(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 382 615**

(51) Int. CI.:
G07F 7/10 (2006.01)
G06F 7/72 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **00990805 .4**
(96) Fecha de presentación: **20.12.2000**
(97) Número de publicación de la solicitud: **1272984**
(97) Fecha de publicación de la solicitud: **08.01.2003**

(54) Título: **Soporte de datos portátil con protección de acceso mediante enmascaramiento de mensajes**

(30) Prioridad:
28.12.1999 DE 19963407

(45) Fecha de publicación de la mención BOPI:
11.06.2012

(45) Fecha de la publicación del folleto de la patente:
11.06.2012

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

(72) Inventor/es:
DREXLER, Hermann y
VATER, Harald

(74) Agente/Representante:
Durán Moya, Luis Alfonso

DESCRIPCIÓN

Soporte de datos portátil con protección de acceso mediante enmascaramiento de mensajes

La presente invención se refiere a un soporte de datos que presenta un chip semiconductor en el que se almacenan y se procesan datos secretos.

Se utilizan para múltiples aplicaciones diferentes soportes de datos que contienen un chip, por ejemplo para realizar transacciones financieras, para pagar bienes o servicios, o como medio de identificación para llevar a cabo controles de acceso o de entrada. En todas estas aplicaciones en el interior del chip del soporte de datos se procesan generalmente datos secretos que han de ser protegidos contra el acceso por parte de terceros no autorizados. Esta protección está garantizada, entre otras cosas, por el hecho de que las estructuras internas del chip presentan dimensiones muy reducidas y, debido a ello, resulta muy difícil acceder a estas estructuras con el fin de tener acceso a los datos que son procesados en estas estructuras. Para dificultar todavía más el acceso a ellos, el chip puede estar embebido en una masa fuertemente adherida que provocará la destrucción de la plaquita semiconductora o, como mínimo, la destrucción de los datos secretos almacenados en ella cuando se intenta retirar violentamente. Asimismo, también es posible dotar la plaquita semiconductora, ya durante su producción, de una capa protectora que no puede ser eliminada sin destruir la plaquita semiconductora.

Con el correspondiente equipamiento técnico que ciertamente es muy caro pero, en principio, está disponible, un atacante podría conseguir eventualmente poner al descubierto y examinar la estructura interna del chip. La puesta al descubierto podría llevarse a cabo, por ejemplo, mediante un procedimiento de grabado especial o por un proceso de rebajado adecuado. Las estructuras del chip puestas al descubierto de esta manera tales como, por ejemplo, circuitos impresos pueden ser contactadas con microsondas o ser examinadas con otros métodos a efectos de detectar las trayectorias de señal en estas estructuras. A continuación se podría intentar averiguar, a partir de las señales detectadas, datos secretos del soporte de datos tales como, por ejemplo claves secretas, para utilizar éstas con fines de manipulación. Asimismo, se podría intentar influir de forma dirigida en las trayectorias de señal en las estructuras puestas al descubierto a través de las microsondas.

Recientemente se han dado a conocer además métodos que permiten deducir los datos secretos, especialmente la clave secreta, mediante la medición del consumo de corriente o el comportamiento en el tiempo durante la encriptación (Paul C. Kocher, “Timing Attacks on implementation of Diffie-Hellman, RSA, DSS, and other Systems”, (“Ataques de medición de tiempos en la implementación de Diffie-Hellman, RSA, DSS y otros sistemas”), edición Springer Verlag 1998; WO 99/35782).

