(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 421 724**

(51) Int. CI.:

H04L 9/06 (2006.01)
G06F 7/00 (2006.01)
G06K 19/073 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.01.2001 E 01400228 (1)**

(97) Fecha y número de publicación de la concesión europea: **17.04.2013 EP 1122909**

(54) Título: **Procedimiento de ejecución de un protocolo criptográfico entre dos entidades electrónicas**

(30) Prioridad:

31.01.2000 FR 0001199

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.09.2013

(73) Titular/es:

OBERTHUR TECHNOLOGIES (100.0%)
50 quai Michelet
92300 Levallois-Perret , FR

(72) Inventor/es:

AKKAR, MEHDI-LAURENT y
DISCHAMP, PAUL

(74) Agente/Representante:

PÉREZ BARQUÍN, Eliana

DESCRIPCIÓN

Procedimiento de ejecución de un protocolo criptográfico entre dos entidades electrónicas

La invención se refiere a un procedimiento de ejecución de un protocolo criptográfico entre dos entidades electrónicas, siendo una de ellas por ejemplo, pero no exclusivamente, una tarjeta de microprocesador. La invención se refiere más particularmente a un perfeccionamiento de dicho protocolo para prevenir los “ataques”, es decir los intentos de fraude basados en el análisis del material en funcionamiento, particularmente por el sesgo de medidas del consumo de corriente durante la ejecución de tal protocolo criptográfico provocado por un estafador.

Se sabe que ciertas entidades electrónicas encriptadas, particularmente las tarjetas de microcircuitos, son vulnerables a ciertos ataques basados en el análisis de ciertos parámetros durante una fase de funcionamiento. Se dice que las informaciones pueden “escaparse” a partir de un cálculo hecho en la tarjeta, típicamente la ejecución de un protocolo criptográfico provocado por el estafador en posesión de la tarjeta. Los parámetros analizados durante la ejecución de tal protocolo pueden ser, típicamente, diferencias de tiempo de cálculo o radiaciones electromagnéticas durante la ejecución del cálculo pero sobre todo el consumo de corriente de la entidad electrónica de la cual se busca forzar el código.

Así, el ataque clásico consiste en hacer ejecutar, por la entidad electrónica que cae en posesión del estafador, un cierto número de protocoles criptográficos basados en unos mensajes cualquiera, destinados por lo tanto al fracaso, pero que tienen por consecuencia hacer ejecutar cada vez, por la entidad (la tarjeta de microcircuito), una cadena de operaciones conocida con la abreviatura DES (*Data Encryption Standard*) analizando a la vez el consumo de corriente en cada ejecución de dicho DES. El objeto de este ataque es encontrar la clave secreta de dicha entidad. El DES es, por su parte, un algoritmo bien conocido, muy ampliamente utilizado actualmente en el campo de las tarjetas bancarias o en de las tarjetas de control de acceso.

A título de ejemplo, en el marco de una autentificación normal entre una entidad A, por ejemplo un servidor, y una entidad B, por ejemplo una tarjeta de microcircuito en el que el DES se encuentra programado, los intercambios de informaciones entre las dos entidades son los siguientes:

- el servidor A solicita a la tarjeta B que envía un mensaje, suponiendo que A y B estén en posesión de la misma clave;

- B envía un mensaje cualquiera y lo guarda en la memoria;

- A aplica el DES al mensaje utilizando su clave y reenvía el resultado a la tarjeta B.

- Paralelamente, la tarjeta B aplica el DES al mensaje A haciendo uso de su propia clave. Esta obtiene un resultado que es comparado al que ha sido elaborado por el servidor A. Si los dos resultados son idénticos, la autentificación es validada.

Por otro lado, en el caso de un fraude, es decir en el caso de que el estafador disponga de la tarjeta y busque determinar la clave, puede conectar la tarjeta a un lector por el que podrá transmitirle mensajes y unirla a unos medios de registro del consumo de corriente durante la ejecución de las operaciones que efectúe.

