(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 606 185**

(51) Int. CI.:

G06F 7/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.01.2013 PCT/EP2013/000173**

(87) Fecha y número de publicación internacional: **22.08.2013 WO13120576**

(96) Fecha de presentación y número de la solicitud europea: **21.01.2013 E 13719371 (0)**

(97) Fecha y número de publicación de la concesión europea: **07.09.2016 EP 2805228**

(54) Título: **Procedimiento de protección contra ataques activos y dispositivo que usa el procedimiento**

(30) Prioridad:

20.01.2012 FR 1200174

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.03.2017

(73) Titular/es:

CASSIDIAN CYBERSECURITY SAS (100.0%)
1 Boulevard Jean Moulin, ZAC de la Clef Saint Pierre
78990 Elancourt, FR

(72) Inventor/es:

FRANCQ, JULIEN y
THUILLET, CÉLINE

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Procedimiento de protección contra ataques activos y dispositivo que usa el procedimiento

Campo de la invención

La presente invención se refiere en general a un procedimiento de protección contra ataques activos y al dispositivo que usa dicho procedimiento. Más particularmente, el objetivo de la invención es proponer un procedimiento para proteger el procesamiento de datos sensibles en un dispositivo contra ataques activos.

Antecedentes de la invención y problemas técnicos encontrados

En general, cuando se implementan primitivas criptográficas en un sistema criptográfico, es necesario tener en cuenta y prevenir los intentos de extraer datos sensibles, de manera fraudulenta, tales como la clave de encriptación. Dichos intentos pueden realizarse mediante ataques físicos que implican un análisis de la información desde el sistema criptográfico e inferir los datos sensibles a partir de la misma. Hay dos categorías de ataques físicos: ataques pasivos y ataques activos.

Los ataques físicos pasivos, que se denominan también SCAs (Side Channel Attacks, ataques de canal lateral), no requieren ninguna interacción directa con el sistema criptográfico. Un atacante simplemente observa las características del circuito criptográfico en funcionamiento e infiere la información sensible. De hecho, existe una correlación entre los datos procesados por el sistema y las características de dicho sistema, tales como el consumo de energía, emanaciones electromagnéticas, tiempo de cálculo, etc. El análisis de estas correlaciones puede hacer que sea posible recuperar información confidencial, tal como las claves de encriptación.

Los ataques físicos activos consisten en alterar el funcionamiento normal del circuito mediante la aplicación de un fallo usando una fuente externa, tal como una fuente de luz (luz blanca, un haz láser), una fuente magnética, una fuente de calor, etc. Los ataques activos, tales como ataques de interferencia, consisten en la modificación de ciertas señales de entrada del sistema, tales como la tensión de alimentación del sistema o su frecuencia de reloj. De esta manera, el atacante puede recuperar potencialmente los resultados criptográficos corruptos en reacción a los ataques. La información sensible de un sistema criptográfico se determina mediante el análisis de las diferencias entre un resultado normal suministrado por el sistema y un resultado corrompido por un ataque.

Una contramedida conocida contra los ataques activos consiste en duplicar la misma operación de encriptación. Sin embargo, esa técnica es vulnerable, tanto durante un ataque activo como durante un ataque pasivo. Esto es debido a que si la duplicación de encriptación es realizada en paralelo, la energía de trabajo del circuito se duplica. La relación ruido-a-señal es fácilmente observable y utilizable por un atacante. Si la duplicación se realiza en serie, el atacante puede realizar un ataque activo en dos posibles tiempos.

Es por esto que existe una necesidad de prevenir tanto los ataques activos como los ataques pasivos durante las operaciones sobre datos sensibles en un dispositivo de procesamiento.

Sumario de la invención

Un objetivo de la invención es proteger el dispositivo de procesamiento de datos sensibles contra posibles ataques activos, y también tener en cuenta el comportamiento del dispositivo de procesamiento para prevenir ataques pasivos.