Un ataque simple de este tipo consiste en el “Simple Power Analysis” (SPA), “(Análisis de potencia simple”). En este método analítico se procede, por ejemplo, a la encriptación de un mensaje conocido M mediante una clave secreta d, es decir, se genera el texto encriptado $Y = M^d \bmod n$. En la exponenciación modular, cuando en el exponente d haya un “1” se lleva a cabo una operación de elevación al cuadrado del resultado intermedio y una operación de multiplicación de M, mientras que cuando haya un “0” en d, sólo se lleva a cabo una operación de elevación al cuadrado del resultado intermedio. Si M es conocido, observando el comportamiento de la corriente y/o en el tiempo durante las operaciones, se podrá detectar en qué momentos se utiliza el mensaje M. Dado que éste se utiliza siempre que exista un “1” en d, se podrá deducir la clave sin más.

Este ataque puede ser contrarrestado por modificaciones en el mensaje M o en la clave d. Por Paul C. Kocher, “Timing Attacks on implementation of Diffie-Hellman, RSA, DSS, and other Systems”, (“Ataques de medición de tiempos en la implementación de Diffie-Hellman, RSA, DDS y otros sistemas”), edición Springer Verlag 1998, y en la solicitud de patente internacional WO 99/35782 se dan a conocer, sin embargo, métodos de análisis con los cuales se puede deducir la clave incluso si el mensaje ha sido modificado, es decir velado o la llave ha sido velada, mediante el registro de múltiples curvas de medición en las que se mide el comportamiento de la corriente del circuito integrado (“Differential Power Analysis” = análisis de potencia diferencial (DPA) o Higher Order DPA).

Para evitar que la clave pueda ser detectada fácilmente, reconociendo la utilización del mensaje encriptado durante el cálculo, se ha propuesto añadir un factor r * n a la encriptación del mensaje. La transformación de un algoritmo de este tipo se conoce por Messerges y otros, “Power analysis attacks of modular exponentiation in smartcards” (“Ataques mediante análisis de potencia de exponenciación modular en tarjetas inteligentes”), Cryptographic hardware and embedded systems (Hardware criptográfico y sistemas embebidos), Primer Taller Internacional, CHES’99 Worcester, MA, USA, 12-13 de agosto de 1999. Páginas 144-157. El texto encriptado $Y = M^d \bmod n$ es modificado, por lo tanto, en $(M+r*n)^d \bmod n$. De esta manera, al hacer el análisis no existe la posibilidad de recurrir al mensaje conocido M. Pero incluso con esta modificación del texto del mensaje M se puede reconocer una repetición de determinados patrones, observando la curva de la corriente. Estos patrones correlacionados contienen muy probablemente (M+r*n), de manera que, una vez más, se puede deducir la multiplicación y, por lo tanto, un 1 en la clave secreta.

Otro problema se presenta cuando durante el análisis de la corriente se puede reconocer si en una multiplicación se multiplican factores idénticos (corresponde a la operación de elevación al cuadrado del resultado intermedio) o

diferentes (corresponde a la operación de multiplicación del resultado intermedio con mensaje), ya que con ello también se pueden identificar multiplicaciones con (M + r*n).

El objetivo de la invención consiste en proteger datos secretos que se encuentran en un soporte de datos portátil contra accesos no autorizados, siguiendo asegurando la utilización eficaz de los datos.

Este objetivo se consigue partiendo de la parte introductoria de las reivindicaciones 1 ó 6 por las características de cada reivindicación.

La invención parte de un soporte de datos con un chip semiconductor que presenta, como mínimo, una memoria en la que está depositado un programa operativo que contiene varias órdenes provocando cada orden señales detectables desde el exterior del chip semiconductor.

De acuerdo con la invención, el soporte de datos está diseñado de tal manera que los datos que son utilizados varias veces para un cálculo son enmascarados mediante diferentes funciones, consistiendo los datos a enmascarar en el mensaje M a encriptar y sumando al mensaje M en cada utilización i (i=1..k) r_i*n, donde r_i es un número aleatorio que puede tener un valor diferente para cada i, y n es el módulo.

Los datos pueden ser un mensaje, pero también pueden ser resultados intermedios que se han generado al realizar un cálculo, o también datos que están almacenados en el soporte de datos.