A partir de estos medios simples, el estafador constituye un sistema F que conecta la tarjeta al sitio del servidor A.

El proceso es entonces el siguiente. F solicita un mensaje a la tarjeta exactamente como en el caso de iniciación de una autentificación. B envía este mensaje. F envía a B otro mensaje que representa supuestamente el resultado del tratamiento por el DES del mensaje enviado por B. Por supuesto, este mensaje es erróneo. No obstante, B hace intervenir su propia clave para ejecutar un DES con el fin de obtener un resultado, con el fin de compararlo con el mensaje (erróneo) enviado por F. El resultado de esta comparación es forzosamente negativo pero el estafador ha conseguido provocar la ejecución de un DES por B. Durante la ejecución de dicho DES, el consumo de corriente es detectado y memorizado.

Si F está en condiciones de hacer efectuar un cierto número de DES, en las mismas condiciones, por la tarjeta B, y memorizar cada vez los consumos de corriente, es posible poner en marcha un ataque cuyo principio es conocido. Este ataque llamado DPA (*Differential Power Analysis*) permite reconstituir la clave secreta de la entidad B.

El documento WO 99/63696 se refiere a oponerse a ataques de este tipo reduciendo las informaciones explotables susceptibles de “escaparse” durante la ejecución de algoritmos. Para hacer esto, sugiere particularmente introducir riesgos en los protocolos criptográficos con el fin de aumentar el número de ciclos necesarios para encontrar la clave secreta.

La patente neerlandesa NL1011800 C describe la protección de una clave secreta durante la ejecución de un procedimiento criptográfico en un circuito integrado. La ejecución del procedimiento criptográfico es una cadena de

operaciones. La protección es realizada porque la clave, los datos de entrada y/o los datos intermedios son enmascarados por datos aleatorios.

La invención propone una parada precisa a un ataque del género DPA por complementación aleatoria de ciertas operaciones del DES.

La invención se aplica particularmente a las entidades que utilizan los DES pero es aplicable también, como se verá más adelante, a otras entidades (tarjetas de microcircuitos) que utilizan algoritmos distintos al DES con tal de que estén constituidos por una sucesión de operaciones que poseen ciertas propiedades que serán explicitadas más adelante.

Más precisamente, la invención se refiere a un procedimiento de elaboración de un protocolo criptográfico entre una primera entidad electrónica y una segunda entidad electrónica susceptible de ataque, según el cual es elaborado un mensaje cualquiera, a partir del cual una cadena de operaciones es efectuada por dicha segunda entidad, dando como resultado la elaboración de un mensaje resultante o respuesta, siendo comparada dicha respuesta con el resultado de otro tratamiento parecido aplicado a dicho mensaje y efectuado por dicha primera entidad, caracterizado porque, al menos en ciertas etapas de dicha cadena de operaciones, dicha segunda entidad efectúa, ya sea una operación de un tipo elegido, ya sea la misma operación complementada, dependiendo la elección de una decisión aleatoria, y porque dicha respuesta está constituida por el resultado de la última operación de dicha cadena, eventualmente complementada.

La complementación puede ser realizada ya sea octeto por octeto, haciendo el O exclusivo del octeto corriente aleatoriamente con uno de los dos valores hexadecimales 00 y FF, ya sea bit a bit, tratando juntos los ocho bits consecutivos del octeto actual y haciendo el O exclusivo con un número elegido aleatoriamente, en cada octeto tratado, entre los 256 valores hexadecimales comprendidos entre 00 y FF.

Entre las operaciones susceptibles de ser complementadas, se puede citar la operación llamada de O exclusivo o incluso una operación de permutación de los bits del mensaje o de un resultado intermedio obtenido efectuando dicha cadena de operaciones, es decir, según el ejemplo descrito, después de la ejecución de una operación dada del DES. Se puede citar incluso la operación de acceso indexado en una tabla o cualquier operación estable en relación con la aplicación de la función O exclusivo, particularmente la operación que consiste en transferir el mensaje o un resultado intermedio precitado, de un emplazamiento a otro, desde un espacio de memorización.