La invención proporciona de esta manera un procedimiento para proteger el procesamiento de datos sensibles implementado por un dispositivo de procesamiento destinado a procesar datos de entrada sensibles con el fin de obtener datos de salida sensibles, en el que el procesamiento de datos se divide en al menos dos funciones de procesamiento. El procedimiento comprende:

- la aplicación de una primera función a los datos de entrada sensibles para obtener los primeros datos intermedios,

  y comprende también las tres etapas recurrentes siguientes para cada aplicación sucesiva de cada una de las funciones siguientes:

- aplicación de la subsiguiente función a los datos intermedios obtenidos anteriormente mediante la aplicación de una función anterior, para obtener los datos intermedios subsiguientes,

- simultáneamente con la aplicación de la función siguiente, detección de un ataque mediante la verificación de la exactitud de los datos intermedios obtenidos anteriormente, e

- infección de los datos intermedios obtenidos subsiguientemente si se detecta un ataque,

los siguientes datos intermedios obtenidos mediante la aplicación de la última función subsiguiente son los datos de salida sensibles con un valor exacto o infectado.

La invención ofrece el beneficio de proteger un dispositivo de procesamiento de datos sensibles tanto contra ataques activos como contra ataques pasivos. Esto es debido a que la ejecución de cada etapa de aplicación de una función subsiguiente simultáneamente con la ejecución de una etapa de detección de ataque hace que sea difícil para un atacante llevar a cabo con precisión un ataque activo. Un atacante activo o pasivo no puede aislar fácilmente la ejecución de cada etapa del procesamiento de los datos sensibles. Además, la etapa de detectar un ataque después de cada aplicación de una función de procesamiento hace que sea posible detectar un ataque activo más rápidamente.

La invención hace que sea posible minimizar la información proporcionada a un atacante gracias a la etapa de infección de los datos de salida después de detectarse un ataque. El atacante no puede correlacionar los datos de salida sensibles infectados con un trabajo particular del dispositivo.

La invención comprende también cualquiera de las características siguientes:

- una última etapa de detección de un ataque mediante el análisis de los últimos datos intermedios subsiguientes obtenidos mediante la aplicación de la última función subsiguiente y una infección de los últimos datos intermedios subsiguientes obtenidos si se detecta un ataque;
- la etapa de detección de un ataque comprende una aplicación de una función inversa de la función anterior, en el que la función inversa es aplicada a los datos intermedios obtenidos anteriormente para obtener un resultado, y una comparación del resultado obtenido con los datos antes de la aplicación de la función anterior, en el que se detecta un ataque si el resultado obtenido y dichos datos no son idénticos;
- la etapa de infección de los datos intermedios subsiguientes comprende la sustitución del valor de los datos intermedios subsiguientes con un valor aleatorio o un valor nulo;
- o la etapa de infección de los datos intermedios subsiguientes comprende un operador lógico OR exclusivo a aplicar a los datos intermedios subsiguientes con un valor aleatorio;
- la etapa de infección de los datos intermedios subsiguientes comprende la sustitución del valor de los datos secretos a aplicar posteriormente a los datos intermedios subsiguientes, con un valor aleatorio o un valor nulo; y
- una aplicación de una función ficticia a los últimos datos intermedios subsiguientes, simultáneamente con una última detección de un ataque mediante el análisis de los últimos datos intermedios subsiguientes.

La invención se refiere también a un dispositivo de procesamiento que implementa un procedimiento para proteger el procesamiento de datos sensibles, destinado a procesar los datos de entrada sensibles con el fin de obtener datos de salida sensibles, en el que el procesamiento de datos se divide en al menos dos funciones de procesamiento. El dispositivo comprende:

- una entidad de procesamiento para aplicar, de manera sucesiva, las funciones de procesamiento a los datos de entrada sensibles, y para obtener los datos de salida sensibles después de aplicar la última función de procesamiento,
- una entidad de protección para detectar un ataque simultáneamente con cada aplicación de una función de procesamiento, e infectar los datos resultantes de la aplicación de cada función de procesamiento si se detecta un ataque.

Breve descripción de las figuras

La invención se comprenderá más fácilmente en la descripción siguiente y las Figuras que la acompañan. Las Figuras se presentan sólo con propósitos ilustrativos y no limitativos. Las Figuras ilustran:

- La Figura 1 es una representación esquemática de un dispositivo criptográfico según la invención; y
- La Figura 2 es un diagrama funcional de un procedimiento para la protección contra ataques invasivos según la invención.

Descripción de la invención

Cabe señalar que las Figuras no están a escala.

