(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 363 939**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07823400 .2**
(96) Fecha de presentación : **07.08.2007**
(97) Número de publicación de la solicitud: **2050221**
(97) Fecha de publicación de la solicitud: **22.04.2009**

(54) Título: **Procedimiento de verificación de la integridad de una clave de cifrado obtenida por combinación de partes de clave.**

(30) Prioridad: **09.08.2006 FR 06 07232**

(45) Fecha de publicación de la mención BOPI:
19.08.2011

(45) Fecha de la publicación del folleto de la patente:
19.08.2011

(73) Titular/es: **MORPHO**
Le Ponant de Paris, 27
rue Leblanc
75015 Paris, FR

(72) Inventor/es: **Pelletier, Hervé**

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

DESCRIPCIÓN

Procedimiento de verificación de la integridad de una clave de cifrado obtenida por combinación de partes de clave.

La presente invención se refiere a un procedimiento de verificación de la integridad de una clave de cifrado obtenida por combinación de partes de clave y utilizada en relación con un algoritmo de cifrado simétrico.

Antecedentes de la invención

Se sabe que un algoritmo de cifrado funciona por medio de una clave que es un elemento esencial para garantizar la seguridad del cifrado.

Se conocen diversos medios para intentar obtener fraudulentamente la clave asociada a un algoritmo de cifrado. Uno de estos medios consiste en analizar fenómenos eléctricos o electromagnéticos que se producen durante la transferencia de la clave desde una memoria muerta de almacenamiento hacia una memoria viva o desde la memoria viva hacia un registro. Para luchar contra este modo de fraude, se conoce dividir la clave en varias partes, generalmente dos partes, que son combinadas por medio de un operador, por ejemplo el operador conmutativo O EXCLUSIVO, en una zona protegida en lectura en la cual el algoritmo es puesto en práctica.

Otro medio de reconstituir la clave consiste en provocar perturbaciones en la clave y en analizar las consecuencias sobre el cifrado de un dato que es utilizado de modo repetitivo provocando perturbaciones sucesivas de la clave de cifrado. Para impedir a un defraudador efectuar perturbaciones sucesivas de la clave sería deseable verificar la integridad de la clave durante una puesta en práctica del algoritmo de cifrado. Ahora bien, la combinación de partes de clave en una zona protegida no accesible en lectura impide cualquier relectura de la clave para verificar su integridad.

Por el estado de la técnica se conoce, por ejemplo por el documento CA2327037, un método para detectar los ataques intencionados contra los algoritmos de cifrado. El citado método comprende una etapa de inicialización en el transcurso de la cual se facilitan un vector de inicialización y una clave para calcular al menos una subclave. Una función de suma de control es aplicada al vector de inicialización y a la subclave, esta suma de control es registrada para verificaciones posteriores.

Durante un cálculo de cifrado en un mensaje, se repita el cálculo de la suma de control. Se detecta entonces un ataque cuando el resultado obtenido es diferente del almacenado.

Por su parte, el documento US200401 9782 describe también un procedimiento de verificación de la integridad de un mensaje cifrado poniendo en práctica funciones de suma de control.

Objeto de la invención

Un objetivo de la invención es proponer un procedimiento que permita verificar la integridad de una clave de cifrado obtenida por una combinación en una zona protegida de varias partes de clave utilizando un operador conmutativo en relación con un algoritmo de cifrado simétrico.

Resumen de la invención

Con miras a la realización de este objetivo, se propone de acuerdo con la invención un procedimiento que comprende las etapas de efectuar por medio del operador conmutativo una primera combinación entre una parte de clave y una clave de cifrado de verificación, efectuar sucesivamente por medio del operador conmutativo una combinación entre una parte de clave no combinada todavía y un resultado de una combinación inmediatamente precedente hasta una última combinación que comprende todas las partes de clave, efectuar en la zona protegida una combinación entre la clave de cifrado que hay que verificar y la última combinación de la clave de cifrado de verificación con las partes de clave para obtener una clave final de verificación, efectuar un cifrado de un dato de verificación por medio de un algoritmo de cifrado simétrico utilizando la clave final de verificación y comparar con un cifrado de verificación obtenido por un cifrado directo del dato de verificación por medio de la clave de cifrado de verificación.

Así, cuando la clave que hay que cifrar no ha sido perturbada, la clave final de verificación es equivalente a la clave de cifrado de verificación y el cifrado del dato de verificación es entonces idéntico al cifrado de verificación. Por el contrario, si la clave de cifrado ha sido perturbada, la clave final de verificación no es equivalente a la clave de cifrado de verificación y se detecta una diferencia entre el cifrado del dato de verificación y el cifrado de verificación. Es posible entonces sacar consecuencias de esto, por ejemplo por bloqueo del algoritmo de cifrado con el fin de impedir a un defraudador proseguir la sucesión de pruebas que le permitan reconstituir la clave de cifrado.