Según un modo de realización posible, se definen en dicha segunda entidad dos cadenas de operaciones para el tratamiento de dicho mensaje, estando constituida una de las cadenas por una sucesión de operaciones dadas y estando constituida la otra cadena por una sucesión de las mismas operaciones complementadas y por una complementación final, y se decide de forma aleatoria ejecutar una de las dos cadenas de operaciones con cada recepción de un mensaje que proviene de dicha primera entidad.

Según otro modo de realización, actualmente juzgado preferible, el procedimiento consiste en utilizar dicho mensaje o un resultado intermedio resultante de la ejecución de una operación precedente de dicha cadena, para aplicarle una nueva operación de dicha cadena, o esta misma operación complementada, en función del estado de un parámetro aleatorio asociado a esta nueva operación, para poner al día un contador de complementaciones y para tener en cuenta el estado de este contador con el fin de la ejecución de dicha cadena de operaciones para decidir la configuración final de dicha respuesta.

Según otra variante ventajosa más, el procedimiento consiste en utilizar dicho mensaje o un resultado intermedio resultante de la ejecución de una operación precedente de dicha cadena, para aplicarle una nueva operación de dicha cadena o esta misma operación complementada, en función del estado de un parámetro aleatorio asociado a esta nueva operación y para transmitir de operación en operación, informaciones que forman parte de dichos resultados intermedios, relativos a la configuración final de dicha respuesta.

Por otro lado, se ha encontrado que la diferencia entre el número de veces que las operaciones son efectuadas de forma normal y el número de veces que son efectuadas con complementación, durante la ejecución del DES o análogo, no debe ser demasiado importante para que el procedimiento conserve todas su eficacia frente al ataque descrito anteriormente. Por consiguiente, el procedimiento es también notable por el hecho de que, mientras se efectúa dicha serie de operaciones, se calcula la diferencia entre el número de veces en que las operaciones han sido efectuadas de forma normal y el número de veces en las que han sido efectuadas con complementación y porque se suprime el riesgo en la decisión de efectuar operaciones de forma normal o complementaria, para cierto número de operaciones subsiguientes, cuando dicha diferencia sobrepasa un valor predeterminado, con el fin de reducir dicha diferencia.

La invención se comprenderá mejor y otras ventajas de la misma aparecerán más claramente a la luz de la descripción que va a seguir, de un procedimiento de ejecución de un protocolo criptográfico conforme a su principio, dada únicamente a título de ejemplo y hecha en referencia a los dibujos adjuntos en los que:

- la figura 1 es un esquema que ilustra una parte de la ejecución de un protocolo criptográfico, más precisamente la ejecución de un DES programado según la invención; y

- la figura 2 es un esquema que ilustra otra forma de ejecutar el DES conforme a la invención.

Considerando más particularmente la figura 1, se señala que el procedimiento de elaboración de un protocolo criptográfico entre dos entidades electrónicas A y B, que está ilustrado parcialmente en el esquema, puede ser ejecutado en una de estas entidades, típicamente en una tarjeta de microprocesador B, mientras está conectada, por ejemplo, a un servidor A. El DES conforme a la invención está programado en la tarjeta de microprocesador B. Esta contiene igualmente en la memoria una clave secreta K que es susceptible de intervenir en ciertas de las operaciones O_1, O_2, O_3…O_n que se encadenan durante la ejecución del DES. Durante la elaboración del protocolo criptográfico, la primera entidad (típicamente el servidor A precitado) solicita a la segunda entidad (la tarjeta B) enviar un mensaje M. El mensaje generado por B es cualquiera; es guardado en memoria en la tarjeta B. Mientras que A trata este mensaje con su propio DES, la tarjeta B aplica el DES conforme a la invención al mensaje M que ha enviado al servidor A, haciendo uso de su propia clave K. En el ejemplo, el DES aplicado en la tarjeta B comprende dos cadenas de operaciones. Una primera cadena Ch_1 de operaciones O_1, O_2, O_3…O_n corresponde a un DES clásico. La segunda cadena Ch_2 de operaciones $\overline{O}_1$, $\overline{O}_2$, $\overline{O}_3$,… $\overline{O}_n$ está constituida por la misma sucesión de las mismas operaciones, pero complementadas. Acaba por una complementación global C del resultado elaborado al final de la última operación complementada $\overline{O}_n$.