Las realizaciones siguientes son ejemplos. Aunque la descripción se refiere a una o más realizaciones, no significa necesariamente que cada referencia se refiere a la misma realización o que las características se aplican a solo una

realización. Las características simples de las diferentes realizaciones pueden combinarse también para proporcionar otras realizaciones.

La Figura 1 representa un dispositivo DT de procesamiento según la invención. El dispositivo DT de procesamiento hace referencia a un dispositivo que comprende una entidad ET de procesamiento capaz de aplicar a los datos DE de entrada sensibles un algoritmo AG para procesar dichos datos de entrada sensibles según los datos secretos para obtener datos DS de salida sensibles. Los datos DE de entrada pueden ser datos a encriptar o desencriptar. Los datos DS de salida pueden ser datos encriptados o desencriptados. Los datos secretos pueden ser cables de encriptación y/o desencriptación, claves de autenticación u otras claves. El dispositivo DT de procesamiento según la invención comprende también una entidad EP de protección capaz de proteger la entidad ET de procesamiento durante su trabajo contra todos los ataques no invasivos. La entidad EP de protección comprende un módulo MD detección que detecta los posibles ataques activos, un módulo MI de infección para infectar los datos DS de salida si se detecta un ataque activo.

Las diferentes entidades y módulos enumerados anteriormente pueden ser elementos de hardware o funcionales, tales como programas grabados en una o más unidades de memoria y ejecutados por una unidad de procesamiento. Las unidades de memoria y la unidad de procesamiento forman una parte integral del dispositivo de procesamiento. Dichas unidades de memoria y de procesamiento son conocidas por la persona con conocimientos en la materia y no están cubiertas por la presente invención. De esta manera, no es necesaria una descripción más detallada de estas unidades.

El dispositivo DT de procesamiento puede ser un microcontrolador con una memoria programable o un circuito integrado especial dedicado.

El algoritmo AG para procesar datos sensibles puede ser un algoritmo de autenticación de clave secreta del tipo AKA (Authentication and Key Agreement, autenticación y acuerdo de claves). El algoritmo AG para procesar datos sensibles puede ser un algoritmo criptográfico que puede encriptar o desencriptar los datos sensibles, por ejemplo encriptación y/o desencriptación de tipo AES (Advanced Encryption Standard, estándar de encriptación avanzada, FIPS 197) o encriptación de bloque o encriptación de clave pública tal como RSA (Rivest Shamir Adleman) o ECC (Elliptic Curve Cryptography, criptografía de curva elíptica). El algoritmo para procesar datos sensibles tiene la característica de que está compuesto de al menos dos funciones f y g de procesamiento a ser ejecutadas sucesivamente. De esta manera, los datos DS de salida obtenidos normalmente por el algoritmo AG en función de los datos DE de entrada se obtienen según la ecuación siguiente: $DS = g°f(DE)$.

En un ejemplo, el algoritmo AG de procesamiento puede ser un algoritmo criptográfico de un tipo AES conocido, dividido en cuatro funciones de procesamiento conocidas: función F = AddRoundKey, función g = SubBytes, función h = ShiftRows y función z = MixColumns. Las cuatro funciones son ejecutadas sucesivamente por la entidad de procesamiento. La división del algoritmo AES puede ser diferente y puede comprender por ejemplo dos funciones de procesamiento: función f = SubBytes°AddRoundKey y función g = MixColumns°ShiftRows.

El diagrama funcional de la Figura 2 representa las etapas del procedimiento en la invención. El ejemplo del algoritmo AG de procesamiento considerado es un algoritmo que comprende cuatro funciones f, g, h y z que se ejecutan sucesivamente.

En la etapa E1, la entidad ET de procesamiento aplica la primera función f a los datos DE de entrada para obtener los primeros datos DI1 intermedios.

En la etapa E2, la entidad ET de procesamiento aplica la segunda función g a los primeros datos DI1 intermedios para obtener los segundos datos DI2 intermedios.

En la etapa E3, que es simultánea con la etapa E2, la entidad PE de protección, y más particularmente el módulo MD de detección, verifica si los primeros datos DI1 intermedios obtenidos son exactos. La verificación E3 comprende dos sub-etapas E30 y E31 sucesivas. Durante una primera sub-etapa E30, el módulo MD de detección aplica a los primeros datos DI1 intermedios una primera función f^{-1} inversa de la primera función f aplicada anteriormente. Durante la segunda sub-etapa E31, el módulo MD compara el resultado obtenido con los datos DE de entrada, que son los datos antes de la aplicación de la primera función f.