Preferentemente, al menos una de las combinaciones que preceden a la última combinación entre las partes de clave y la clave de cifrado de verificación se efectúan fuera de la zona protegida. Se reducen así al mínimo los medios que deben ser puestos en práctica en la zona protegida.

Breve descripción de los dibujos

Otras características y ventajas de la invención se pondrán de manifiesto con la lectura de la descripción que sigue de un modo de realización preferido no limitativo de la invención, refiriéndose a la figura adjunta que ilustra de modo esquemático el procedimiento de acuerdo con la invención.

Descripción detallada de la invención

Refiriéndose a la figura, el procedimiento de acuerdo con la invención es puesto en práctica utilizando medios en sí conocidos que comprenden una memoria estática 1 tal como una EEPROM, una memoria viva 2 y un registro 3 que forma una zona protegida en lectura configurado para poner en práctica un algoritmo de cifrado simétrico (DES, TDES, AES…) utilizando una clave de cifrado K. De modo en sí conocido, la clave de cifrado K es obtenida por combinación de dos partes de clave KM y M utilizando un operador conmutativo tal como un O EXCLUSIVO que, en las ecuaciones que siguen estará indicado por (+).

A tal efecto, los valores de clave KM y M son leídos a partir de la memoria estática en la memoria viva y después transferidos a la zona protegida 3 en la cual estos son combinados según la ecuación K = KM (+) M. Se recuerda que la clave K no puede ser leída en la zona protegida 3.

De acuerdo con la invención, la memoria estática 1 contiene igualmente una clave de cifrado de verificación Kv, un dato de verificación Dv y un cifrado de verificación Cv, habiendo sido obtenido el cifrado de verificación Cv por un cifrado directo del dato de verificación por el algoritmo de cifrado utilizando la clave de cifrado de verificación. Utilizando un algoritmo DES se tiene por tanto Cv = DES (Kv, Dv).

Para provocar una perturbación de la clave K, es posible para un defraudador intervenir sobre las partes de clave KM y/o M cuando éstas están en la memoria estática o en la memoria viva.

Con el fin de verificar la integridad de la clave de cifrado K contenida en el registro 3, el procedimiento de acuerdo con la invención comprende las etapas de:

- efectuar en la memoria viva 2 una combinación entre la clave de cifrado de verificación Kv y una primera parte de clave KM. Se obtiene, así:

$$T = KM\ (+)\ Kv$$

- efectuar una segunda combinación entre el resultado obtenido de la combinación precedente y la segunda parte de clave M. En el modo de puesta en práctica descrito, se obtiene así una última combinación Mv dada por la ecuación:

$$Mv = T\ (+)\ M$$

- combinar la combinación de verificación Mv en la zona protegida 3 con la clave de cifrado K para obtener una clave final de verificación Kf dada por la ecuación:

$$Kf = K\ (+)\ Mv$$

- efectuar un cifrado del dato de verificación Dv por medio del algoritmo de cifrado simétrico DES utilizando la clave final de verificación Kf para obtener un cifrado de dato de verificación CDv tal que CDv = DES (Kf, Dv).

- comparar el cifrado de dato de verificación CDv obtenido, con el cifrado de verificación Cv extraído de la memoria estática 1.

Se observará que si se desarrolla la fórmula de la clave final de verificación, se obtiene:

$$Kf = K\ (+)\ KM\ (+)\ Kv\ (+)\ M$$

o sea, teniendo en cuenta la conmutatividad del operador O EXCLUSIVO:

$$Kf = K\ (+)\ KM\ (+)\ M\ (+)\ Kv$$

Si los datos de partida no han sido objeto de un ataque, se tiene:

$$KM\ (+)\ M = K$$

y la expresión de Kf se transforma en:

$$Kf = K\ (+)\ K\ (+)\ Kv = Kv$$

Si, por el contrario, uno de los datos ha sido perturbado, no hay identidad entre K y KM (+) M de modo que la clave final de verificación Kf es entonces diferente de la clave de cifrado de verificación Kv. El cifrado del dato de verifica-

ción Dv con la clave de cifrado final de verificación Kf da entonces un resultado CDv diferente del cifrado de verificación Cv.

Así pues, la comparación de CDv y Cv permite detectar un ataque y activar una acción defensiva, por ejemplo un bloqueo del algoritmo.

Se observará que el procedimiento de acuerdo con la invención permite, no solamente verificar la integridad de la clave de cifrado K, sino igualmente verificar cuándo se ha efectuado un ataque sobre la clave de cifrado de verificación Kv, el dato de verificación Dv o el cifrado de verificación Cv.

Aunque la detección de un ataque sobre estos datos no sea el primer objetivo de la invención, ésta, sin embargo, permite reaccionar con el fin de evitar que el ataque pase a continuación sobre los datos relativos a las partes de clave KM o M.