También se puede prever que los datos sean un resultado intermedio y una subsiguiente operación de elevación al cuadrado se lleve a cabo como una multiplicación, siendo el resultado intermedio enmascarado previamente mediante diferentes funciones, o que los datos sean un resultado intermedio y una subsiguiente multiplicación por dos del resultado intermedio se lleve a cabo como una adición, siendo el resultado intermedio enmascarado previamente mediante diferentes funciones. De esta manera, se pueden asegurar también ventajosamente operaciones con el resultado intermedio (elevación al cuadrado, adición, etc.).

En especial se prevé que el enmascaramiento de la función sea una encriptación mediante operaciones de módulo en la que se utiliza el mensaje M cuando hay un “1” en el exponente d, y en la que el mensaje M es modificado con una función diferente cada vez que se utiliza.

Según una realización ventajosa de la invención, también pueden aparecer varias veces potencias en el mensaje M a las que se suma con cada utilización r_i*n.

Se podrá aumentar todavía más la seguridad si el módulo n es multiplicado con un factor constante k y sólo más tarde se realiza otra operación de módulo con el módulo n, ya que entonces los resultados intermedios también están enmascarados.

A continuación se describirá la invención por medio de un ejemplo de realización para la exponenciación modular. Sin limitar la generalidad se parte del hecho de que la exponenciación modular se calcula para generar un mensaje encriptado $Y = M^d \bmod n$, llevando a cabo una operación de elevación al cuadrado del resultado intermedio, así como una multiplicación del mensaje M cuando hay un “1” en d, y una operación de elevación al cuadrado del resultado intermedio cuando hay un “0”.

De acuerdo con la invención, para la encriptación primero se elige un número aleatorio r y se forma el producto r*n. A continuación empieza la exponenciación con una operación de elevación al cuadrado en la que se suma el producto r*n al resultado intermedio Z, a efectos de calcular la expresión (Z*(Z+r*n) mod k*n) en lugar de Z*Z mod n, donde k es un número entero. En el caso de que el exponente, es decir la clave secreta d, contiene un “1” en el dígito, se seguirá con una operación de multiplicación para la cual se añade primero (r_i*n) al mensaje M, es decir se forma M + r_i*n, y en lugar de Z*M mod n se calcula (Z*(M + r_i*n) mod k*n)). Se pasará tantas veces como sea necesario por este bucle hasta que todos los dígitos de la clave secreta hayan sido trabajados, aumentando i en 1 en cada una de las multiplicaciones subsiguientes. Una vez terminada la exponenciación, el resultado se reduce a mod n.

Debido a la característica de que el resultado no es modificado por la adición de un múltiple entero del módulo al mensaje M, se puede introducir sin más una ampliación de este tipo y se obtiene la ventaja de que mediante un análisis del comportamiento de la corriente del chip, el mensaje M ya no es detectable, dado que los sucesivos procesamientos del mensaje ya no son correlacionados y, por lo tanto, no se puede reconocer ningún patrón idéntico que se repita.

Además, resulta prácticamente imposible diferenciar mediante un análisis una operación de multiplicación de una operación de elevación al cuadrado, ya que tanto los resultados intermedios Z, como también el mensaje procesado M + r_i*n son modificados en cada operación y, por lo tanto, se forma un producto del resultado intermedio y de un factor no correlacionado con respecto al mismo, tanto en una operación de multiplicación como también en una operación de elevación al cuadrado.

Se podrá aumentar todavía más la seguridad si las operaciones de cálculo críticas para la seguridad f(z) que poseen una correlación entre z y f(z) son divididas en operaciones de cálculo g1(z) y (g2 f(g1(z)) de manera que g1(z) y g2 f(g1(z)) no están correlacionados entre sí. En esta caso, g1(z) y g2(z) son funciones de enmascaramiento adecuadas.