En la etapa E4, si los datos DI1 intermedios son exactos, es decir, si los datos DE y el resultado obtenido mediante la aplicación de la función f^{-1} inversa son idénticos, entonces los segundos datos DI2 intermedios no se modifican y la entidad ET de procesamiento ejecuta directamente la etapa E5.

Si, por el contrario, en la etapa E4, los primeros datos DI1 intermedios no son exactos, se detecta un ataque activo. En ese caso, la entidad EP de protección, más particularmente el módulo MI de infección, infecta el valor de los segundos datos DI2 intermedios. Una infección consiste en sustituir el valor de los datos por un valor aleatorio desde una fuente aleatoria comprendida en el dispositivo de procesamiento. Como alternativa, el módulo MI de infección puede sumar

una variable aleatoria a los datos intermedios corrompidos mediante la aplicación de un operador lógico OR exclusivo. En otra alternativa, si el dispositivo DT de procesamiento no comprende una fuente aleatoria, el módulo MI de infección sustituye el valor de los datos con un valor nulo. El objetivo de la etapa de infección es des-correlacionar las funciones de procesamiento realizadas anteriormente y los datos intermedios obtenidos. De esta manera, un atacante obtiene un resultado que comprende información inservible. Después de infectar los segundos datos DI2 intermedios, la entidad ET de procesamiento ejecuta la siguiente etapa E5 usando los datos DI2 intermedios infectados. El procedimiento no se detiene en cuanto se detecta un ataque activo con el fin de no informar al atacante que está observándolo que se ha detectado un ataque y que los datos de salida sensibles están comprometidos.

En una alternativa, después de una detección de un ataque, el módulo de infección puede infectar también los datos secretos usados en la siguiente función a aplicar. De esta manera, los datos secretos pueden ser sustituidos por un valor aleatorio o un valor nulo. Se produce una doble infección en los datos intermedios y los datos secretos.

La ejecución de las etapas E2 a E4 se repite en las etapas E5 a E7 y E8 a E10 para procesar cada función, h, z no procesada todavía y para verificar los datos emitidos desde cada función g, h aplicada anteriormente.

De esta manera, las etapas E5, E6 y E7, relacionadas con el procesamiento de la tercera función h respectiva, se refieren a:

- aplicación de la etapa E5 de la tercera función h a los segundos datos DI2 intermedios obtenidos anteriormente con un valor exacto o infectado, con el fin de obtener los terceros datos DI3 intermedios,
- etapa E6 de detección, simultáneamente con la etapa E5 anterior, para verificar la exactitud de los segundos datos DI2 intermedios obtenidos anteriormente mediante la aplicación (E60) de la función g^{-1} inversa de la función g y mediante la comparación (E61) del valor obtenido con el valor de los primeros datos DI1 intermedios, y
- etapa de infección de los terceros datos DI3 intermedios si se encuentra que los segundos datos DI2 intermedios obtenidos anteriormente no son correctos.

De manera similar, las etapas E8, E9 y E10, se refieren al procesamiento de la cuarta función z, respectivamente, relacionada con:

- etapa E8 de aplicación de la cuarta función z a los terceros datos DI3 intermedios obtenidos anteriormente con un valor exacto o infectado, con el fin de obtener los cuartos datos DI4 intermedios,
- etapa E9 de detección, simultáneamente con la etapa E8 anterior, para comprobar la exactitud de los terceros datos DI3 intermedios obtenidos anteriormente mediante la aplicación (E90) de la función h^{-1} inversa de la función h y mediante la comparación (E91) del valor obtenido con el valor de los segundos datos DI2 intermedios, y
- etapa de infección de los cuartos datos DI4 intermedios si se encuentra que los terceros datos DI3 intermedios obtenidos anteriormente no son correctos.

La recurrencia de la ejecución de las etapas simultáneas para el procesamiento de una función y para la verificación de los datos obtenidos mediante la aplicación de la función de procesamiento anterior puede ser ejecutada tantas veces como funciones de procesamiento sucesivas comprenda el algoritmo. De esta manera, el procedimiento de la invención hace que sea posible verificar, una función tras otra, la precisión de los resultados intermedios a lo largo de todo el procesamiento y, de esta manera, detectar muy rápidamente si se ha producido un ataque activo. De manera similar, la ejecución simultánea de las etapas de procesamiento y de detección hace posible ocultar el funcionamiento interno exacto del dispositivo de procesamiento a un observador externo que quiere realizar un ataque pasivo sobre el dispositivo. Dicha recurrencia hace posible también proteger todas las etapas de procesamiento, detección e infección.