Naturalmente, la invención no está limitada al modo de puesta en servicio descrito y a ésta pueden aportarse variantes de realización sin salirse del marco de la invención, tal como se define por las reivindicaciones.

En particular, aunque la invención se haya descrito con una clave en dos partes solamente, el procedimiento de acuerdo con la invención puede aplicarse a una clave recombinada a partir de un número cualquiera de partes de clave utilizando un operador conmutativo y un algoritmo de cifrado simétrico.

Aunque las etapas de combinación de las partes de cifrado KM y M con la clave de verificación Kv se hayan previsto para ser realizadas en la memoria viva 2, se puede igualmente realizarlas en la zona protegida 3, pero se monopolizan entonces inútilmente los recursos de cálculo de la zona protegida 3.

REIVINDICACIONES

1. Procedimiento de verificación de la integridad de una clave de cifrado (K) obtenida por una combinación en una zona protegida (3) de al menos dos partes de claves (KM, M) utilizando un operador conmutativo, caracterizado por que comprende las etapas de efectuar por medio del operador conmutativo una primera combinación entre una parte de clave (KM) y una clave de cifrado de verificación (Kv), efectuar sucesivamente por medio del operador conmutativo una combinación entre una parte de clave no combinada todavía y un resultado de una combinación inmediatamente precedente hasta una última combinación (Mv) que comprende todas las partes de clave, efectuar en la zona protegida (3) una combinación entre la clave de cifrado (K) que hay que verificar y la última combinación (Mv) de la clave de cifrado de verificación (Kv) con las partes de clave (KM, M) para obtener una clave final de verificación (Kf), efectuar un cifrado de un dato de verificación (Dv) por medio de un algoritmo de cifrado simétrico (DES) utilizando la clave final de verificación (Kf), y comparar con un cifrado de verificación (Cv) obtenido por un cifrado directo del dato de verificación (Dv) por medio de la clave de cifrado de verificación (Kv).

2. Procedimiento de acuerdo con la reivindicación 1, caracterizado por que al menos una de las combinaciones que preceden a la última combinación (Mv) entre las partes de clave (KM, M) y la clave de verificación (Kv), se efectúan fuera de la zona protegida 3.

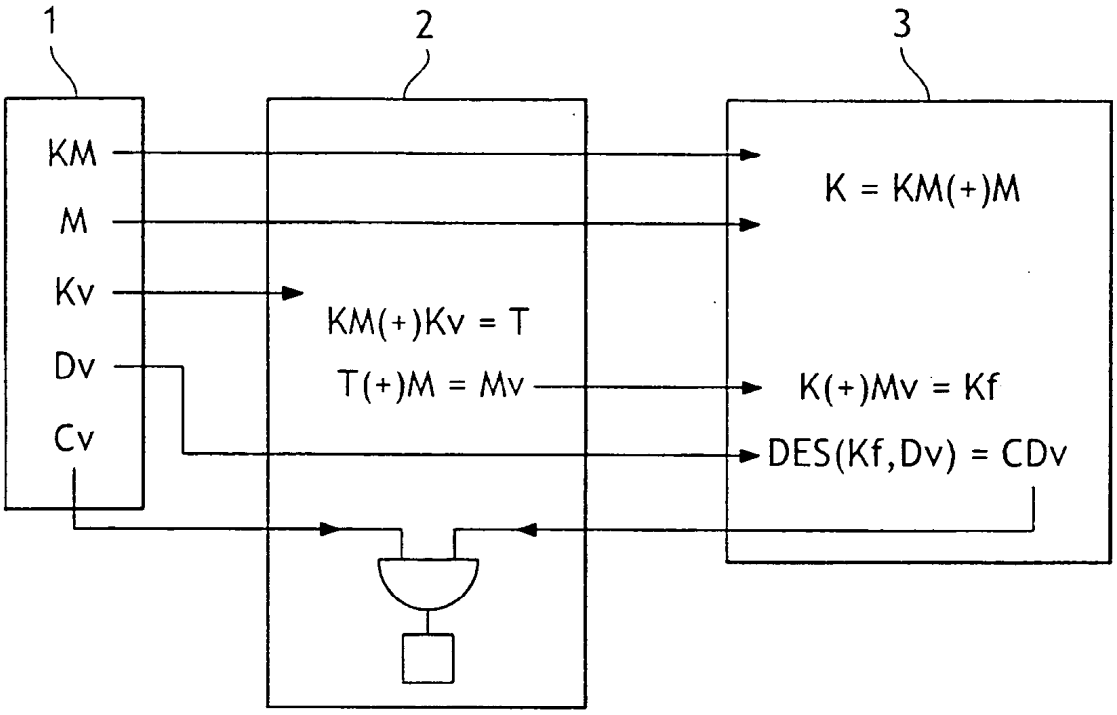

FIG.1