Además, se decide de forma aleatoria ejecutar una u otra de las dos cadenas de operaciones en cada elaboración de un mensaje cualquiera precitado. Esta elección aleatoria es simbolizada por un selector S_a interpuesto entre el mensaje M y cada una de las dos cadenas de operación. El posicionamiento del selector es aleatorio, lo que significa que cada vez que ser debe tratar un mensaje M, una u otra de las dos cadenas de operaciones Ch_1, Ch_2 es elegida de forma aleatoria.

Si ha sido elegida la cadena no complementada, el resultado dado por la última operación O_n constituye la respuesta R que será comparada a la que habrá elaborado el servidor A. En caso de que haya sido seleccionada la cadena de operaciones complementadas, el resultado de la última operación $\overline{O}_n$ es complementado y constituye la respuesta R.

En el modo de realización de la figura 2, se encuentra un DES programado conforme al principio de la invención, es decir que comprende las operaciones habituales de un DES: O_1, O_2, O_3… O_n o las operaciones semejantes complementadas $\overline{O}_1$, $\overline{O}_2$, $\overline{O}_3$,… $\overline{O}_n$. El mensaje mismo puede ser complementado, es decir utilizado tal cual al principio de la ejecución del DES o en forma complementada $\overline{M}$. La clave K interviene para la ejecución de ciertas operaciones al menos. No obstante, la selección de las operaciones (es decir, la elección entre la operación normal o su versión complementada) es decidida de forma aleatoria de una operación a otra. Dicho de otro modo, se utiliza el mensaje M o un resultado intermedio que resulta de la ejecución de una operación precedente O_i (o $\overline{O}_i$), se le aplica una nueva operación de la cadena o su versión complementada (es decir, O_{i+1} o $\overline{O}_{i+1}$) en función del estado de un parámetro aleatorio asociado a la nueva operación. Este parámetro aleatorio es elaborado por el selector S'_a. Así, siguiendo la trayectoria de la figura 2, se ve que es el mensaje M, tal cual, el que es utilizado, y no su complemento $\overline{M}$ (comando 1 generado por S'_a), que es la operación $\overline{O}_1$ la que es seleccionada (comando 2) y después la operación $\overline{O}_2$ (comando 3), y después la operación O_3 (comando 4) y que al final desemboca en la selección de la operación $\overline{O}_n$ (comando n). El resultado de la última operación, en lo que ocurre aquí $\overline{O}_n$, puede constituir el resultado R o el resultado $\underline{R}$ complementado que será comparado con otro resultado elaborado por la entidad A por puesta en marcha de su propio DES. La elección entre R y $\overline{R}$ viene dada por el estado de un contador de complementación C_c alimentado a todo lo largo de la elaboración del proceso por el selector S'_a. Dicho de otro modo, el estado del contador de complementación C_c permite saber si debe validar el resultado R o su complemento $\overline{R}$ para la configuración final de la respuesta para comparar con los cálculos de la entidad A.

Hay que señalar que una variante permite suprimir el contador C_c. Basta con transmitir, de operación en operación, informaciones que forman parte de los resultados intermedios y que representan el número de veces que una operación del DES ha sido ejecutada en forma complementada. En este caso, los resultados intermedios transmitidos de una operación a la otra comprenden ellos mismos la información equivalente a la que da al final el contador C_c en el modo de realización de la figura 2. En este caso, el último resultado intermedio dado por la ejecución de la operación O_n u $\overline{O}_n$ es o no complementado en función de una parte de las informaciones propias que contiene. Se deduce de ello la configuración final de la respuesta R.