Uno de los propósitos de la invención es minimizar la información suministrada de manera pasiva a un observador externo. De esta manera, para mantener el funcionamiento homogéneo del dispositivo de procesamiento, durante la etapa E12 (E120, E121) para la detección mediante la verificación de la exactitud de los últimos datos obtenidos mediante la aplicación de la última función (z) del algoritmo de procesamiento, una etapa E11 para la aplicación de una función ficticia a aplicar a los últimos datos obtenidos puede ser añadida de manera simultánea a la etapa E12. La función ficticia es una función que no modifica el valor de los datos a procesar. La etapa E12 de detección comprende un comportamiento idéntico a las etapas E3, E6 y E9 de detección. Dependiendo del resultado de la detección E12, en la etapa E13, el módulo de infección sustituye o no sustituye el valor de los datos procesados en la etapa E11. La recurrencia del procesamiento y de la detección de ataques se mantiene. Los últimos datos obtenidos mediante la aplicación de la última función son los datos DS de salida sensibles con un valor exacto o infectado.

La función ficticia hace que sea posible prevenir que un observador externo, que ataca el dispositivo de manera pasiva,

detecte una diferencia en el trabajo del dispositivo de tratamiento.

Si el algoritmo de procesamiento debe dividirse, puede añadirse una etapa ficticia simultáneamente con la verificación de los datos obtenidos durante la aplicación de la última función del algoritmo de procesamiento.

En una alternativa, para la protección contra ataques pasivos, pueden añadirse de manera regular otras etapas ficticias después de las etapas de procesamiento. Estas etapas ficticias tienen una duración predeterminada para permitir la desincronización del procesamiento llevado a cabo sobre los datos sensibles.

REIVINDICACIONES

1. Procedimiento para proteger un procesamiento (AG) de datos sensibles implementado por un dispositivo (DT) de procesamiento destinado a procesar datos (DE) de entrada sensibles con el fin de obtener datos (DS) de salida sensibles, en el que el procesamiento de datos se divide en al menos dos funciones (f, g, h, z) de procesamiento, en el que el procedimiento comprende:

- una aplicación (E1) de una primera función (f) a los datos (DE) de entrada sensibles para obtener los primeros datos (DI1) intermedios,

y comprende también las tres etapas recurrentes siguientes para cada aplicación sucesiva de cada una de las funciones (g, h, z) siguientes:

- una aplicación (E2, E5, E8) de la función (g, h, z) subsiguiente a los datos (DI1, DI2, DI3) intermedios obtenidos anteriormente mediante la aplicación de una función (f, g, h) anterior, para obtener los datos (DI2, DI3, DI4) intermedios subsiguientes,
- simultáneamente con la aplicación de la función siguiente, una detección (E3, E6, E9) de un ataque mediante la verificación de la exactitud de los datos (DI1, DI2, DI3) intermedios obtenidos anteriormente, y
- una infección (E4, E7, E10) de los datos (DI2, DI3, DI4) intermedios obtenidos posteriormente si se detecta un ataque,

los datos intermedios siguientes obtenidos mediante la aplicación de la última función subsiguiente son los datos (DS) de salida sensibles con un valor exacto o infectado.

2. Procedimiento según la reivindicación 1, que comprende una última etapa (E12) de detección de un ataque mediante el análisis de los últimos datos (DI4) intermedios subsiguientes obtenidos mediante la aplicación de la última función (z) subsiguiente y una infección (E13) de los últimos datos (DI4) intermedios subsiguientes obtenidos si se detecta un ataque.

3. Procedimiento según la reivindicación 1 o 2, en el que la etapa (E3, E6, E9, E12) de detección de un ataque comprende:

- una aplicación (E30, E60, E90, E120) de una función (f^{-1}, g^{-1}, h^{-1}, z^{-1}) inversa de la función (f, g, h, z) anterior, en el que la función inversa se aplica a los datos (DI1, DI2, DI3, DI4) intermedios obtenidos anteriormente para obtener un resultado, y
- una comparación (E31, E61, E91, E121) del resultado obtenido con los datos (DE, DI1, DI2, DI3) antes de la aplicación de la función (f, g, h, z) anterior, en la que se detecta un ataque si el resultado obtenido y dichos datos no son idénticos.

4. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que la etapa (E4, E7, E10, E13) de infección de los datos (DI2, DI3, DI4) intermedios subsiguientes comprende una sustitución del valor de los datos intermedios subsiguientes con un valor aleatorio.

5. Procedimiento según cualquiera de las reivindicaciones 1 a 3, en el que la etapa (E4, E7, E10, E13) de infección de los datos (DI2, DI3, DI4) intermedios subsiguientes comprende una sustitución del valor de los datos intermedios subsiguientes con un valor nulo.

6. Procedimiento según cualquiera de las reivindicaciones 1 a 3, en el que la etapa (E4, E7, E10, E13) de infección de los datos (DI2, DI3, DI4) intermedios subsiguientes comprende un operador lógico OR exclusivo a aplicar a los datos intermedios subsiguientes con un valor aleatorio.

7. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que la etapa (E4, E7, E10) de infección de los datos (DI2, DI3, DI4) intermedios subsiguientes comprende la sustitución del valor de los datos secretos a aplicar posteriormente a los datos intermedios subsiguientes, con un valor aleatorio o un valor nulo.

8. Procedimiento según cualquiera de las reivindicaciones anteriores, que comprende una aplicación (E11) de una función ficticia a los últimos datos (DI4) intermedios subsiguientes, simultáneamente con una última detección (E12) de un ataque mediante el análisis de la exactitud de los últimos datos intermedios subsiguientes.

9. Dispositivo de procesamiento que implementa un procedimiento para proteger el procesamiento (AG) de datos sensibles según cualquiera de las reivindicaciones 1 a 8, destinado a procesar datos (DE) de entrada sensibles con el fin de obtener datos (DS) de salida sensibles, en el que el procesamiento de datos se divide en al menos dos funciones (f, g) de procesamiento, en el que el dispositivo comprende:

- una entidad (ET) de procesamiento para aplicar sucesivamente las funciones de procesamiento a los datos de entrada sensibles, y para obtener los datos de salida sensibles después de aplicar la última función de procesamiento, y

- una entidad (EP) de protección para detectar un ataque simultáneamente con cada aplicación de una función de procesamiento, e infectar los datos resultantes de la aplicación de cada función de procesamiento si se detecta un ataque.

