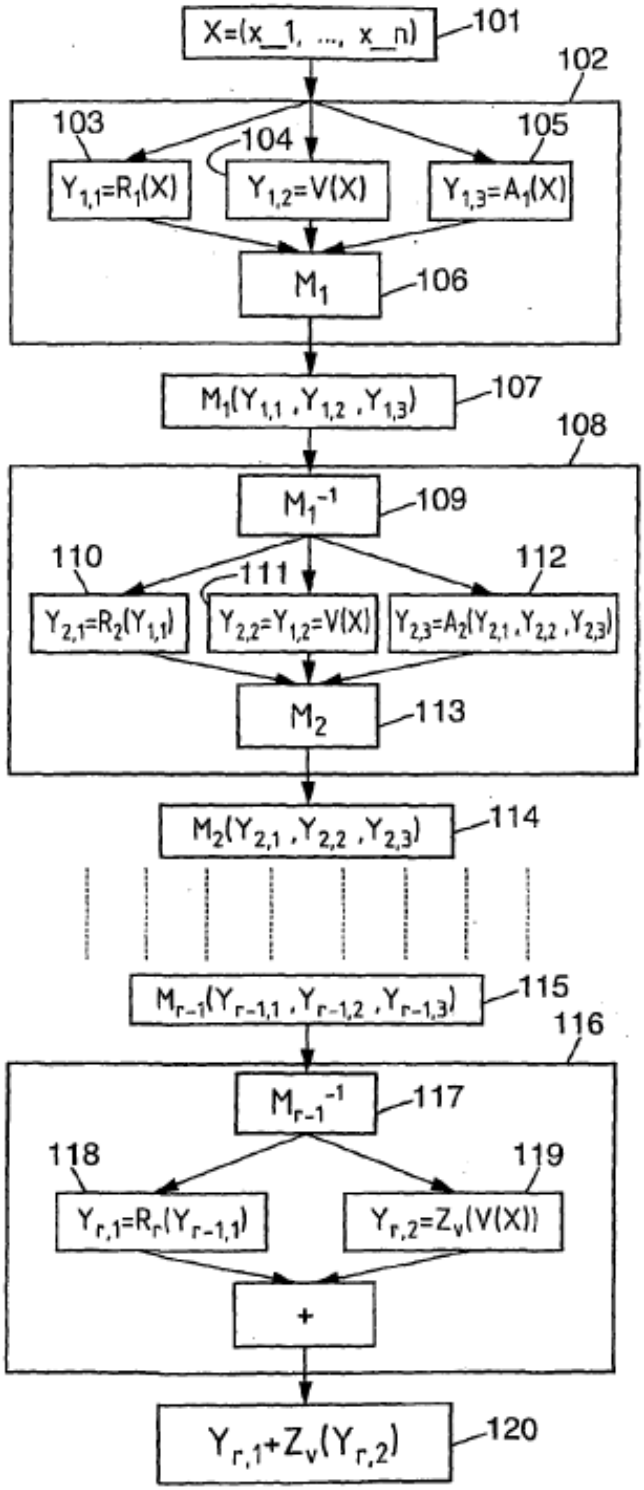
X=(x_1, ..., x_n)
101
102
103
104
105
Y1,1=R1(X)
Y1,2=V(X)
Y1,3=A1(X)
M1
106
M1(Y1,1 ,Y1,2 ,Y1,3)
107
108
M1-1
109
110
111
112
Y2,1=R2(Y1,1)
Y2,2=Y1,2=V(X)
Y2,3=A2(Y2,1 ,Y2,2 ,Y2,3)
M2
113
M2(Y2,1 ,Y2,2 ,Y2,3)
114
Mr-1(Yr-1,1 ,Yr-1,2 ,Yr-1,3)
115
116
Mr-1-1
117
118
119
Yr,1=Rr(Yr-1,1)
Yr,2=Zv(V(X))
+
Yr,1+Zv(Yr,2)
120

FIG. 2