Volviendo a la figura 1 ó 2, se señala que el selector S_a o S'_a se aprovecha para calcular la diferencia entre el número de veces que las operaciones han sido efectuadas de forma normal y el número de veces que han sido efectuadas con complementación. Esta diferencia $\underline{d}$ es memorizada y actualizada de operación en operación.

Cuando la diferencia sobrepasa un valor predeterminado, lo que puede reducir la eficacia del procedimiento frente al ataque DPA, se genera un orden que inhibe momentáneamente el selector S'_a. Dicho de otro modo, se suprime el riesgo en la decisión de efectuar operaciones de forma normal o complementada, para ejecutar un cierto número de operaciones subsiguientes en el modo (normal o complementado) menos utilizado hasta ahí. El riesgo se vuelve a poner en marcha cuando el valor de la diferencia d se ha reducido suficientemente.

Se encuentra que todas las operaciones de un DES clásico permiten la puesta en marcha del procedimiento según una u otra de las variantes que acaban de ser descritas.

A título de ejemplo, se van a mencionar más adelante ciertas operaciones susceptibles de ser complementadas y por consiguiente compatibles con la puesta en marcha del procedimiento que acaba de ser descrito.

Una operación susceptible de ser complementada es la operación llamada de O exclusivo.

Otra operación susceptible de ser complementada es una operación conocida de permutación de los bits del mensaje M o de un resultado intermedio obtenido efectuando la cadena de operaciones. Para las permutaciones (simples, compresivas o expansivas), se almacenará ventajosamente la máscara permutada en la memoria.

Otra operación susceptible de ser complementada es la operación llamada de acceso indexado a una tabla.

Otra operación susceptible de ser complementada es la transferencia del mensaje, o de un resultado intermedio obtenido efectuando una operación de la cadena, de un emplazamiento a otro de un espacio de memorización definido en la entidad B. Prácticamente, se aplica de manera aleatoria una máscara mediante O exclusivo al dato transferido.

Más generalmente, una operación susceptible de ser complementada es una operación estable con respecto a la aplicación de la función o exclusiva, es decir tal que:

$$\forall (x, y): f(x \oplus y) = f(x) \oplus f(y)$$

Este es el caso, entre otros, de las permutaciones y de la transferencia de datos.

Como se mencionó precedentemente, un DES clásico se compone de operaciones que responden a los criterios definidos anteriormente pero la invención se aplica también a todo algoritmo que cumple las condiciones enunciadas anteriormente.

Otras operaciones de carácter aleatorio pueden ser combinadas con las que definen el procedimiento descrito anteriormente. Particularmente, cuando varias operaciones consecutivas de la cadena son conmutativas, se puede permutar la orden de su ejecución, de forma aleatoria.

REIVINDICACIONES

1.- Procedimiento de elaboración de un protocolo criptográfico entre una primera entidad electrónica (A) y una segunda entidad electrónica (B) susceptible de ataque, según el cual se elabora un mensaje cualquiera (M), a partir del cual es efectuada una cadena de operaciones por dicha segunda entidad, desembocando en la elaboración de un mensaje resultante o respuesta (R), siendo comparada dicha respuesta con el resultado de otro tratamiento semejante aplicado al mensaje y efectuado por dicha primera entidad, caracterizado porque, al menos en ciertas etapas de dicha cadena de operaciones, dicha segunda entidad efectúa, ya sea una operación de un tipo elegido (O_1, O_2, O_3…O_n), ya sea la misma operación complementada ($\overline{O}_1$, $\overline{O}_2$, $\overline{O}_3$,… $\overline{O}_n$), dependiendo la elección de una decisión aleatoria, y porque dicha respuesta está constituida por el resultado de la última operación ($\overline{O}_n$) de dicha cadena, eventualmente complementada.