FIG. 1

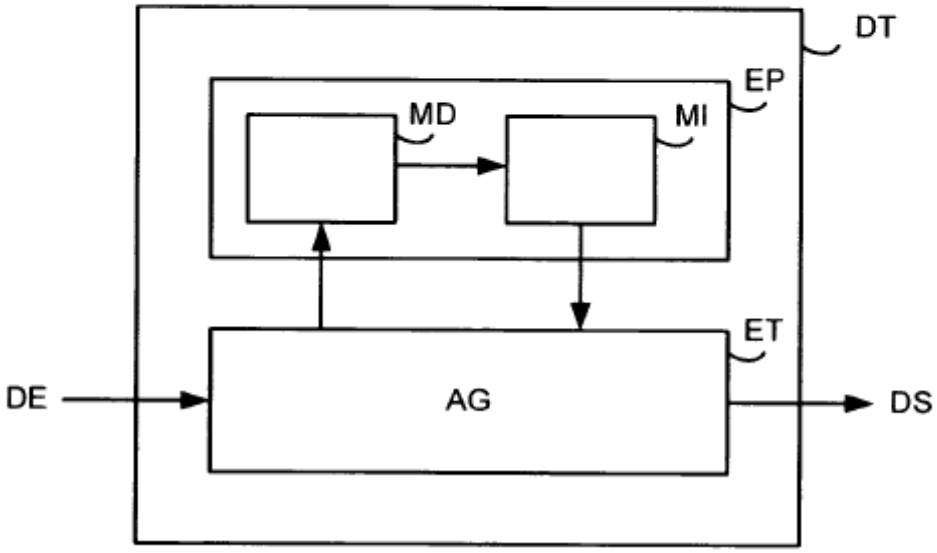
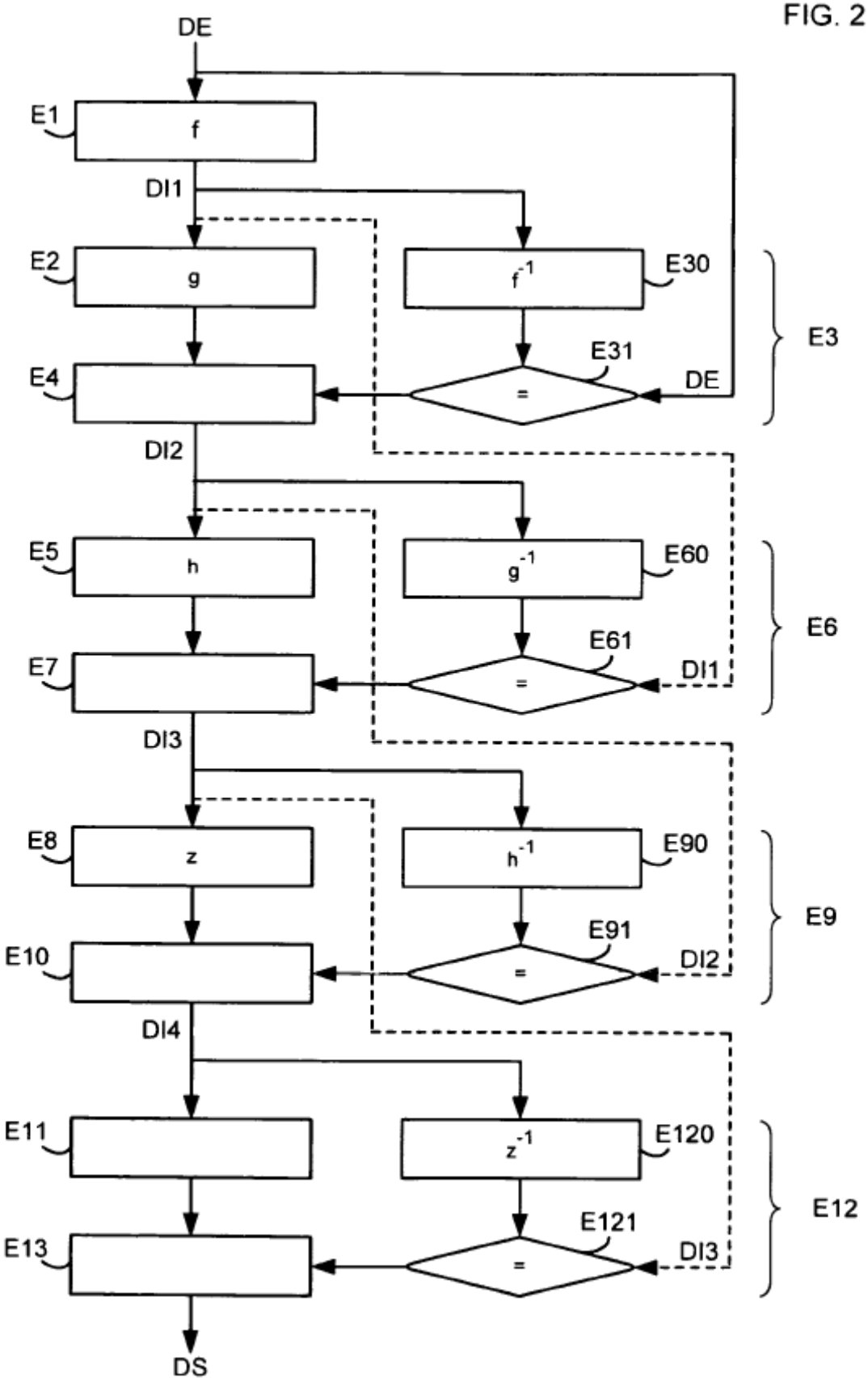


FIG. 2


DE
E1
f
DI1
E2
g
f^{-1}
E30
E31
E4
=
DE
E3
DI2
E5
h
g^{-1}
E60
E61
E7
=
DI1
E6
DI3
E8
z
h^{-1}
E90
E91
E10
=
DI2
E9
DI4
E11
z^{-1}
E120
E121
E13
=
DI3
E12
DS