REIVINDICACIONES

1. Soporte de datos con un chip semiconductor que presenta al menos una memoria en la que está depositada un programa operativo que contiene varias órdenes, provocando cada orden señales detectables desde el exterior del chip semiconductor, y estando el soporte de datos diseñado de tal manera que los datos que son utilizados varias veces para un cálculo en una encriptación con operaciones de módulo son enmascarados mediante diferentes funciones, consistiendo los datos a enmascarar en el mensaje M a encriptar, **caracterizado porque** al mensaje M se suma en cada utilización i (i=1..k) r_i*n, donde r_i es un número aleatorio que puede tener un valor diferente para cada i, y n es el módulo.

2. Soporte de datos, según la reivindicación 1, **caracterizado porque** los datos utilizados son un resultado intermedio y una subsiguiente operación de elevación al cuadrado se lleva a cabo como una multiplicación, siendo el resultado intermedio enmascarado previamente mediante diferentes funciones.

3. Soporte de datos, según la reivindicación 1, **caracterizado porque** los datos utilizados son un resultado intermedio y una subsiguiente multiplicación por dos del resultado intermedio se lleva a cabo como una adición, siendo el resultado intermedio enmascarado previamente mediante diferentes funciones.

4. Soporte de datos, según la reivindicación 1, **caracterizado porque** el cálculo consiste en una operación de módulo en la que se utilizan las potencias del mensaje, siendo estas potencias modificadas con una función diferente en cada utilización, sumando al mensaje M en cada utilización i (i=1..k) r_i*n, donde r_i es un número aleatorio que puede tener un valor diferente para cada i, y n es el módulo.

5. Soporte de datos, según una de las reivindicaciones anteriores, **caracterizado porque** el módulo n es multiplicado por un factor constante k y porque se realiza otra operación de módulo con el módulo n.

6. Procedimiento para la protección de datos secretos en soportes de datos en un chip semiconductor que presenta al menos una memoria en la que está depositada un programa operativo que contiene varias órdenes, provocando cada orden señales detectables desde el exterior del chip semiconductor, en el que los datos que son utilizados varias veces para un cálculo en una encriptación con operaciones de módulo son enmascarados mediante diferentes funciones y los datos a enmascarar consisten en el mensaje M a encriptar, **caracterizado porque** al mensaje M se suma en cada utilización i (i=1..k) r_i*n, donde r_i es un número aleatorio que puede tener un valor diferente para cada i, y n es el módulo.

7. Procedimiento, según la reivindicación 6, **caracterizado porque** los datos utilizados son un resultado intermedio y una subsiguiente operación de elevación al cuadrado se lleva a cabo como una multiplicación, siendo el resultado intermedio enmascarado previamente mediante diferentes funciones.

8. Procedimiento, según la reivindicación 6, **caracterizado porque** los datos utilizados son un resultado intermedio y una subsiguiente multiplicación por dos del resultado intermedio se lleva a cabo como una adición, siendo el resultado intermedio enmascarado previamente mediante diferentes funciones, sumando al mensaje M en cada utilización i (i=1..k) r_i*n, donde r_i es un número aleatorio que puede tener un valor diferente para cada i, y n es el módulo.

9. Procedimiento, según una de las reivindicaciones 6 a 8, **caracterizado porque** el cálculo consiste en una operación de módulo en la que se utilizan las potencias del mensaje, siendo estas potencias modificadas con una función diferente en cada utilización.

10. Procedimiento, según una de las reivindicaciones 6 a 9, **caracterizado porque** el módulo n es multiplicado por un factor constante k y porque se realiza otra operación de módulo con el módulo n.

11. Procedimiento, según una de las reivindicaciones 6 a 10, **caracterizado porque** operaciones de cálculo críticas para la seguridad f(z) que poseen una correlación entre z y f(z) son divididas en operaciones de cálculo g1(z) y (g2 f(g1(z)) de manera que g1(z) y g2 f(g1(z)) no están correlacionados entre sí.