2.- Procedimiento según la reivindicación 1, caracterizado porque una operación susceptible de ser complementada es la operación llamada de O exclusivo.

3.- Procedimiento según la reivindicación 1 ó 2, caracterizado porque una operación susceptible de ser complementada es una operación de permutación de los bits de dicho mensaje o de un resultado intermedio obtenido efectuando dicha cadena de operaciones.

4.- Procedimiento según una de las reivindicaciones 1 a 3, caracterizado porque una operación susceptible de ser complementada es una operación de acceso indexado a una tabla.

5.- Procedimiento según una de las reivindicaciones 1 a 4, caracterizado porque una operación susceptible de ser complementada es una operación estable con respecto a la aplicación de la función O exclusivo.

6.- Procedimiento según la reivindicación 5, caracterizado porque una operación susceptible de ser complementada es la transferencia de dicho mensaje o de un resultado intermedio obtenido efectuando una operación de dicha cadena, de un emplazamiento a otro de un espacio de memorización.

7.- Procedimiento según una de las reivindicaciones precedentes, caracterizado porque consiste en utilizar dicho mensaje, o un resultado intermedio resultante de la ejecución de una operación precedente de dicha cadena, para aplicarle una nueva operación de dicha cadena, o esta misma operación complementada, en función del estado de un parámetro aleatorio (S'_a) asociado a esta nueva operación, para poner al día un contador de complementaciones (C_c) y para tener en cuenta el estado de este contador al final de la ejecución de dicha cadena de operaciones para decidir la configuración final de dicha respuesta.

8.- Procedimiento según una de las reivindicaciones 1 a 6, caracterizado porque consiste en utilizar dicho mensaje, o un resultado intermedio resultante de la ejecución de una operación precedente de dicha cadena, para aplicarle una nueva operación y para transmitir, de operación en operación, informaciones que forman parte de dichos resultados intermedios, necesarios para la configuración final de dicha respuesta.

9.- Procedimiento según una de las reivindicaciones 1 a 6, caracterizado porque se definen en dicha segunda entidad dos cadenas de operaciones (CH_1, CH_2) para el tratamiento de dicho mensaje, estando constituida una de las cadenas por una sucesión de operaciones dada y estando constituida la otra cadena por una sucesión de las mismas operaciones complementadas y de una complementación final (C), y porque se decide de forma aleatoria ejecutar una de las dos cadenas de operaciones en cada elaboración de un mensaje precitado.

10.- Procedimiento según una de las reivindicaciones precedentes, caracterizado porque, mientras que se efectúa dicha serie de operaciones, se calcula la diferencia (d) entre el número de veces que las operaciones han sido efectuadas de forma normal y el número de veces que han sido efectuadas con complementación, y porque se suprime el riesgo (S'_a) en la decisión de efectuar operaciones de forma normal o complementada, para ejecutar un cierto número de operaciones subsiguientes, cuando dicha diferencia sobrepasa un valor predeterminado en el modo (normal o complementario) menos utilizado hasta ahí, con vistas a reducir suficientemente dicha diferencia.

11.- Procedimiento según una de las reivindicaciones precedentes, caracterizado porque la complementación se efectúa octeto por octeto.

12.- Procedimiento según una de las reivindicaciones 1 a 10, caracterizado porque la complementación se efectúa bit a bit.

13.- Procedimiento según una de las reivindicaciones precedentes, caracterizado porque, cuando varias operaciones consecutivas de dicha cadena son conmutativas, se permuta el orden de su ejecución, de forma aleatoria.

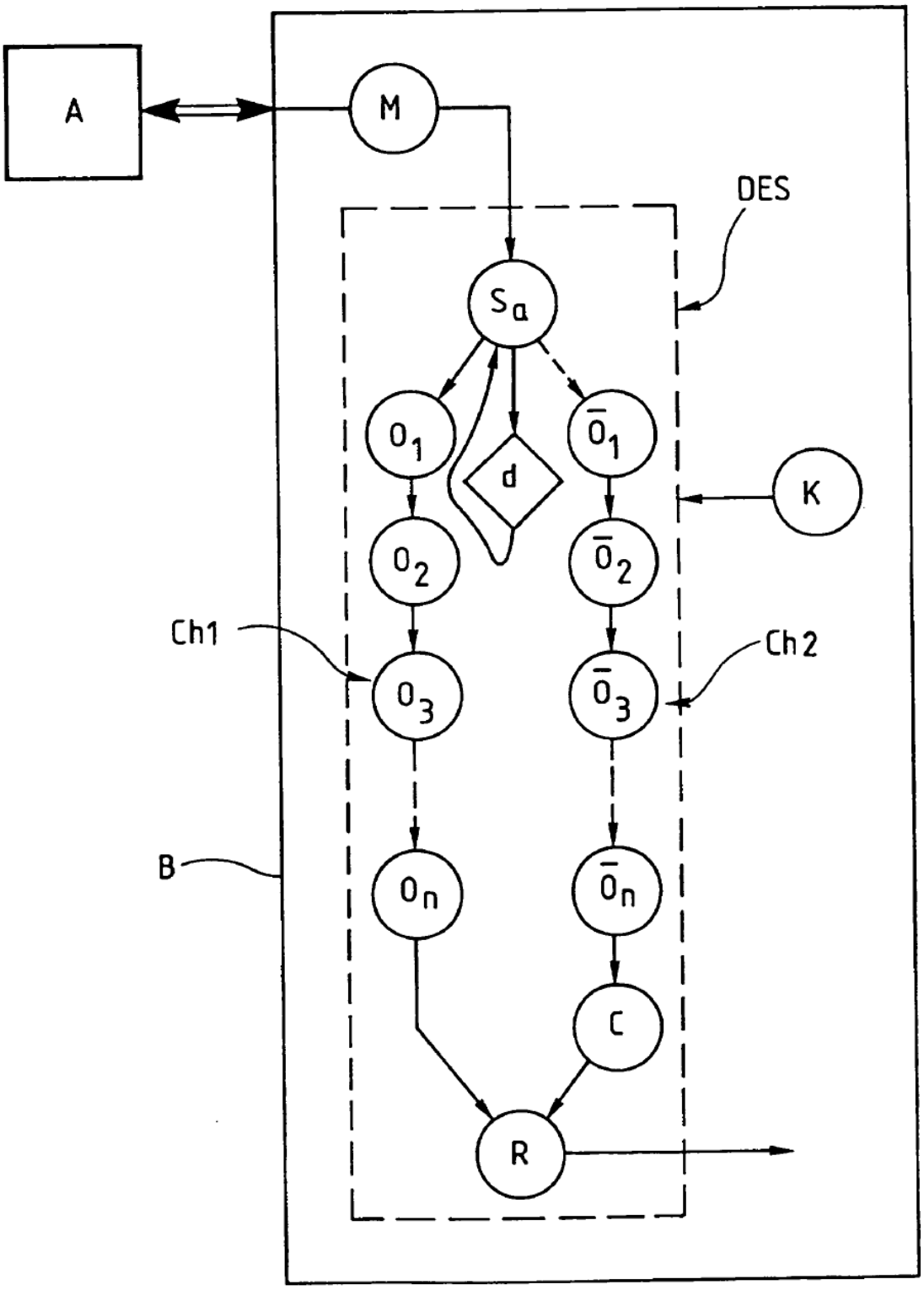

Fig.1

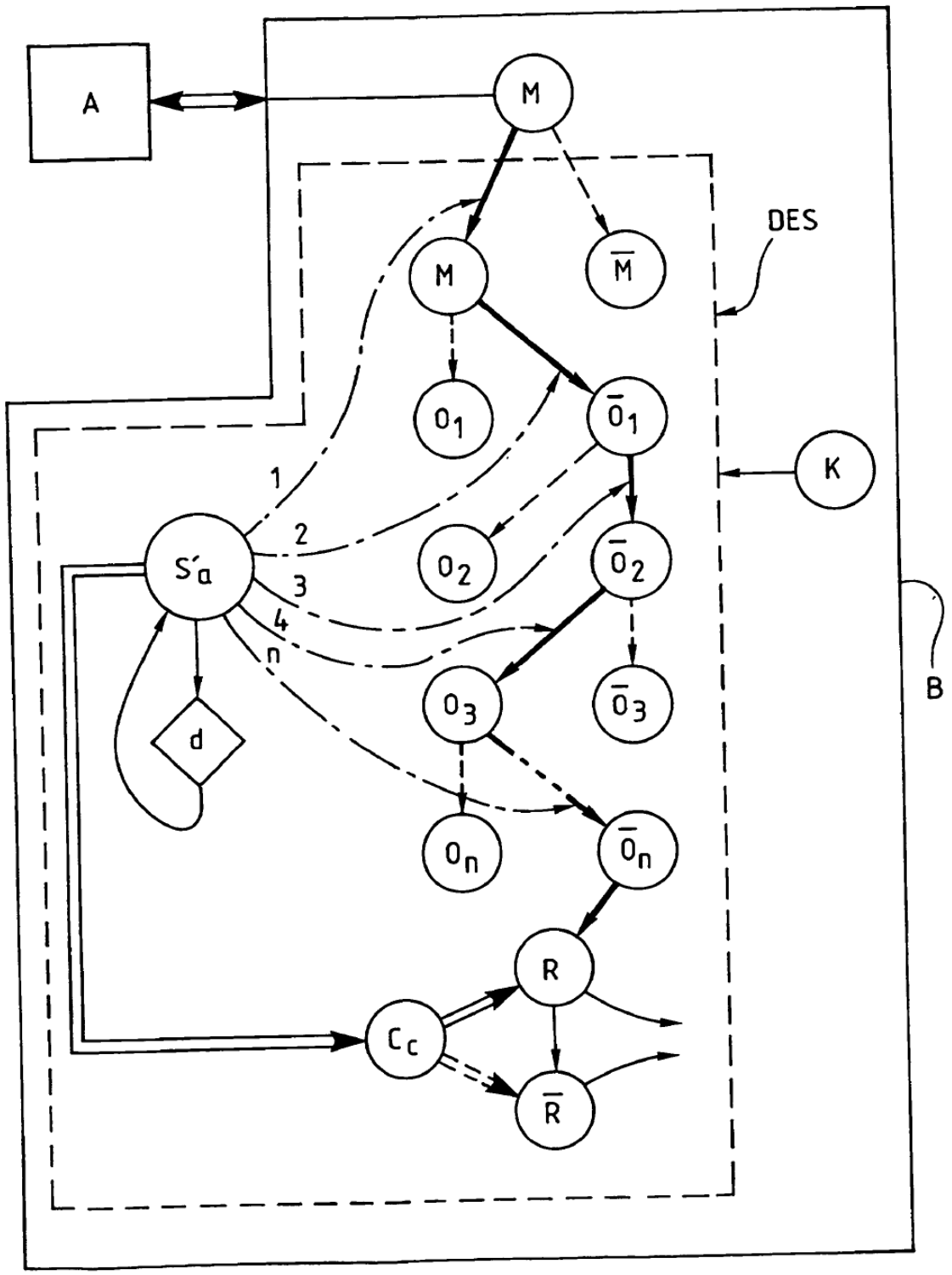
A
M
DES
M
$\overline{M}$
O_1
$\overline{O}_1$
K
1
2
3
4
n
S'a
O_2
$\overline{O}_2$
O_3
$\overline{O}_3$
d
O_n
$\overline{O}_n$
R
C_c
$\overline{R}$
B

Fig. 2